

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

На правах рукописи



Харисова Зарина Ирековна

**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ПРИКЛАДНЫЕ АСПЕКТЫ
РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ
В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

Специальность 5.1.4. Уголовно-правовые науки
(юридические науки)

ДИССЕРТАЦИЯ
на соискание ученой степени
доктора юридических наук

Научный консультант:
доктор юридических наук, профессор
Макаренко Илона Анатольевна

Уфа – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	5

ГЛАВА 1. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ И МОДЕЛИРОВАНИЯ, ФАКТОРЫ ИХ ЭВОЛЮЦИИ И ТРАНСФОРМАЦИИ ... 32

1.1. Преступления в сфере компьютерной информации как объект криминалистического исследования	32

1.2. Криминалистическая модель преступлений в сфере компьютерной информации (структурно-содержательный анализ элементов криминалистической характеристики)	59

1.2.1. Криминалистическая характеристика неправомерного доступа к компьютерной информации	67

1.2.2. Криминалистическая характеристика незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а равно создания и (или) обеспечения функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения	82

1.2.3. Криминалистическая характеристика создания, использования и распространения вредоносных компьютерных программ	95

1.2.4. Криминалистическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	108

1.2.5. Криминалистическая характеристика неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации	119

1.3. Генезис преступлений, совершаемых в сфере компьютерной информации, и их детерминанты	138

ГЛАВА 2. КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ОСНОВЫ ИССЛЕДОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ 150

2.1. Криминалистические средства расследования преступлений в сфере компьютерной информации	150

2.2. Роль программных технико-криминалистических средств при расследовании преступлений в сфере компьютерной информации	162

2.3. Проблемы и пути совершенствования деятельности по собиранию, исследованию, оценке и использованию цифровых доказательств при расследовании преступлений в сфере компьютерной информации	176

ГЛАВА 3. ОСНОВЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ 196

3.1. Особенности возбуждения уголовных дел о преступлениях в сфере компьютерной информации 196

3.2. Организационно-тактические особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации 206

ГЛАВА 4. ОРГАНИЗАЦИОННЫЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ АЛГОРИТМИЗАЦИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 239

4.1. Соотношение следственных ситуаций и алгоритмов расследования преступлений в сфере компьютерной информации 239

4.2. Криминалистическое кодирование преступлений в сфере компьютерной информации и его роль в формировании интеллектуальных алгоритмов расследования 257

4.3. Правовые, методические, организационные и технические основы применения типовых алгоритмов расследования преступлений в сфере компьютерной информации 274

ГЛАВА 5. ИНТЕЛЛЕКТУАЛИЗАЦИЯ ПРОЦЕССА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ КАК ОСНОВА РАЗВИТИЯ ТЕОРИИ ИНФОРМАЦИОННО-КОМПЬЮТЕРНОГО ОБЕСПЕЧЕНИЯ КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ 304

5.1. Концептуальные основы учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности 304

5.2. Концепция нейросетевого криминалистического кластера данных как основа систематизации криминалистически значимой компьютерной информации 323

5.3. Цифровая криминалистическая модель преступления в сфере компьютерной информации (модель цифрового двойника преступного деяния) на основе нейросетевого криминалистического кластера данных 336

ЗАКЛЮЧЕНИЕ 363

СПИСОК ЛИТЕРАТУРЫ 380

ПРИЛОЖЕНИЯ 442

ПРИЛОЖЕНИЕ 1. Обобщенные данные по результатам опроса сотрудников органов дознания, следствия и оперативных подразделений (с указанием результатов опроса 560 человек)	442
ПРИЛОЖЕНИЕ 2. Динамика использования населением РФ сети «Интернет» за период с 2014 по 2024 г.г.	461
ПРИЛОЖЕНИЕ 3. Динамика количества подключенных к сети «Интернет» пользователей в мире за период с 2005 по 2024 г.г.	462
ПРИЛОЖЕНИЕ 4. Динамика зарегистрированных преступлений, совершаемых в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий за период с 2020 по 2024 г.г.	463
ПРИЛОЖЕНИЕ 5. Формы направления заявлений (сообщений) о преступлениях.....	464
ПРИЛОЖЕНИЕ 6. Свидетельства о государственной регистрации программ для ЭВМ (программные технико-криминалистические средства, применяемые при расследовании преступлений в сфере компьютерной информации)	466
ПРИЛОЖЕНИЕ 7. Аналитическая справка по результатам исследования материалов уголовных дел о преступлениях в сфере компьютерной информации (обобщенные данные о наиболее значимых признаках рассматриваемых преступных деяний)	472

ВВЕДЕНИЕ

Актуальность темы исследования. Стремительное развитие информационно-телекоммуникационных технологий неизбежно привело к цифровой трансформации экономики и общества. Перевод различных процессов повседневной жизнедеятельности человека в онлайн-формат, повышение доступности использования сетей «Интернет» и блокчейн, устройств связи и технических средств, в том числе интеллектуальных, построенных на базе облачных технологий и Интернета вещей, экспоненциально расширили область воздействия преступников. Низкая осведомленность населения в области защиты информации в совокупности с отсутствием специальных знаний в сфере безопасной эксплуатации вычислительной техники, информационно-телекоммуникационных систем и каналов связи планомерно определили относительно легкую мишень для реализации кибератак в целях завладения охраняемой законом информацией и неправомерного ее использования. Стоит также отметить относительную доступность информации, размещаемой в настоящее время в открытом доступе и раскрывающей различные методы и средства совершения преступлений в сфере компьютерной информации, точки входа для воздействия на потенциальных жертв, а также способы обхода имеющихся систем безопасности. Возможность реализации анонимных соединений, получения значительной выгоды без использования труднодоступных инструментов, вывод полученных ценностей в виде цифровых активов и транснациональный характер указанных деяний привели к проблеме отслеживания и привлечения к ответственности такого рода преступников. Таким образом, преступления в сфере компьютерной информации становятся все более распространенной и опасной угрозой для граждан, организаций и государств.

Актуальность проблемы подтверждается проводимым Главным информационно-аналитическим центром МВД России ежегодным анализом статистических сведений о состоянии преступности, так, по состоянию на 2021 год было отмечено, что каждое четвертое преступление совершалось с использованием информационных технологий¹ (25,83 % от числа зарегистрированных за год), в

¹ Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: <https://media.mvd.ru/files/application/2315310> (дата обращения: 22.10.2025).

аналогичном периоде аналитического отчета, сформированного по состоянию на 2024 год², приводится информация о совокупной доли указанного вида преступлений в размере более трети (40,05 % от числа зарегистрированных за год). Имеющиеся статистические данные по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий в Российской Федерации за последние десять лет, позволяют с уверенностью констатировать, что сформированные методики расследования рассматриваемых преступлений не всегда являются результативными, а традиционные методы противодействия указанному виду преступности оказываются недостаточно эффективными.

Актуальность исследования также подтверждается рядом национальных стратегических направлений в области информатизации общества, что в отсутствие действенных инструментов расследования преступлений в сфере компьютерной информации закономерно может усугубить сложившуюся ситуацию. Так, Указом Президента Российской Федерации от 07 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»³ в качестве одного из направлений наращивания потенциала нашей страны определена цель цифровой трансформации, в рамках которой к 2030 году установлены показатели в виде увеличения до 99 % доли социально-значимых услуг, доступных в электронном формате и роста до 97 % доли использования домохозяйствами широкополосного доступа к сети «Интернет», а также формирования рынка данных и их активного вовлечения в оборот. Кроме того, Указом Президента Российской Федерации от 10 октября 2019 г. № 490 утверждена национальная стратегия развития искусственного интеллекта⁴ на период до 2030 г., которая предусматривает обеспечение национальных интересов страны и

² Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: <https://media.mvd.ru/files/application/9209203> (дата обращения: 22.01.2025).

³ О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента Российской Федерации от 07 мая 2024 г. № 309 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_475991 (дата обращения: 22.10.2025).

⁴ О развитии искусственного интеллекта в Российской Федерации : Указ Президента Российской Федерации от 10 октября 2019 г. № 490 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_335184 (дата обращения: 22.10.2025).

реализацию приоритетов в области технологического развития, в частности, в целях повышения доступности информации и вычислительных ресурсов для пользователей в этой сфере.

Указанное в совокупности определяет появление новых угроз, связанных с использованием различных технологий в противоправных целях. Высокая степень латентности преступлений в сфере компьютерной информации с учетом широкой их распространенности, в свою очередь, определяет данную проблему на уровне национальной угрозы безопасности и, соответственно, требует принятия необходимых мер в целях выявления актуальных на сегодняшний день методик расследования рассматриваемых преступных деяний.

Необходимо констатировать, что проблемы расследования указанного вида преступлений на сегодняшний день требуют формирования принципиально новой системы знаний, которая позволит учесть фактор постоянного развития информационных технологий и цифровизации общественных отношений. Это определяет сложность возникающих перед правоохранительными органами задач. По этой причине в диссертационном исследовании затрагиваются особенности применения новых, прежде всего сквозных технологий (в том числе технологии искусственного интеллекта) применительно к расследованию преступлений в сфере компьютерной информации, что соответствует Концепции технологического развития Российской Федерации на период до 2030 г.⁵.

Отдельного рассмотрения требует потенциально новое поле для преступной деятельности в виде метавселенной (от англ. «metaverse» – метавселенная), которая определяется как онлайн-среда взаимосвязанных цифровых экосистем, созданных на базе виртуальных многопользовательских миров и технологий расширенной реальности, позволяющих осуществлять децентрализованное взаимодействие пользователей, представленных аватарами, с цифровыми объектами и активами⁶. Новый стек технологий для разработки

⁵ Об утверждении Концепции технологического развития на период до 2030 года : распоряжение Правительства Российской Федерации от 20 мая 2023 г. № 1315-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_447895 (дата обращения: 22.10.2025).

⁶ Метавселенная: точка зрения правоохранительных органов (примеры использования, преступления, криминалистика, расследования и управление) // Международная организация уголовной полиции Интерпол : офиц. сайт. URL: <https://www.interpol.int/content/download/20828/file/Metaverse%20%20a%20law%20enforcement%20perspective.pdf> (дата обращения: 22.10.2025).

децентрализованных веб-приложений в настоящее время позволяет пользователям не только формировать, но и управлять собственной цифровой личностью и активами не только в киберпространстве, но и в метасреде, в распределенных реестрах, квантовых вычислительных средах и пр. Таким образом, на примере лишь метапреступности можно отметить эволюционную грань в спектре киберпространства, которая не только сохраняет все неотъемлемые сходства с киберпреступностью, но и открывает множество новых беспрецедентных возможностей.

Несмотря на свой пока еще абстрактный и иммерсивный характер уже на сегодняшний день можно выявить предположительные проблемы и угрозы, которые порождает эволюция киберпространства в другие формы, соответственно, необходим новый подход к рассмотрению указанных проблем и формированию методик расследования преступлений, совершаемых в цифровом пространстве различного рода. Важность обозначенных проблем подтверждается и на международном уровне, в частности, одним из итогов работы государств-членов Организации Объединенных Наций, за период с 2019 по 2024 г.г. стало одобрение разработанной по инициативе Российской Федерации Конвенции против киберпреступности⁷ в целях укрепления международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных систем, и в обмене доказательствами в цифровой форме, которая запланирована основой для налаживания сотрудничества правоохранительных органов в области противодействия использованию информационных технологий в преступных целях.

В этой связи представляется актуальным: проведение структурно-содержательного анализа преступлений в сфере компьютерной информации с выявлением и систематизацией элементов их криминалистической характеристики; выявление эффективных методов и средств расследования указанного вида преступлений; определение наиболее перспективных направлений совершенствования деятельности по поиску и исследованию цифровых

⁷ Конвенция Организации Объединенных Наций против киберпреступности: укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям от 27 ноября 2024 г. (A/79/460) // Министерство иностранных дел Российской Федерации : офиц. сайт. URL: https://www.mid.ru/ru/foreign_policy/news/1989289 (дата обращения: 22.10.2025).

доказательств, в том числе на основе современных технологий анализа, обработки и интерпретации данных, выявление особенностей внедрения и использования программных технико-криминалистических средств; рассмотрение организационных и методических основ расследования преступлений в сфере компьютерной информации с применением типовых алгоритмов, основанных на технологии искусственного интеллекта; выявление возможности создания новейших криминалистических информационно-аналитических учетов с функционалом предиктивной аналитики; формирование цифровой криминалистической модели преступлений в сфере компьютерной информации как основы реализации типовых алгоритмов их расследования.

Степень научной разработанности темы исследования.

Мультидисциплинарный подход к изучению преступлений в сфере компьютерной информации обусловил подбор и использование относительно обширной базы источников, включающей не только криминалистическую литературу, но и исследования в области ряда иных социально-гуманитарных и технических наук.

Проблема расследования преступлений в сфере компьютерной информации стала актуальным объектом для криминалистического исследования преимущественно с приходом XXI века, хотя особенностям собирания и использования компьютерной информации при расследовании преступлений уделялось внимание с 90-х годов прошлого столетия. Необходимо отметить значительную степень научной разработанности отдельных вопросов рассматриваемой темы.

Различные аспекты расследования преступлений в сфере компьютерной информации рассматривались в диссертационных и иных криминалистических исследованиях таких авторов как А. В. Остроушко (2000), Н. Г. Шурухнова (2001), В. А. Мещерякова (2001), С. В. Крыгина (2002), Л. Н. Соловьева (2003), А. С. Егорышева (2004), В. П. Хомколова (2004), Р. А. Белевского (2006), И. Г. Ивановой (2007), В. Б. Вехова (2008), И. М. Рассолова (2008), Р. И. Дремлюги (2008), Ю. В. Гаврилина (2009), Н. А. Зигуры (2010), В. О. Давыдова (2013), Н. А. Подольного (2013), И. Г. Чекунова (2013), Е. С. Шевченко (2016), В. В. Коломинова (2017), И. А. Пузарица (2019), С. М. Голятиной (2020), А. М. Каминского (2020), Е. Р. Россинской (2021), А. А. Рудых (2020), О. П. Бердниковой (2021), Е. А. Рускевич (2021),

Р. А. Дерюгина (2021), Д. В. Завьяловой (2021), И. С. Пантюхина (2023), Н. И. Старостенко (2023), Ю. Н. Соколова (2023), Е. А. Хариной (2024), Б. Э. Шавалеева (2024) и многих других ученых.

Возможности алгоритмизации и программирования расследования, а также алгоритмы собирания и исследования доказательственной информации анализировались в научной и учебной литературе Н. С. Полевым (1982), М. Б. Вандером (1998), А. Р. Белкиным (2000), Е. Р. Россинской (2001), В. Б. Веховым (2002), А. С. Шаталовым (2002), В. Я. Колдиным (2002), Н. П. Яблоковым (2005), О. Я. Баевым (2010), Л. Я. Драпкиным (2014), О. П. Грибуновым (2016), И. М. Комаровым (2018), Е. П. Ищенко (2021), А. Ф. Волынским (2021), В. Н. Карагодиным (2021), Д. О. Буйновым (2024), А. Д. Цыплаковой (2025) и др.

Особенностям поиска и исследования цифровой информации при расследовании рассматриваемых преступлений посвящены работы А. В. Касаткина (1997), А. И. Усова (2002), А. И. Семикаленовой (2005), А. А. Шаевича (2007), А. В. Наружного (2009), Р. Р. Шарипова (2011), В. Ю. Агibalова (2012), Т. В. Аверьяновой (2013), Л. П. Зверьянской (2016), А. Р. Смолиной (2017), Е. В. Пискуновой (2017), А. Г. Себякина (2021), Е. Р. Россинской (2022), Д. О. Буйнова (2024), А. А. Саркисян (2025), А. Г. Волеводза (2025), А. Б. Смушкина (2025) и др.

Ряд исследований в области определения общеправового и криминалистического значения технологий искусственного интеллекта рассматривались в работах М. П. Морхата (2017), А. Г. Себякина (2019), А. Н. Охлупиной (2019), В. С. Овчинского (2020), А. А. Бессонова (2021), Р. В. Мещерякова (2021), И. Р. Бегишева (2021), Д. В. Бахтеева (2022), В. Ф. Васюкова (2022), Т. С. Волчецкой (2022), С. В. Зуева (2022), А. В. Незнамова (2022), В. Б. Вехова (2023), А. И. Усова (2024) и других ученых.

Проблемы предупреждения преступности в сфере компьютерной информации и противодействия ей посвящены труды А. А. Косынкина (2011), К. Н. Евдокимова (2023), И. И. Малыгина (2023), Н. А. Лихачева (2024), Г. Ф. Шипулина (2024) и других авторов.

Исследование возможностей применения различных технических средств и информационных технологий при расследовании преступлений в сфере компьютерной информации представлено в работах В. Д. Зеленского (1998), И. Н. Яковенко (2005), Л. Б. Красновой (2005), А. И. Семикаленовой (2005), Д. Ю. Гостевского (2010), В. Б. Вехова (2014), С. А. Ковалева (2014), Е. Г. Кравеца (2016), Л. В. Бертовского (2017), В. В. Глимеиды (2024), А. В. Нестерова (2024), А. Б. Смушкина (2025) и др.

Возможностям формирования цифровых и информационных криминалистических моделей преступлений, компьютерного моделирования их расследования посвящены работы таких авторов, как Т. С. Волчецкая (1991), М. К. Каминский (1996), В. Е. Корноухов (2000), Е. П. Ищенко (2006), В. Я. Колдин (2006), В. О. Давыдов (2012), В. Б. Вехов (2015), С. А. Ковалев (2015), Р. Л. Ахмедишин (2020), А. А. Бессонов (2020), Е. Р. Россинская (2021), А. И. Семикаленова (2021), У. А. Мусаева (2024) и др.

Имеется ряд трудов зарубежных ученых по рассматриваемой теме исследования таких, как В. Carrier (США, 2005), S. Garfinkel (США, 2007), А. Reyes (США, 2007), Р. Hunton (США, 2010), А. Khater (Катар, 2010), С. Hooper (Австралия, 2013), F. Iqbal (ОАЭ, 2013), W. Chang (Тайвань, 2014), С. Brown (Австралия, 2015), E. Vincze (США, 2016), V. Kebande (Швеция, 2018), A. Mbaziira (США, 2018), A. Powell (Австралия, 2018), J. Hou (Китай, 2019), I. Yaqoob (ОАЭ, 2019), R. Vinayakumar (ОАЭ, 2019), N. Karie (Австралия, 2020), A. Karimi (Иран 2020), I. Saha (Бангладеш, 2020), P. Sharma (Индия, 2020), M. Stamp (США, 2020), X. Chen (Китай, 2021), M. Elhoseny (ОАЭ, 2021), M. Garcia (Испания, 2021), J. Nicholls (Ирландия, 2021), K. Padma (Индия, 2021), Y. Baroniya (Индия, 2023), K. Barik (Испания, 2022), M. Brivot (Канада, 2023), N. Ganesh (Индия, 2022), A. Djenna (Алжир, 2023), A. Harisha (Индия, 2023), A. Mishra (Индия, 2023), Y. Narayana (Индия, 2023), O. Pal (Индия, 2023), E. Raj (Индия, 2023), P. Watters (Австралия, 2023), D. Dunsin (США, 2024), J. Edwards (США, 2024), R. Jain (Индия, 2025), S. Caneppele (Швейцария, 2025), S. Shetty (Индия, 2025), C. Singh (ЮАР, 2025) и других авторов.

Признавая важное значение трудов указанных исследователей необходимо отметить, что положения и разрабатываемые на их основе рекомендации, касающиеся расследования преступлений в сфере компьютерной информации,

рассмотрены не в полной мере, либо не рассмотрены вообще. До сегодняшнего дня комплексного исследования, посвященного структурно-содержательному анализу криминалистического обеспечения расследования преступлений в сфере компьютерной информации и способам интеграции технологий искусственного интеллекта в различные его этапы не проводилось. Очевидно, что сложившаяся практика расследования рассматриваемого вида преступлений требует своего уточнения, равно как требуется принципиально новый подход к собиранию, исследованию и оценке цифровых доказательств с использованием наиболее эффективных алгоритмов, в том числе на основе искусственного интеллекта.

По этой причине криминалистическая теория и практика раскрытия и расследования преступлений в сфере компьютерной информации нуждается в реализации нового подхода, основанного на структурированном исследовании обозначенной проблемы, анализе сложившейся судебной-следственной практики, в котором будут учтены фундаментальные работы криминалистов, посвященные рассматриваемому предмету.

Объектом диссертационного исследования выступают преступная деятельность в сфере компьютерной информации, а также деятельность правоохранительных органов по раскрытию и расследованию рассматриваемого вида преступлений.

Предметом диссертационного исследования являются закономерности механизма преступной деятельности в сфере компьютерной информации, а также основанные на познании этих закономерностей ситуационные и организационные особенности расследования данного вида преступлений, в том числе на основе практики формирования и использования интеллектуальных криминалистических средств и моделей рассматриваемых преступных деяний.

Цель диссертационного исследования состоит в разработке новой криминалистической концепции расследования преступлений в сфере компьютерной информации на основе интеграции алгоритмов искусственного интеллекта, направленной на совершенствование криминалистических методов и средств борьбы с указанными преступными деяниями в условиях их трансформации и эволюции, а также формулировании направлений совершенствования деятельности по поиску, анализу и интерпретации цифровых доказательств при расследовании противоправных деяний рассматриваемого вида.

Достижение данной цели обеспечивалось постановкой и решением ряда взаимосвязанных частных **задач**:

1. Провести анализ преступлений в сфере компьютерной информации, как объекта криминалистического исследования, определить значимость среды совершения рассматриваемых преступных деяний;

2. Раскрыть содержание и взаимосвязь элементов криминалистической характеристики преступлений в сфере компьютерной информации, позволяющих сформировать цифровую криминалистическую модель преступного деяния;

3. Изучить генезис преступлений, совершаемых в сфере компьютерной информации, показать их детерминанты и дискретность процесса противодействия им, рассмотреть возможные направления их трансформации с целью выявления наиболее перспективных прогностических методов расследования указанных противоправных деяний;

4. Рассмотреть криминалистические средства расследования преступлений в сфере компьютерной информации, среди которых выявить наиболее перспективные и универсальные инструменты;

5. Выявить ряд общих закономерностей механизма преступной деятельности в сфере компьютерной информации, а также роль программных технико-криминалистических средств при расследовании рассматриваемых преступлений;

6. Определить типичные проблемы и пути совершенствования деятельности по поиску цифровых доказательств при расследовании преступлений в сфере компьютерной информации;

7. Рассмотреть особенности и типичные алгоритмы действий на стадии возбуждения уголовного дела о преступлении в сфере компьютерной информации;

8. Рассмотреть организационно-тактические особенности отдельных следственных действий как системы закрепления собранных цифровых доказательств и расширения доказательственной базы при расследовании преступлений в сфере компьютерной информации;

9. Выявить роль следственных ситуаций как исходных условий для формирования алгоритмов расследования преступлений в сфере компьютерной информации;

10. Рассмотреть возможность криминалистического кодирования преступлений в сфере компьютерной информации в целях разработки

универсальной концепции их расследования в условиях постоянной трансформации и эволюции киберпреступности;

11. Сформировать основные правовые, методические, организационные и технические основы применения типовых алгоритмов расследования преступлений в сфере компьютерной информации, на основе которых предложить общий алгоритм их расследования в соответствии с категорией преступных деяний, способами совершения этих преступлений, способами обнаружения следов преступных деяний, а также мерами противодействия расследованию;

12. Сформировать концептуальные основы учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности в виде вектора развития частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности;

13. Сформировать концепцию нейросетевого криминалистического кластера данных как основу систематизации криминалистически значимой компьютерной информации;

14. Сформировать цифровую криминалистическую модель преступления в сфере компьютерной информации (модель цифрового двойника преступления) на основе нейросетевого криминалистического кластера данных, подтвердив применимость методов науки о данных в расследовании преступных деяний и обеспечив право на интеграцию учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности в практику расследования.

Основной начальной гипотезой исследования выступила идея об использовании элементов криминалистической характеристики преступных деяний, совершаемых в сфере компьютерной информации, в качестве обучающего набора данных для формирования интеллектуальной системы в виде цифровой криминалистической модели преступления (модели цифрового двойника), способствующей повышению эффективности расследования рассматриваемых преступлений, выявлению взаимосвязей между элементами их криминалистической характеристики и обеспечению выдачи оптимального алгоритма принятия решений в условиях информационной неопределенности.

Методологическую основу исследования составил диалектический метод познания с фокусировкой на системный подход к изучению возможностей поиска цифровых доказательств, что позволило выявить закономерности и взаимосвязи между элементами криминалистической характеристики преступлений в сфере компьютерной информации, определить перспективные направления их расследования. Инструментарий диссертационного исследования представлен комплексным использованием совокупности общенаучных (дедукции и индукции, анализа, синтеза, моделирования, формализации, описания, наблюдения, идеализации, обобщения, сравнения, классификации и др.) и частнонаучных методов научного познания (кибернетический, статистический, социологический, сравнительно-правовой и пр.).

Использование указанных методов позволило провести анализ и систематизацию научных знаний в области организации расследования преступлений, совершаемых в сфере компьютерной информации, осуществить обобщение и интерпретацию теоретического, правового и эмпирического материала. В частности, методы идеализации и обобщения способствовали выявлению проблемных ситуаций, складывающихся при расследовании рассматриваемых преступлений.

Методы сравнения, классификации, моделирования и формализации позволили всесторонне проанализировать и систематизировать имеющиеся сведения в области организации расследования преступлений, совершаемых в сфере компьютерной информации, выявить тенденции развития криминалистических знаний по собиранию цифровых доказательств.

Применительно к использованию программных технико-криминалистических средств при расследовании преступлений, совершаемых в сфере компьютерной информации, был рассмотрен кибернетический подход с фокусировкой на алгоритмизацию процессов расследования и методы интеллектуального анализа данных: моделирования (для формирования криминалистической модели преступления); классификации и прогнозирования (в целях установления принадлежности цифровых данных к соответствующим классам); кластеризации (выделения групп цифровых данных, имеющих сходные признаки); ассоциации (поиска корреляционных связей между данными); визуализации (использования графических методов отображения информации с

возможностью отображения скрытых закономерностей и пр.); машинного обучения, эволюционного моделирования, нечеткой логики и нечетких множеств (для создания модели системы, адаптированной под входные данные и алгоритмы расследования).

Статистический метод позволил осуществить сбор и интерпретацию статистических данных о состоянии преступности в рассматриваемой сфере, провести анализ материалов уголовных дел и организации деятельности правоохранительных органов. Социологический метод, применяемый при анкетировании сотрудников правоохранительных органов, способствовал обобщению наиболее значимых проблем, связанных с расследованием преступлений, совершаемых в сфере компьютерной информации.

Сравнительно-правовой метод способствовал изучению норм уголовного и уголовно-процессуального права, практики их применения. Кроме указанных в исследовании использовался ряд специальных методов: анализа распределенных баз данных (для рассмотрения возможностей обработки больших объемов информации); научно-технического прогнозирования и предиктивной аналитики (для выявления возможностей предотвращения преступлений); обеспечения достоверности информации (в целях признания результатов исследования объективными).

Использование совокупности вышеуказанных методов позволило определить перспективные пути решения проблем в области расследования преступлений в сфере компьютерной информации, а также выработать новые подходы в рассматриваемом направлении научного знания.

Теоретическую основу исследования составили научные труды в области таких дисциплин как криминалистика, логика, кибернетика, математическая статистика, информационные технологии в юридической деятельности, анализ данных, анализ распределенных данных, теория принятия решений, искусственный интеллект, нейронные сети, машинное обучение, компьютерное зрение, технология разработки программного обеспечения, системный анализ и управление и др.

Наибольшее внимание уделялось ключевым трудам отечественных ученых в области криминалистики, принадлежащим Т. В. Аверьяновой, Ф. Г. Аминеву, О. Я. Баеву, Д. В. Бахтееву, Р. С. Белкину, Л. В. Бертовскому, А. А. Бессонову, А. В. Варданяну, В. Ф. Васюкову, В. Б. Вехову, Т. С. Волчецкой, А. Ф. Волынскому, В. К. Гавло, Ю. В. Гаврилину, Ю. П. Гармаеву, А. Ю. Головину, О. П. Грибунову, Е. В. Денисову, Л. Я. Драпкину, К. Н. Евдокимову, Р. И. Зайнуллину, С. В. Зуеву, Е. П. Ищенко, А. М. Каминскому, М. К. Каминскому, В. Н. Карагодину, А. С. Князькову, С. А. Ковалеву, В. Я. Колдину, И. М. Комарову, О. Н. Коршуновой, И. М. Лузгину, Н. П. Майлис, И. А. Макаренко, В. А. Мещерякову, Т. Ф. Моисеевой, А. В. Незнамову, В. А. Образцову, В. С. Овчинскому, Н. А. Подольному, Е. В. Пискуновой, О. В. Полстовалову, А. А. Протасевичу, Е. Р. Россинской, Ю. Н. Соколову, Д. А. Степаненко, А. А. Тарасову, А. И. Усову, А. Н. Халикову, С. Е. Чаннову, А. С. Шаталову, А. А. Эксархопуло, Н. П. Яблокову и другим исследователям.

Нормативную базу исследования составили положения Конституции Российской Федерации, Уголовного кодекса Российской Федерации, Уголовно-процессуального кодекса Российской Федерации, Федеральные законы («О полиции», «Об оперативно-розыскной деятельности», «Об информации, информационных технологиях и о защите информации», «О безопасности», «О безопасности критической информационной инфраструктуры Российской Федерации», «О связи», «О государственной судебной-экспертной деятельности в Российской Федерации», «О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» и др.), Указы Президента Российской Федерации («О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», «О развитии искусственного интеллекта в Российской Федерации» и пр.), Доктрина информационной безопасности Российской Федерации, Постановления и распоряжения Правительства Российской Федерации, подзаконные нормативные акты министерств и ведомств в области расследования преступлений в сфере

компьютерной информации, обеспечения информационной безопасности и защиты информации, Национальная стратегия развития искусственного интеллекта на период до 2030 г., Стратегия национальной безопасности Российской Федерации, Стратегия развития информационного общества в Российской Федерации на 2017–2030 г.г., а также международные правовые акты в области борьбы с рассматриваемым видом преступности, зарубежные акты, регламентирующие ответственность за преступления, совершенные с использованием информационно-телекоммуникационных технологий («Окинавская хартия глобального информационного общества», «Будапештская конвенция о киберпреступности ETS № 185», «Руководство по разработке национальной стратегии кибербезопасности» Международного союза электросвязи ITU и пр.), Конвенция против киберпреступности: укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в цифровой форме, относящимися к серьезным преступлениям (A/79/460), международные стандарты в области кибербезопасности (ISO / IEC TS 27110:2021 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие указания по разработке основ кибербезопасности» («Information technology, cybersecurity and privacy protection Cybersecurity framework development guidelines»), ISO / IEC 27014:2020 «Информационная безопасность, кибербезопасность и защита конфиденциальности» («Information security, cybersecurity and privacy protection»), ISO / IEC 27032:2023 «Кибербезопасность. Руководство по обеспечению безопасности в сети «Интернет» («Cybersecurity guidelines for internet security»)) и др.

Эмпирическую базу исследования составили официальные статистические данные различных ведомств (МВД России, Федеральной службы государственной статистики, Генеральной прокуратуры Российской Федерации и пр.), информационно-аналитические материалы Судебного департамента при Верховном Суде Российской Федерации, результаты исследований Всероссийского научно-исследовательского института МВД России; статистические отчеты Акционерного общества «Лаборатория Касперского», сформированные на базе комплексной распределенной инфраструктуры для

интеллектуальной обработки потоков данных за период с 2017 по 2025 г.г.; открытые наборы данных (датасеты) различных ведомств, организаций и коммерческих платформ; информационно-аналитические обзоры по проблемам расследования преступлений в сфере компьютерной информации; отчеты и аналитические обзоры международных организаций (отчеты Международного союза электросвязи ITU, полицейской службы Европейского союза (Европол), Управления Организации Объединенных Наций по наркотикам и преступности и др.); результаты изучения экспертно-аналитических отчетов российских и зарубежных компаний, деятельность которых связана с расследованием преступлений в сфере компьютерной информации, обеспечения информационной безопасности и защиты информации (Центрального банка Российской Федерации, Акционерных обществ «Лаборатория Касперского», «Солар секьюрити», а также корпорации Google и пр.).

В рамках исследования было изучено 284 уголовных дела о преступлениях в сфере компьютерной информации, совершенных за период с 2020 по 2025 г.г. на территориях 17 регионов Российской Федерации, при помощи инструментов автоматизированного сбора и обработки данных были изучены 2500 приговоров, размещенных на официальных сайтах судов общей юрисдикции в сети «Интернет», по преступлениям в сфере компьютерной информации, совершенным за период с 2010 по 2025 г.г. на территориях 34 регионов Российской Федерации, а также 240 обезличенных отчетных форм по состоянию оперативной обстановки на территории обслуживания органа МВД России (Республика Башкортостан), сформированных в Сервисе обеспечения деятельности дежурных частей системы информационно-аналитического обеспечения деятельности МВД России по преступлениям в сфере компьютерной информации, совершенным за период с 2020 по 2025 г.г. (по ст. ст. 272, 272.1, 273, 274, 274.1, 274.2, 274.3, 274.4, 274.5 главы 28 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ, при этом на момент исследования практика применения норм по ст. ст. 274.2, 274.3, 274.4 и 274.5 отсутствовала).

Обобщены данные, полученные в результате анализа справок, обзоров, методических рекомендаций и других сведений следственных управлений Следственного комитета Российской Федерации, содержащие информацию о состоянии и тенденциях организации деятельности по выявлению, расследованию

и предупреждению преступлений в сфере компьютерной информации за период с 2020 по 2025 г.г.

Для обеспечения репрезентативности исследования сбор эмпирического материала осуществлялся в регионах с наибольшими и наименьшими темпами прироста зарегистрированных преступлений рассматриваемого вида, а также с наиболее высокими и низкими показателями коэффициента преступлений на 100 тыс. населения (Архангельская область, Воронежская область, Ивановская область, Калининградская область, Кировская область, Костромская область, Ленинградская область, Липецкая область, Мурманская область, Ненецкий автономный округ, Нижегородская область, Новгородская область, Новосибирская область, Орловская область, Республика Башкортостан, Республика Бурятия, Республика Дагестан, Республика Ингушетия, Республика Калмыкия, Республика Карелия, Республика Коми, Республика Крым, Республика Марий Эл, Республика Мордовия, Республика Татарстан, Республика Тыва, Республика Хакасия, Смоленская область, Томская область, Удмуртская Республика, Ханты-Мансийский автономный округ – Югра, Челябинская область, Ямало-Ненецкий автономный округ, Ярославская область).

Эмпирическую базу исследования также составили результаты анкетирования 560 сотрудников органов дознания, следствия и оперативных подразделений по вопросам использования программных технико-криминалистических средств и криминалистических характеристик при расследовании преступлений в сфере компьютерной информации (Приложение 1).

Научная новизна диссертации определяется концептуально новыми знаниями об объекте исследования, которые позволили определить направления совершенствования практики расследования преступлений, совершаемых в сфере компьютерной информации, выявить их эволюционные особенности, обеспечив противодействие потенциально новым формам преступлений рассматриваемого вида в динамике, а также сформулировать теоретические положения и основополагающие закономерности, принципы реализации и внедрения новой криминалистической концепции расследования преступлений в сфере компьютерной информации в научно-исследовательскую, образовательную и практическую деятельность.

В диссертационном исследовании решена научная проблема, заключающаяся в формировании нового подхода к расследованию одних из наиболее распространенных в настоящее время преступных деяний, наносящих существенный вред как отдельным гражданам государства, так и экономике, объектам критической информационной инфраструктуры и смежным отраслям промышленности страны в целом. В работе изложены новые научно обоснованные решения, внедрение которых может внести значительный вклад в развитие науки криминалистики: приведены результаты экстраполяции имеющихся научных знаний и междисциплинарного синтеза, использованы достижения ряда смежных наук в целях формирования новых криминалистических методов и средств, используемых в расследовании преступлений в сфере компьютерной информации.

Наиболее значимые результаты исследования, отвечающие критерию научной новизны, заключаются **в положениях, выносимых на защиту.**

1. Соответствующие текущему уровню развития информационных технологий криминалистические характеристики преступлений в сфере компьютерной информации, по которым в настоящее время имеется судебно-следственная практика, сформированные с точки зрения системно-структурного, а также кибернетического подходов, позволяющие заложить основу информационной модели (цифрового двойника) преступных деяний в целях выявления зависимостей между элементами криминалистической характеристики и объективных закономерностей для оптимизации дальнейшего расследования.

2. Классификация применяемых при расследовании преступлений в сфере компьютерной информации технико-криминалистических средств, включающих в себя широкий круг аппаратных, программно-аппаратных и программных средств, структурированных по различным основаниям (криминалистическим и правовым, по сфере применения, доказательственному значению, правовой регламентации и функциональной направленности) и позволяющих наиболее эффективно обеспечить обнаружение, фиксацию, изъятие, исследование и сохранность цифровых доказательств, а также целостность следовой картины, точность и воспроизводимость результатов анализа криминалистически значимой компьютерной информации.

3. Совокупность факторов, определяющих значимость применения программных средств при расследовании преступлений в сфере компьютерной информации, заключающихся в возможности непосредственного обнаружения, фиксации, изъятия и исследования цифровых доказательств (за счет использования экспертных и поисковых систем), их верификации, проверки подлинности и сохранности, восстановления удаленных и зашифрованных данных (за счет применения методов цифровой стеганографии или интеграции блокчейн-технологий), удобстве и оперативности обработки больших массивов данных (за счет использования технологий машинного обучения и распределенного хранения данных), выдаче прогнозов и рекомендаций (на базе предиктивного анализа и корреляции данных).

4. Система принципов, позволяющих повысить эффективность расследования преступлений в сфере компьютерной информации, обеспечить юридическую и техническую состоятельность цифровых доказательств (принцип хронологической документации (обеспечивающий фиксацию всех этапов работы с цифровыми доказательствами, предотвращение утраты сведений путем организации центров обработки данных на основе распределенных баз и облачных массивов), принцип независимых дисковых данных (с возможностью расчета контрольных сумм и контроля версий хранилищ данных) и принцип реализации защиты цифровых данных от посягательств (на основе использования алгоритмов шифрования с временными метками и внедрения блокчейн-технологий)).

5. Направления совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации, которые заключаются в подробной регламентации и алгоритмизации процесса собирания, хранения и использования цифровых доказательств, введении национальных стандартов по их фиксации и анализу, развитии систем сертификации специалистов, задействованных в расследовании рассматриваемых преступных деяний, расширении перечня используемых ими программных средств (в том числе реализованных на базе технологий искусственного интеллекта и анализа больших данных), развитии облачных платформ для безопасного и неизменного хранения цифровых доказательств с применением распределенных реестров, создании единого кластера данных с возможностью оперативного

доступа к цифровым доказательствам, а также поиска и обработки криминалистически значимой информации с использованием ключевых слов и фильтров в едином сегменте сети.

6. Структура частной криминалистической методики расследования преступлений в сфере компьютерной информации (закладываемая в основу информационно-компьютерной модели (цифрового двойника) рассматриваемого преступления) с возможностью выдачи наиболее эффективного алгоритма расследования преступного деяния и вероятности его раскрытия), включающая обстоятельства, подлежащие установлению при расследовании (установление признаков определенного состава преступления, обстоятельств, подлежащих доказыванию, и иных обстоятельств, выяснение которых требуется при расследовании преступлений данного вида), криминалистическую характеристику преступлений (как научную абстракцию, содержащую в себе общие черты, свойственные криминалистическим характеристикам рассматриваемой группы преступлений), а также криминалистическую характеристику расследования преступления (в виде алгоритмической системы обобщенных сведений, раскрывающих основные закономерные черты механизма расследования преступлений по различным следственным ситуациям).

7. Авторская позиция о трансформации описательной формы изложения классических рекомендаций по расследованию преступлений в сфере компьютерной информации в интеллектуальные (недетерминированные, вариативные, самообучающиеся) алгоритмы машинного обучения, определяющая новый подход к развитию частной криминалистической методики расследования преступлений и заключающаяся в возможности формирования цифрового двойника преступного деяния, примером которого может служить цифровой двойник преступления в сфере компьютерной информации.

8. Универсальная система криминалистического кодирования преступлений в сфере компьютерной информации, позволяющая заложить основу их стандартизированного учета и классификации, присвоения им уникальных кодов для формирования информационной модели преступного деяния, а также способствующая учету многообразия способов и средств совершения преступлений в сфере компьютерной информации (в том числе в условиях их

эволюции), выдвижению унифицированной методики их расследования и устранению сложности обработки больших объемов цифровых данных, нашедшая свое отражение в программном технико-криминалистическом средстве «КиберКодекс [CyberCodex] с кодификатором преступлений в сфере компьютерной информации».

9. Авторская позиция о возможности восполнения дефицита исходной информации на начальной стадии досудебного расследования путем использования массивов сведений, содержащихся в информационной модели преступления, аналогичного расследуемому и заключение о том, что алгоритм построения плана расследования сводится к рассмотрению конкретной сложившейся ситуации, подбору типовой информационной модели преступления, максимально схожей с условиями сложившейся ситуации, на базе которых выдвигается рабочая версия и составляется план расследования.

10. Общий для преступлений в сфере компьютерной информации алгоритм их расследования с учетом вида и особенностей конкретного преступления, классификации способов совершения рассматриваемого преступления (по объекту воздействия, по доступу к объекту воздействия, уровню автоматизации и мотиву действий) и соответствующих методик его расследования.

11. Авторское заключение о допустимости получения объяснений по факту совершения преступления в удаленном формате (в качестве альтернативной возможности) и возможности их представления по специально разработанной форме, реализованной в виде информационной системы (веб-ресурса) на основе искусственного интеллекта, что позволит снизить временные затраты на процесс подачи заявления о преступном деянии, автоматизировать процесс обработки криминалистически значимой информации и послужит отправной точкой алгоритмизации процесса расследования рассматриваемых преступных деяний и процесса поддержки принятия решений по уголовному делу должностным лицом.

12. Сформулированное учение об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности (предмет и объект учения, объективные закономерности, определяющие его), концептуальная основа которого развивает отдельные положения частной криминалистической теории информационно-

компьютерного обеспечения криминалистической деятельности в части применения интеллектуальных систем для выявления, моделирования, интерпретации и верификации цифровых следов преступной деятельности в современных условиях, а также прогнозирования возможности расследования преступного деяния, формирования рекомендаций по выбору наиболее эффективной методики расследования.

13. Концепция систематизации криминалистически значимой компьютерной информации в целях формирования кластера обучающих данных для интеллектуального программного технико-криминалистического средства с возможностью гибкой настройки и выдачи отчетов по интересующим следствием направлениям, а также структура интегрированной системы учета цифровых доказательств по преступлениям в сфере компьютерной информации, элементами которой выступили подсистемы: сбора и агрегации данных; классификации и структурирования криминалистически значимой информации; анализа, оценки и хранения данных; генерации отчетов и визуализации информации.

14. Цифровой двойник преступного деяния (представляющий собой разработанную автором виртуальную модель, отражающую состояние и динамику реального преступления в сфере компьютерной информации и позволяющую исследовать различные сценарии его совершения, выявлять закономерности между элементами его криминалистической характеристики), нашедший свое отражение в интеллектуальном программном технико-криминалистическом средстве «Cybercrime DT Model (AI) – [Цифровой двойник киберпреступления]», обеспечивающем на основе введенных пользователем данных о совершенном преступлении формирование наиболее соответствующего ему алгоритма расследования и определение вероятности раскрытия смоделированного преступления с интерпретацией принимаемых моделью решений.

15. Выявленные на основе статистического анализа категориальных данных (данных, описывающих принадлежность характерных признаков определенному виду преступного деяния) элементы криминалистической характеристики преступлений в сфере компьютерной информации, в наибольшей степени влияющие на вероятность их раскрытия.

16. Сформированные на основе материалов судебно-следственной практики корреляционные матрицы по элементам криминалистической характеристики преступлений в сфере компьютерной информации, использование которых возможно для анализа больших массивов криминалистически значимой компьютерной информации, отбора значимых в них признаков, выявления и визуализации скрытых закономерностей в цифровых данных.

17. Графическое представление связей между совокупностью разрозненных преступлений в сфере компьютерной информации (графовая криминалистическая модель данных), которое позволило выявить признаки и закономерности, связанные с их раскрытием, в том или ином отдельном кластере криминалистических данных, а также показать особенности расследования отдельных видов преступных деяний, совершенных в сфере компьютерной информации.

Теоретическая значимость исследования определяется разработкой криминалистической концепции, в основе которой лежит принципиально новый мультидисциплинарный подход к расследованию преступлений в сфере компьютерной информации на базе унифицированных алгоритмов, обученных на множестве аналогичных ситуаций (обстоятельств). В рамках предложенной концепции сформулированы ее теоретические положения, определены задачи и место в системе науки криминалистики, подробно рассмотрены ее структура, а также основополагающие закономерности, принципы реализации, функционирования и ее внедрения. Предлагаемый подход представляет собой перспективное и неотъемлемое направление развития теории и практики криминалистики, направленное на углубление и расширение знаний по вопросам расследования преступлений в сфере компьютерной информации, способствуя разрешению их проблемных положений.

Практическая значимость исследования заключается в сформулированных предложениях по совершенствованию деятельности правоохранительных органов в области расследования преступлений в сфере компьютерной информации. Обоснован вывод о необходимости расследования таких преступлений с задействованием программных технико-криминалистических средств, реализуемых на основе искусственного интеллекта, что положительно отразится на эффективности расследования преступлений рассматриваемого вида.

Изложенные в диссертации выводы и рекомендации могут быть использованы в образовательном процессе высших учебных заведений юридического и, отчасти, технического профиля при изучении таких дисциплин как «Криминалистика», «Компьютерная криминалистика», «Расследование киберпреступлений», «Расследование преступлений в сфере компьютерной информации», «Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации», «Практикум по проведению отдельных следственных действий по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий», «Информационные технологии в правоохранительной деятельности», «Анализ и интерпретация данных» и пр. Предлагаемая концепция также может использоваться как методика преподавания цикла специальных дисциплин криминалистического профиля, при подготовке методических и иных материалов, а также в целях повышения квалификации сотрудников, задействованных в раскрытии и расследовании преступлений в сфере компьютерной информации.

Достоверность полученных результатов исследования обеспечена: применением апробированных методов и методик проведения диссертационных исследований; соблюдением научных требований в области криминалистики, их фундаментальных методов и принципов, а также применением новых информационных технологий в раскрытии и расследовании преступлений; междисциплинарным подходом исследования; тщательным отбором эмпирического материала и репрезентативной базой статистических данных; обобщением практического опыта правоохранительных органов и материалов судебно-следственной практики; опытом практической реализации полученных результатов исследований, их апробацией, валидацией и государственной регистрацией; соответствием результатов исследования с экспериментальными данными; использованием в диссертационном исследовании научных работ общепризнанных отечественных и зарубежных ученых в области криминалистики и уголовно-процессуального права.

Апробация и внедрение результатов исследования. Результаты исследований и текст диссертации обсуждены на кафедре криминалистики Института права Уфимского университета науки и технологий. Ряд предложений и рекомендаций, сформулированных в результате проведенного исследования, внедрены в образовательный процесс по дисциплинам «Криминалистика», «Расследование киберпреступлений», «Расследование преступлений в сфере компьютерной информации», «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий», «Цифровые следы преступлений против личности», преподаваемым в Институте права Уфимского университета науки и технологий, Уфимском юридическом институте МВД России и Московской академии Следственного комитета имени А. Я. Сухарева.

Разработанные в рамках исследования программные технико-криминалистические средства внедрены в практическую деятельность Главного следственного управления МВД по Республике Башкортостан, а также отдела компьютерных, фоноскопических и лингвистических экспертиз Экспертно-криминалистического центра Главного управления МВД России по Саратовской области. Отдельные положения диссертационного исследования внедрены в научно-исследовательскую деятельность Уфимского юридического института МВД России.

Ряд положений были использованы в выступлениях и докладах перед действующими сотрудниками правоохранительных органов, задействованными в области расследования преступлений в сфере компьютерной информации, в том числе в рамках образовательного проекта МВД России «Научный лекторий». Отдельные положения применялись при подготовке методических материалов для курсантов, слушателей и профессорско-преподавательского состава Уфимского юридического института МВД России, студентов Уфимского университета науки и технологий, сотрудников Главного следственного управления МВД по Республике Башкортостан.

Часть результатов диссертационного исследования были получены в рамках реализации проекта «Центр противодействия ИТ-преступности «КиберПолигон» на всероссийском грантовом конкурсе, проводимом в 2024–2025 г.г.

Разработанный в рамках исследования программно-аналитический комплекс «Киберпреступность»⁸ в 2022 году был признан положительным опытом, связанным с образовательным процессом в системе МВД России, зарегистрированное программное технико-криминалистическое средство «BIOSCAN – Интеллектуальная система распознавания биометрических данных на основе машинного обучения (ML), компьютерного зрения (CV) и искусственного интеллекта (AI)»⁹ в 2024 году было признано положительным опытом деятельности на уровне МВД России¹⁰.

Теоретические основы и прикладные положения диссертационного исследования докладывались и представлялись на международных, всероссийских, региональных, ведомственных, межвузовских конференциях, семинарах и круглых столах: «Правовое обеспечение развития социального государства в свете целей устойчивого развития» (г. Уфа, 2018 год); «Актуальные проблемы права и государства в XXI веке» (г. Уфа, 2019 год); «Использование современных цифровых технологий в деятельности силовых ведомств» (г. Уфа, 2019 год); «Актуальные вопросы изучения технологий использования криптовалют в противоправных целях: российский и зарубежный опыт» (г. Уфа, 2019 год); «Организация Объединенных Наций и глобальные проблемы человечества в XXI веке» (г. Уфа, 2019 год); «Information Technologies for Intelligent Decision Making Support» (г. Ставрополь, 2020 год); «Актуальные проблемы деятельности органов внутренних дел по обеспечению безопасности лиц, подлежащих государственной защите» (г. Уфа, 2020 год); «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (г. Уфа, 2020 год); «Общественная безопасность, законность и правопорядок в III тысячелетии»

⁸ Свидетельство о государственной регистрации программы для ЭВМ № 2020661720 Российская Федерация. Программно-аналитический комплекс «КиберПреступность» : № 2020660996 : заявл. 23.09.2020 : опубли. 30.09.2020.

⁹ Свидетельство о государственной регистрации программы для ЭВМ № 2023667481 Российская Федерация. BIOSCAN – Интеллектуальная система распознавания биометрических данных на основе машинного обучения (ML), компьютерного зрения (CV) и искусственного интеллекта (AI) : № 2023666662 : заявл. 08.08.2023 : опубли. 15.08.2023.

¹⁰ Инновационные образовательные технологии и методики в образовательных организациях МВД России // Информационный бюллетень Федерального государственного казенного образовательного учреждения высшего образования «Московский университет Министерства внутренних дел Российской Федерации им. В. Я. Кикотя». 2024. С. 128.

(г. Воронеж, 2020 год); «Современные цифровые технологии в деятельности образовательных организаций силовых ведомств: концепция, практика, инновации» (г. Уфа, 2020 год); «Теория и практика расследования преступлений» (г. Краснодар, 2020 год); «Современные проблемы уголовного процесса: пути решения» (г. Уфа, 2020 год); «Актуальные проблемы кибербезопасности в сети Интернет» (г. Москва, 2020 год); «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (Ставрополь, 2020 год); «Современная наука: актуальные проблемы, достижения и инновации» (г. Белебей, 2021 год), «Fundamental information security problems in terms of the digital transformation» (г. Ставрополь, 2021), «Теория и практика расследования преступлений» (г. Краснодар, 2022 год); «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации» (г. Екатеринбург, 2022 год); «Международные и национальные тенденции: перспективы развития судебной экспертизы» (г. Казань, 2022 год); «Innovative technologies in criminalism» (г. Караганда, 2022 год); «Актуальные проблемы раскрытия и расследования преступлений» (г. Екатеринбург, 2023 год); «Международная научная конференция по междисциплинарным исследованиям» (г. Екатеринбург, 2023 год); «Актуальные проблемы борьбы с преступлениями, связанные с криптовалютой» (г. Улан-Батор, 2023 год); «Актуальные вопросы права в условиях цифровизации общества» (г. Сочи, 2023 год); «Криминалистика: актуальные вопросы теории и практики» (г. Ростов-на-Дону, 2023 год); «Современное образование: традиции и инновации» (г. Волгоград, 2023 год); «Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений» (г. Воронеж, 2024 год); «Актуальные вопросы противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий» (г. Уфа, 2024 год); «Цифровые системы и модели: теория и практика проектирования, разработки и применения» (г. Казань, 2024 год); «Высокотехнологичное право: ожидание и реальность» (г. Москва, 2025 год); «Актуальные проблемы правового регулирования, организации и тактики производства следственных действий» (г. Омск, 2025 год); «Актуальные проблемы расследования преступлений,

совершенных в сфере информационно-телекоммуникационных технологий в современных условиях» (г. Волгоград, 2025 год); «Цифровая криминалистика '25» (г. Уфа, 2025 год); «Искусственный интеллект и правоприменение: перспективы и вызовы» (г. Уфа, 2025); «Актуальные вопросы расследования преступлений в условиях развития цифровых технологий» (г. Уфа, 2025 год); «Криминалистика: вчера, сегодня завтра» (г. Москва, 2025 год); «Актуальные проблемы использования специальных знаний в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях» (г. Уфа, 2025 год).

Содержание диссертационного исследования нашло отражение в 82 научных работах. Среди них: 11 учебных изданий, 59 статей, включающие 18 работ, опубликованных в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации, и 2 работы, индексируемые в международной наукометрической базе данных (Web of Science), а также 12 свидетельств о государственной регистрации программ для ЭВМ.

Структура диссертации обусловлена объектом, предметом, целью, задачами и результатами исследования. Работа состоит из введения, пяти глав, объединяющих четырнадцать параграфов, заключения, списка литературы и приложений.

ГЛАВА 1. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ И МОДЕЛИРОВАНИЯ, ФАКТОРЫ ИХ ЭВОЛЮЦИИ И ТРАНСФОРМАЦИИ

1.1. Преступления в сфере компьютерной информации как объект криминалистического исследования

Информационные технологии, как фундаментальный элемент построения глобального цифрового сообщества, служат неотъемлемым инструментом мирового развития во всей совокупности его социальных, экономических, политических, научных, интеллектуальных и иных аспектов. В рамках проведения мониторинга развития информационного общества, формирования индексов и рейтингов по уровню развития информационно-телекоммуникационных технологий в Российской Федерации, обеспечения мониторинга процесса реализации целей в области устойчивого развития Организации Объединенных Наций¹¹ и реализации выборочного федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей¹² ежегодно осуществляется расчет показателей, характеризующих использование населением персональных компьютеров, мобильных телефонов и сети «Интернет», наличие в домохозяйствах информационных технологий и информационно-телекоммуникационных сетей, использование средств защиты информации и сети «Интернет» для заказов товаров (услуг), получение государственных услуг в электронной форме, а также определение влияния информационных технологий и информационно-телекоммуникационных сетей на жизнь людей и т.п.

Сформированные Федеральной службой государственной статистики данные¹³ позволяют выявить практически ежегодный прирост числа использования

¹¹ Цели в области устойчивого развития (sustainable development goals) // Организация объединенных наций : офиц. сайт. URL: <https://www.un.org/sustainabledevelopment/ru/sustainable-development-goals> (дата обращения: 22.10.2025).

¹² Выборочное федеральное статистическое наблюдение по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей // Федеральная служба государственной статистики : офиц. сайт. URL: https://rosstat.gov.ru/free_doc/new_site/business/it/ikt23/index.html (дата обращения: 22.10.2025).

¹³ Мониторинг развития информационного общества в Российской Федерации // Федеральная служба государственной статистики : офиц. сайт. URL: <https://rosstat.gov.ru/storage/mediabank/monitor.xlsx> (дата обращения: 22.10.2025).

технических устройств (в пересчете на 100 домохозяйств), доли населения, характеризующейся активным использованием сети «Интернет» и имеющей широкополосный доступ к ней, а также общей численности населения, использующей информационно-телекоммуникационную сеть для заказа товаров, услуг и пр. (Приложение 2).

В 2024 году по всему миру зарегистрировано 5,5 млрд человек, использующих сеть «Интернет» (равно как и технические устройства для выхода в информационно-телекоммуникационную сеть), что составляет 68 % населения мира по сравнению с 65 %, рассчитанными годом ранее¹⁴ (Приложение 3). В соответствии с Концепцией государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-телекоммуникационных технологий в Российской Федерации по состоянию на 2024 год активными пользователями информационно-телекоммуникационной сети «Интернет» являлись около 90 % населения страны (130 млн. чел), что обусловлено широким распространением электронных средств массовой информации, информационных систем, социальных сетей, финансовых инструментов, электронных средств платежа, а также системы предоставления государственных услуг в электронной форме.

Несомненна польза развития и внедрения информационно-телекоммуникационных технологий со всеми реализованными на их основе за последнее десятилетие технологическими возможностями, однако в условиях роста пользования техническими средствами и увеличения проникновения информационных технологий в повседневную жизнь населения число противоправных деяний, связанных с ними, пропорционально возрастает¹⁵. В комплексном анализе состояния преступности в Российской Федерации, проводимом Всероссийским научно-исследовательским институтом МВД России, и ежегодном анализе статистических сведений о состоянии преступности Главного информационно-аналитического центра МВД России отмечается стабильный рост количества преступлений, совершаемых в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий (+ 29,7 % в 2023 году по сравнению с 2022 годом, + 13,1 % в 2024 году по сравнению с 2023

¹⁴ Глобальное число пользователей сети «Интернет» // Международный союз электросвязи МСЭ (ITU) : офиц. сайт. URL: <https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use> (дата обращения: 08.02.2025).

¹⁵ Глобальный отчет по цифровым технологиям по состоянию на октябрь 2024 года // Международный статистический сервис «Datareportal» : офиц. сайт. URL: <https://datareportal.com/reports/digital-2024-october-global-statshot> (дата обращения: 08.02.2025).

годом¹⁶ (Приложение 4)), а также рост доли такого рода преступлений в общей структуре преступности по итогам 2024 года до 40 %, 60 % от общего количества которых являются латентными. В связи с этим, целесообразно рассмотрение понятия преступления в сфере компьютерной информации как базового элемента частной криминалистической методики расследования.

Понятийный аппарат, применяемый в области информационных технологий, определяется множеством нормативных правовых актов, среди которых основополагающее значение имеют Федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 07 июля 2003 г. № 126-ФЗ «О связи», от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», от 26 июля 2016 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», от 01 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации», а также ряд Указов Президента Российской Федерации, государственных и международных стандартов в области цифровых технологий, информационной безопасности и защиты информации.

Для обеспечения дальнейшего удобства в пользовании терминологией, а также с целью устранения возможных противоречий необходимо систематизировать понятийный аппарат в рассматриваемой сфере. Понятие, являясь основной структурной единицей мышления¹⁷, представляет собой целостную совокупность суждений об отличительных признаках исследуемого объекта. Преступление с точки зрения криминалистической теории – это обусловленная субъективными и объективными факторами система, которая состоит из совокупности взаимосвязанных между собой элементов, образующих

¹⁶ Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития : аналитический обзор / Федеральное государственное казенное учреждение «Всероссийский научно-исследовательский институт Министерства внутренних дел Российской Федерации» / М. В. Гончарова, М. М. Бабаев, Р.В. Черкасов [и др.]. М. : ФГКУ «ВНИИ МВД России», 2025. С. 54.

¹⁷ Петровская В. Н., Щепин В. И. Концепции современного естествознания : словарь терминов. Иркутск : Изд-во ИрГТУ, 2008. С. 58.

общественно опасное явление, предотвращение которого возможно под угрозой¹⁸.

Преступления в сфере компьютерной информации – это законодательное определение преступлений, предусмотренных главой 28 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ¹⁹ (далее – УК РФ), объединяющей статьи, связанные с: неправомерным доступом к компьютерной информации (ст. 272 УК РФ); незаконным использованием и (или) передачей, сбором и (или) хранением компьютерной информации, содержащей персональные данные, созданием и (или) обеспечением функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения (ст. 272.1 УК РФ); созданием, использованием и распространением вредоносных компьютерных программ (ст. 273 УК РФ); нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ); несоблюдением порядка централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ); незаконным использованием абонентского терминала пропуска трафика или виртуальной телефонной станции (ст. 274.3 УК РФ); организацией деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации (ст. 274.4 УК РФ) и информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям информационных систем (ст. 274.5 УК РФ)²⁰.

Преступления в сфере компьютерной информации тесно связаны со множеством других видов преступлений, поскольку часто выступают способом совершения таких уголовных деяний как кража, вымогательство, незаконный

¹⁸ Курс криминалистики : сборник научных трудов в 3 томах / под ред. О. Н. Коршуновой. Т. 1 : Общая теория криминалистики. Криминалистическая техника. Криминалистическая тактика. М. : Юридический центр, 2024. С. 57.

¹⁹ Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ : в ред. от 17 ноября 2025 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_10699 (дата обращения: 17.11.2025).

²⁰ О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 31 июля 2025 г. № 282-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_34481/a8ce863fe783cf2bec75f4f1de3e5ffb7b4cc043/ (дата обращения: 26.08.2025).

оборот наркотических и психотропных веществ, экстремизм²¹, терроризм²² и пр. В соответствии с перечнем преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации (перечень 25), утвержденным указанием Генеральной прокуратуры Российской Федерации № 503/11 и МВД России № 1 от 28 июля 2025 г.²³, имеется часть схожих с рассматриваемыми преступлениями форм девиантного поведения, криминализированных в российском уголовном праве, однако, в настоящем исследовании будут рассматриваться только деяния, относящиеся к предмету преступлений, предусмотренных главой 28 УК РФ.

Для решения задач обработки информации и других функциональных задач (сбор, хранение и пр.) используются совокупности взаимосвязанных средств вычислительной техники, составляющие компьютерные системы. Под вычислительной техникой подразумевается совокупность технических средств, методов и приемов, используемых для автоматических и автоматизированных процессов вычислений и обработки информации²⁴. Под средством вычислительной техники понимают, как правило, совокупность технических устройств и программное обеспечение, а под техническими средствами понимается совокупность технических устройств средств вычислительной техники либо их частей (в виде аппаратного устройства)²⁵. В соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» под информационными технологиями в работе будут подразумеваться процессы и методы поиска, сбора, хранения, обработки, предоставления, распространения

²¹ Волчецкая Т. С., Авакьян М. В. Прикладные аспекты противодействия информационно-мировоззренческим угрозам в цифровом пространстве и особенности их профилактики // Актуальные проблемы российского права. 2021. Т. 16. № 6 (127). С. 196.

²² Кибербезопасность и новые технологии. Руководство для персонала оперативного реагирования по изъятию цифровых устройств // Контртеррористическое управление Организации Объединенных Наций : офиц. сайт. URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/guide_for_first_responders_on_the_collection_of_digital_devices_in_the_battlefield_finalout_web_ru.pdf (дата обращения: 08.02.2025).

²³ О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генеральной прокуратуры Российской Федерации от 28 июля 2025 г. № 503/11, МВД России № 1 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_517620/251f7ac207ca304c6331640eb36b162351c24684 (дата обращения: 26.08.2025).

²⁴ ГОСТ Р 71223–2024. Вычислительная техника. Термины и определения; дата введения: 01 июня 2025 г. М. : Российский институт стандартизации, 2025. С. 6.

²⁵ ГОСТ Р 57429–2017. Национальный стандарт Российской Федерации. Судебная компьютерно-техническая экспертиза. Термины и определения; дата введения: 28 марта 2017 г. М. : Стандартинформ, 2018. С. 1.

информации и способы осуществления таких процессов и методов, под информационно-телекоммуникационными сетями – системы, предназначенные для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, под информационными системами – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств²⁶.

Под компьютерной информацией понимаются сведения в виде сообщений либо данных, представленных в форме электрических сигналов, вне зависимости от средств их хранения, обработки и передачи. Компьютерная информация не может существовать вне запоминающего устройства²⁷, совокупность ячеек которого обеспечивает хранение данных и определяется как электронный носитель информации²⁸. Именно электронный носитель информации, равно как съемный машинный носитель информации, зачастую выступает в качестве основного вещественного доказательства²⁹ по преступлениям в сфере компьютерной информации.

Под цифровой информацией понимают совокупность данных, отображаемых в цифровой форме, пригодных для дальнейшего хранения, обработки или передачи с помощью технических средств и информационных систем, и существующих в виде файлов, сетевых пакетов, реестров или метаданных³⁰. Определение «цифровая информация» фокусируется на всех видах цифровых данных, включая те, что существуют вне компьютерных систем (например, на машинных носителях информации), и является более широким в сравнении с понятием «компьютерная информация», определяющим данные, которые создаются, обрабатываются или хранятся в рамках компьютерных систем, хотя в подавляющем большинстве оба

²⁶ Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_61798 (дата обращения: 22.10.2025).

²⁷ Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, З. И. Харисова, В. Р. Гайнельзянова. М. : ГУРЛС МВД России, 2024. С. 6.

²⁸ ГОСТ Р 70942–2023. Устройства цифровых вычислительных машин запоминающие. Термины и определения; дата введения: 12 октября 2023 г. М. : Российский институт стандартизации, 2023. С. 5.

²⁹ Агафонов В. В. Вазюлин С. А., Васюков В. Ф. Особенности формирования доказательств с использованием информации о соединениях между абонентами и (или) абонентскими устройствами: криминалистические и процессуальные аспекты : монография. М. : Юрлитинформ, 2015. С. 93.

³⁰ Цифровая криминалистика : учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. М. : Юрайт, 2025. С. 84.

термина повсеместно применяются синонимично³¹.

Общими криминалистическими признаками компьютерной информации могут являться:

- принадлежность к одной из объективных форм существования информации, в частности, к электронной форме;
- опосредованность через электронный носитель информации;
- доступность в единообразном виде одновременно для нескольких пользователей;
- возможность ее преобразования в электронном виде;
- доступность копирования на различные виды электронных носителей информации с возможностью дальнейшей передачи на расстоянии³²;
- сбор, обработка и ее анализ осуществим только при помощи электронных технических средств, информационных систем, программного обеспечения, баз данных, носителей информации и пр.

Рассмотрим классификацию компьютерной информации по различным основаниям.

Так, по юридическому положению различают³³:

- недокументированную информацию (данные, образующиеся и (или) используемые в процессе обработки информации, но не обладающие признаками документа, например, сетевой адрес, доменное имя, данные авторизации для входа в систему и пр.);
- документированную информацию (зафиксированные на носителе информации данные с реквизитами, позволяющими определить такую информацию, или, в установленных законодательством Российской Федерации случаях, ее материальный носитель).

Компьютерная информация и средство вычислительной техники могут одновременно выступать предметом преступного посяательства³⁴, средством совершения преступления либо источником информации о преступном деянии.

³¹ Воронков Д. В. О соотношении традиционной криминалистики и цифровой криминалистики // *Baikal Research Journal*. 2025. № 16 (1). С. 73.

³² Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие / под ред. С. В. Зуева, В. Б. Вехова. М. : Юрайт, 2025. С. 16.

³³ Вехов В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // *Уголовное право*. 2004. № 4. С. 17.

³⁴ Попов А. Н. Преступления в сфере компьютерной информации : учебное пособие. Санкт-Петербург : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. С. 23.

При этом в уголовном судопроизводстве компьютерная информация рассматривается как вещественное доказательство или иной документ в соответствии со ст. ст. 81 и 84 Уголовно-процессуального кодекса Российской Федерации от 18 декабря 2001 года № 174-ФЗ (далее – УПК РФ) соответственно³⁵. Кроме того, при определенных условиях средство вычислительной техники также может быть признано вещественным доказательством.

Под правовым режимом информации понимают нормативно установленные правила, которые определяют степень открытости, правила доступа, хранения, распространения и защиты информации, которая может являться объектом публичных, гражданских и иных правовых отношений.

По доступности третьим лицам подразделяют:

- информацию, находящуюся в общем доступе (общедоступная информация);
- информацию ограниченного доступа (сведения, доступ к которым ограничен федеральными законами, составляющие, например, государственную, служебную, нотариальную, коммерческую, банковскую тайну и др. виды) в соответствии со ст. 5 Федерального закона «Об информации, информационных технологиях и о защите информации».

По форме представления компьютерная информация может выступать в виде:

- файла (поименованной области записей на электронном носителе, где в закодированном виде хранится строго определенная информация с реквизитами, позволяющими ее идентифицировать);
- сетевого адреса (идентификатора в сети передачи данных, определяющего при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационно-телекоммуникационную сеть, например, IP-адрес (от англ. «internet protocol» – протокол передачи данных в сети «Интернет») в виде идентификатора компьютера, работающего в сети «Интернет») или доменного имени DNS (от англ. «domain name system» – система доменных имен), предназначенного для адресации сайтов в сети «Интернет» (во взаимосвязи с IP-адресом ресурса) в целях обеспечения доступа к информации, размещенной в

³⁵ Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18 декабря 2001 г. № 174-ФЗ : в ред. от 27 октября 2025 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_34481 (дата обращения: 17.11.2025).

этой сети³⁶);

- информационной системы (совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств)³⁷;

- базы данных, являющейся составным элементом информационных систем, обеспечивающих систематизацию данных, их поиск и обработку с помощью компьютера;

- программного обеспечения для электронных вычислительных машин (компьютерной программы), представленной в форме совокупности данных и команд, предназначенных для функционирования технических устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе ее разработки и порождаемые ею аудиовизуальные отображения, либо компьютер целиком;

- электронного сообщения (информации, переданной или полученной пользователем компьютерной сети);

- электронной подписи (информации в электронной форме, которая «присоединена» к другой информации, находящейся в такой же форме (подписываемой информации), или иным образом связана с ней и которая используется для определения лица, подписывающего эту информацию (п. 1 ст. 2 Федерального закона «Об электронной подписи»))³⁸;

- электронных денежных средств, цифровых финансовых активов и пр.

Под цифровым (электронным) доказательством, в общем смысле, понимают любую информацию, обладающую доказательной силой и хранимой или передаваемой в цифровой форме³⁹.

Под киберпространством понимается обобщенное наименование упорядоченной по определенным протоколам автоматизированной обработки

³⁶ Расследование преступлений в сфере компьютерной информации и электронных средств платежа. Указ. соч. С. 19.

³⁷ ГОСТ Р 56545–2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей; дата введения: 01 апреля 2016 г. М. : Стандартиформ, 2015. С. 1; ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем; дата введения: 19 августа 2015 г. М. : Стандартиформ, 2015. С. 5.

³⁸ Об электронной подписи : Федеральный закон от 06 апреля 2011 г. № 63-ФЗ : в ред. от 28 декабря 2024 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_112701 (дата обращения: 22.10.2025).

³⁹ Практическое руководство по истребованию электронных доказательств // Управление Организации Объединенных Наций по наркотикам и преступлениям : офиц. сайт. URL: <https://sherloc.unodc.org/cld/ru/st/evidence/electronic-evidence.html> (дата обращения: 08.02.2025).

информации системы программных средств и файлов, расположенных в памяти электронных устройств либо электронной цифровой информации, находящейся в процессе передачи любым доступным способом, либо информации, распределенной в информационно-телекоммуникационной сети⁴⁰. Киберпространство по своей сути является уникальным носителем информации, не находящимся на конкретной территории определенного государства, но доступным каждому пользователю в любой точке мира посредством использования сети «Интернет». В рамках российского законодательства определение киберпреступления в явном виде отсутствует, однако указанный тип противоправных деяний часто синонимично рассматривается как преступления в сфере компьютерной информации (как составной элемент).

Стоит также отметить, что на международном уровне определение киберпреступности преимущественно зависит от цели использования этого термина, а за его основу берут круг деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных или информационных систем⁴¹. Кроме того, под киберпреступлением может пониматься нарушающее закон действие, которое совершается с использованием информационно-телекоммуникационных технологий и нацелено на информационно-телекоммуникационные сети, информационные системы, информационные ресурсы, веб-сайты и пр.⁴².

В узком значении под киберпреступлениями понимают только преступные деяния, совершаемые в виртуальном пространстве сети «Интернет» и посредством использования этой сети. При этом компьютеры или средства мобильной связи являются либо орудиями, либо предметами посягательств⁴³.

Проблема расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, стала значимым объектом исследований многих ученых, начиная с 70-х годов XX века, что потребовало

⁴⁰ Ефремова И. А., Смушкин А. Б., Донченко А. Б. Киберпространство как новая среда преступности // Вестник Томского государственного университета. 2021. № 472. С. 248; Мещеряков В. А. Теоретические основы механизма слеодообразования в цифровой криминалистике : монография. М. : Проспект, 2022. С. 55.

⁴¹ Всестороннее исследование проблемы киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступлениям : офиц. сайт. URL: https://www.unodc.org/documents/organized-crime/cybercrime/cybercrime_study_russian.pdf (дата обращения: 08.02.2025).

⁴² Понимание киберпреступности: явления, проблемы и правовой ответ // Международный союз электросвязи МСЭ (ITU) : офиц. сайт. URL: <https://www.itu.int/en/itu-d/cybersecurity/documents/cybercrime2014.pdf> (дата обращения: 08.02.2025).

⁴³ Чекунов И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. 2012. № 3. С. 182.

формирования принципиально новой нормативной базы, так, в 1998 году исследователем и консультантом в области информационной безопасности Д. Б. Паркером было обозначено, что компьютер является как объектом преступления, так и орудием, используемым для получения различных преимуществ⁴⁴.

Данный подход стал основой большинства последующих исследований, в ходе которых, независимо от обоснования применимости того или иного термина («киберпреступления», «преступления в сфере компьютерной информации», «преступления в сфере информационных технологий», «высокотехнологичные преступления», «компьютерные преступления», «интернет-преступления», «информационные компьютерные преступления», «преступления, относящиеся к компьютерам и сетям», «преступления, совершаемые с использованием информационно-телекоммуникационных технологий», «электронные преступления» и пр.), авторы исходят из особенностей подобных противоправных деяний в киберпространстве, как в рамках компьютерной сети.

Будапештской конвенцией Совета Европы ETS 185 (не ратифицирована РФ) все киберпреступления объединены в пять групп, связанных с: обеспечением конфиденциальности, целостности и доступности компьютерных данных и информационных систем; использованием компьютера; содержанием информации (контентом); нарушением авторских и смежных прав; использованием виртуального пространства для совершения актов насилия и иных противоправных деяний, посягающих на общественную безопасность⁴⁵.

В международной практике довольно распространен подход, когда любая противоправная деятельность, в которой компьютер, сеть компьютеров или сетевое устройство выступают объектом правонарушения, либо средством, используемым для совершения преступных действий, подпадает под сферу понимания киберпреступности⁴⁶, т. о. киберпреступность – это незаконные действия, в которых указанные технические средства в совокупности с использованием тех или иных информационных технологий являются либо объектом посягательства, либо средством совершения преступления, либо и тем и другим одновременно.

⁴⁴ Parker D. B. Computer crime: criminal justice resource manual. National institute of justice, 1989. P. 13.

⁴⁵ Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. (ETS № 185) // Совет Европы: офиц. сайт. URL: <https://www.europarl.europa.eu/meetdocs/20142019/documents/libe/dv/7convbudapest/7convbudapesten.pdf> (дата обращения: 22.10.2025).

⁴⁶ Chawki M., Darwish A., Khan S. Cybercrime, digital forensics and jurisdiction. Springer International Publishing. Switzerland, 2015. P. 19.

Однако в Российской Федерации чаще используется официальный подход, закрепленный главой 28 УК РФ, где данный вид преступлений определен через родовый объект как «преступления в сфере компьютерной информации»⁴⁷. Техническая составляющая рассматриваемых преступлений не сводится исключительно к применению компьютера как технического средства, поскольку компьютеры выступают лишь своего рода «орудием» либо физическим объектом воплощения виртуальной компьютерной системы, в которой хранится информация в виде объекта преступного посягательства.

В целом, рассматривая дефиницию «компьютерное преступление», стоит отметить, что ее использование нецелесообразно в уголовно-правовом, но возможно в криминалистическом аспекте, поскольку она связана не с квалификацией, а со способом преступления и, соответственно, с методикой его раскрытия и расследования⁴⁸. Помимо преступлений в сфере компьютерной информации Всероссийский научно-исследовательский институт МВД России к киберпреступлениям относит также перечень деяний, по которым квалифицирующим значением может являться средство совершения преступления⁴⁹, например, в виде использования сети «Интернет», компьютерной техники и вспомогательного компьютерного оборудования, мобильных устройств связи и т. п., например, по ст. ст.: 137 УК РФ (нарушение неприкосновенности частной жизни); 138 УК РФ (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений); 138.1 УК РФ (незаконный оборот специальных технических средств, предназначенных для негласного получения информации), 159.6 УК РФ (мошенничество в сфере компьютерной информации); 187 УК РФ (неправомерный оборот средств платежей) и пр.

Концепцией государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-телекоммуникационных технологий, рассматриваемые противоправные деяния с учетом критериев их квалификации классифицируются по трем основным типам: правонарушения и преступления в сфере компьютерной информации

⁴⁷ Старкова Л. М. Подходы к пониманию и нормативному определению категории «киберпреступность» и смежных понятий в практике региональных международных организаций // Московский журнал международного права. № 4. 2021. С. 130.

⁴⁸ Россинская Е. Р. Криминалистика. М. : Юр. Норма, НИЦ ИНФРА-М, 2025. С. 555.

⁴⁹ Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 года и ожидаемые тенденции ее развития : аналитический обзор. М. В. Гончарова, М. М. Бабаев, Р.В. Черкасов [и др.]. М. : ФГКУ «ВНИИ МВД России», 2024. С. 57.

(гл. 28 УК РФ); правонарушения и преступления, криминообразующим или квалифицирующим признаком которых является их совершение с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»; правонарушения и преступления, при совершении которых применение информационно-телекоммуникационных технологий является альтернативным способом.

Существенное увеличение количества преступлений, связанных с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), рост их доли в общем числе преступлений, совершаемых с использованием информационно-телекоммуникационных технологий⁵⁰, крайне низкая раскрываемость указанного вида преступных деяний, а также рост утечек конфиденциальных данных в результате данных преступных деяний, способный нанести существенный ущерб как отдельным гражданам государства, так и объектам критической информационной инфраструктуры РФ (ст. 274.1 УК РФ), оборонно-промышленного комплекса и смежных отраслей промышленности, говорит о том, что рассмотрение преступлений в сфере компьютерной информации является довольно актуальной задачей.

Негативное влияние на обстановку в сфере информационно-телекоммуникационных технологий также оказывает сложившаяся международная ситуация, связанная с деятельностью транснациональных организованных преступных групп, нацеленных на хищение персональных данных граждан Российской Федерации и их неправомерное использование и распространение (ст. 272.1 УК РФ).

Так, по итогам 2024 года отмечен двухкратный рост количества обнаруженных фишинговых веб-ресурсов, ресурсов с запрещенным контентом и скомпрометированными персональными данными граждан⁵¹. Отдельная проблема заключается в противоправном применении информационно-телекоммуникационных технологий организованными преступными группами, которые все чаще используют вредоносное программное обеспечение (ст. 273 УК РФ), фишинговые сайты, специальные технические средства, электронные платформы и колл-центры для совершения массовых телефонных

⁵⁰ Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. Указ. соч. С. 54.

⁵¹ Информационно-аналитический отчет «Результаты работы информационной системы «Антифишинг» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (ФГБУ «Научно-исследовательский институт «Интеграл») : офиц. сайт. URL: <https://digital.gov.ru/ru/ministry/departments/46> (дата обращения: 22.01.2025).

звонков. Довольно часто нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей приводит к тяжким последствиям или создает угрозу их наступления (ст. 274 УК РФ). Кроме того, существенными проблемами в настоящее время являются незаконное использование абонентских терминалов в виде GSM-шлюзов и SIM-боксов (от англ. «subscriber identity module box» – устройство для массового использования и хранения SIM-карт (от англ. «subscriber identity module» – модуль идентификации абонента в сотовой связи)), а также виртуальных телефонных станций (ст. 274.3 УК РФ), организация деятельности по незаконному обороту SIM-карт (ст. 274.4 УК РФ), аккаунтов и учетных данных (ст. 274.5 УК РФ). В связи с этим необходимо создание надежного механизма противодействия преступлениям именно в сфере компьютерной информации.

Интересен подход к определению преступлений, совершаемых с использованием новейших информационных технологий, которые можно определить как совокупность взаимосвязанных и образующих единство общественно опасных деяний, совершенных с использованием новейших информационных технологий (информационно-телекоммуникационных сетей или информационных систем), различных когнитивных, робототехнических, интеллектуальных средств и методов. Такое определение представляется вполне логичным и обоснованным в связи с широким распространением в настоящее время технологий распределенного реестра, квантовых вычислений, дополненной и виртуальной реальности, а также разработок в области искусственного интеллекта, Интернета вещей, облачных данных и пр.

С учетом вышеизложенного, наряду с официальным наименованием «преступления в сфере компьютерной информации», в ряде случаев можно синонимично употреблять термин «киберпреступление» (во-первых, как наиболее обоснованный и часто употребляемый (в том числе на международном уровне), во-вторых, определяемый наличием приставки «кибер», как указание на связь с наукой кибернетикой и, в-третьих, как составной элемент общей группы преступлений).

Отдельного внимания заслуживает понятие метaprостранства (метавселенной, метасреды), которая объединяет физическое пространство с цифровым и в общем своем понимании является закономерно последующим этапом развития киберпространства⁵², а также мощным инструментом для

⁵² Zhou Y., Tiwari M., Bernot A. Metacrime and cybercrime: exploring the convergence and divergence in digital criminality // Asian Journal of Criminology. 2024. V. 19. P. 420.

преобразования различных аспектов общественной жизни в цифровые. Метавселенная представляет собой онлайн-среду взаимосвязанных цифровых экосистем, созданных на базе виртуальных многопользовательских миров и технологий дополненной, виртуальной и расширенной реальностей, позволяющих осуществлять децентрализованное взаимодействие пользователей, представленных в виде аватаров⁵³, с различными цифровыми объектами и активами.

Поскольку информационные технологии с течением времени продолжают активно развиваться, метавселенная, отвечая потребностям общества, будет соответственно расширяться⁵⁴. В этой связи необходимо рассмотрение как особенностей неправомерного использования метасреды преступниками, так и возможностей ее использования в качестве инструмента для обеспечения правопорядка. Так, по прогнозу аналитической компании Gartner, в ближайшее время четверть населения будет находиться в метaprостранстве не менее одного часа в сутки⁵⁵.

Метапреступность, как эволюционная грань в спектре киберпространства, не только сохраняет все неотъемлемые сходства с киберпреступностью, но и открывает множество новых беспрецедентных преступных возможностей. Если традиционными объектами атак для киберпреступлений выступают цифровые данные, компьютеры, информационные системы, пользовательские учетные записи граждан или информационные ресурсы, то для метапреступлений объектами служат аватары (виртуальный представитель пользователя в метасреде), виртуальные личности, токены и активы. Таким образом, для киберпреступлений средой воздействия является традиционное интернет-пространство, веб-сайты, социальные сети, базы данных и т. п., для метапреступлений – это метавселенная в виде иммерсивного виртуального пространства с элементами дополненной реальности. Также стоит отметить, что существует проблема разграничения кибер- и метапреступлений, например, кража учетной записи пользователя в метавселенной может быть как киберпреступлением (кража данных), так и

⁵³ Cheong B. Avatars in the metaverse: potential legal issues and remedies // International cybersecurity law review. 2022. V. 3. P. 468.

⁵⁴ Метавселенная: точка зрения правоохранительных органов (примеры использования, преступления, криминалистика, расследования и управление). Указ. соч. С. 5.

⁵⁵ Метавселенная, особенности внедрения : аналитический отчет // Корпорация Гартнер (Gartner Inc.) : офиц. сайт. URL: <https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026> (дата обращения: 22.10.2025).

метапреступлением (использование аватара для мошенничества). Помимо указанных сред отдельного внимания заслуживают распределенные реестры (блокчейн), а также квантовые вычислительные среды. С учетом изложенного, целесообразно считать метапреступления, а также иные вариации преступных деяний, определяемые средой их совершения, эволюционным видом киберпреступлений, которые требуют адаптации существующих методик расследования и разработки принципиально новых подходов с учетом специфики новой среды. Так, на примере развития метасреды, несмотря на свой пока еще абстрактный и иммерсивный характер, уже на сегодняшний день можно выявить предположительные проблемы и угрозы, которые порождает эволюционное развитие киберпространства в метапространство, соответственно, сформировать рекомендации по их предотвращению. Не останавливаясь подробно на принципах функционирования каждой из сред стоит лишь отметить, что с ростом задействования новых цифровых «пространств» и числа вовлеченных в них участников возникает необходимость в определении вновь возникающих преступлений (угроз) в них. Международная организация уголовной полиции Интерпол несмотря на быструю смену тенденций преступных деяний в указанной сфере уже предложила базовую классификацию, согласно которой все метапреступления делятся на десять групп, охватывающих:

- терроризм (киберфизические атаки, финансирование терроризма, радикализация и идеологическое склонение);
- киберпреступления (неправомерный доступ в информационные системы или компьютер или к данным, кража данных, использование программ-вымогателей, доксинг (от англ. «doxing» – незаконный сбор и распространение личной информации без согласия человека) и пр.);
- преступления против детей (сексуальная эксплуатация и домогательство, эксплуатация детского труда);
- преступления против общественной безопасности (незаконный оборот и пропаганда наркотических средств, дезинформация);
- преступления против личности (взлом, кража личных данных, дипфейки (от англ. «deepfake» – как словообразование «deep learning» – «глубокое обучение» и «fake» – «подделка»), нарушение конфиденциальности и пр.);
- преступления против интеллектуальной собственности (нарушение авторских прав);
- преступные действия, направленные на то, чтобы вызвать страх или

эмоциональный стресс (вымогательство и шантаж, клевета, несогласованный обмен личными (интимными) изображениями, преследование, домогательство);

- сексуальные преступления и нападения (неприличное обнажение, эксплуатация, домогательство, злоупотребление доверием и пр.);

- имущественные преступления (повреждение имущества, ограбление аватара, виртуальное ограбление, кража виртуальной собственности и активов, несанкционированное проникновение в частное виртуальное пространство);

- финансовые преступления (фишинг, отмывание денег, налоговые преступления, мошенничество).

Необходимо отметить также, что метавселенная, объединяющая физическую, дополненную и виртуальную реальность, представляет собой многогранную платформу реализации программного обеспечения⁵⁶, которое отчасти может быть задействовано в сфере охраны правопорядка (например, для трехмерного иммерсивного обучения (с погружением в искусственно созданную виртуальную среду), оцифровки, воссоздания и анализа мест преступлений и пр.). Так, правоохранительные органы могут использовать метавселенную для создания виртуальных копий мест преступлений, к которым можно получить доступ и проанализировать их спустя долгое время после того, как физические места были изменены. Метавселенную можно использовать в качестве платформы для моделирования не только преступлений и мест их совершения, но и крупномасштабных чрезвычайных ситуаций, проведения репетиций реагирования на террористические атаки, тем самым позволяя правоохранительным органам участвовать в комплексных учениях по реагированию на крупные инциденты. С этой целью необходимо проведение комплексного анализа не только проблем киберпреступности, но и метапреступности, как отдельного направления профилактики метапреступных деяний.

Возможности пресечения преступлений, совершаемых с использованием информационных технологий, в том числе легализации преступных доходов, организации незаконного распространения запрещенных товаров и услуг, а также противоправного использования цифровых активов отчасти заложен в Стратегии национальной безопасности Российской Федерации⁵⁷, которая, однако, определяет

⁵⁶ Ritterbusch G. D., Teichmann M. R. Defining the metaverse: a systematic literature review // IEEE Access. 2023. V. 11. P. 12368.

⁵⁷ О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02 июля 2021 г. № 400 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_389271 (дата обращения: 22.10.2025).

лишь ряд предупредительных мер в области обеспечения общественной безопасности. Стоит также отметить необходимость непрерывного мониторинга и анализа угроз, возникающих в связи с внедрением новых информационно-телекоммуникационных технологий, с целью своевременного реагирования на них в соответствии со Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы»⁵⁸, а также важность борьбы с рассматриваемыми преступлениями и реализации концепции, определяющей принципы, цели, задачи и функции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий в целом, основным назначением которой является обеспечение проведения единой политики, направленной на защиту основных прав и свобод человека и гражданина и обеспечение национальной безопасности Российской Федерации в цифровой среде⁵⁹. Таким образом, все вышеуказанное подчеркивает сонаправленность проводимого исследования актуальным на сегодняшний день задачам в области обеспечения общественной и государственной безопасности, а также научно-технологического развития страны. Но, несмотря на перспективы реализации указанных программ (мероприятий) и дальновидность технологических планов, целесообразно формирование современных научно-прикладных основ методики расследования преступлений в сфере компьютерной информации с учетом сложившихся к настоящему времени тенденций их эволюции.

Нейтрализовать преступную деятельность в кибер- и метaprостранстве возможно лишь посредством формирования и последовательной реализации системы социально-экономических, организационно-правовых и научно-технических мер. Значительную роль в формировании указанной системы занимает криминалистика, одной из задач которой является разработка технико-криминалистических и тактико-криминалистических средств и методов раскрытия и расследования киберпреступлений. Криминалистическая методика, как раздел, завершающий курс криминалистики, представляет собой систему сведений о технических средствах собирания и исследования доказательств, а также

⁵⁸ О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 09 мая 2017 г. № 203 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_216363 (дата обращения: 22.10.2025).

⁵⁹ Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_495619 (дата обращения: 11.01.2025).

тактических приемах производства различных следственных действий, используемых в условиях расследования преступлений. Особенностью частной (типовой) методики расследования является ее структура, поскольку в ней отражена последовательность действий следователя по уголовному делу. Структура имеет практический смысл, поскольку способствует реализации теоретических положений и практических рекомендаций науки, обеспечивающих максимально эффективную организацию следственной работы⁶⁰. Разнообразие совершаемых преступлений в сфере компьютерной информации, их трансформация и эволюция с течением времени требует обобщения криминалистических знаний с целью выработки приемов, методов и средств выявления, расследования, а также противодействия им.

Рассматриваемые преступления представляют собой особый вид преступной деятельности и единый объект криминалистического исследования. Зачастую они объединены единым подходом преступника к способу подготовки, его совершения и сокрытия, имеют специфику места и времени совершения, обусловленные схожей обстановкой. Перечисленные характеристики позволяют объединить несколько видов преступных деяний в отдельный род (группу), однако методики их расследования могут довольно сильно отличаться.

К числу основных криминалистических категорий науки криминалистики относят криминалистическую характеристику преступлений⁶¹, которая, образует систему сведений о типичных криминалистически значимых признаках преступлений и связях между ними⁶². Криминалистическая характеристика складывается из элементов, в совокупности составляющих систему характерных криминалистических признаков конкретного преступления, на основе которых становится возможным выдвижение криминалистических версий и расследование⁶³.

Единого подхода к определению структуры и состава криминалистической характеристики преступлений не существует. Это обусловлено тем, что каждый случай в расследовании определенного вида преступного деяния имеет конкретное,

⁶⁰ Макаренко И. А., Эксархопуло А. А., Зайнуллин Р. И. Структура частной криминалистической методики: история формирования и перспективы развития. Часть 1 // Правовое государство: теория и практика. 2018. № 4 (54). С. 147.

⁶¹ Аверьянова Т. В. Криминалистика : учебник / под ред. Р. С. Белкина. М. : Норма : ИНФРА-М, 2023. С. 58.

⁶² Криминалистическая методика расследования отдельных видов и групп преступлений : учебное пособие / под ред. В. Д. Зеленского. Краснодар : КубГАУ, 2013. С. 8.

⁶³ Эксархопуло А. А. Криминалистика : учебник. Санкт-Петербург : Лема, 2010. С. 676.

неповторимое содержание этих элементов и их взаимосвязей, а также индивидуальное содержание способов его совершения.

Типовая криминалистическая характеристика преступления представляет собой систематизированную совокупность данных о преступном деянии, элементах его состава, имеющих значение для установления и изобличения виновного лица⁶⁴. В свете рассмотрения теоретических основ расследования преступлений в сфере компьютерной информации целесообразно выделить элементы их криминалистической характеристики. Кроме того, необходимость знания сущности криминалистической характеристики преступления, ее роли в процессе построения следственных версий⁶⁵, а также содержания типовой криминалистической характеристики определенной группы преступлений отражена в действующем на сегодняшний день профессиональном стандарте «Следователь-криминалист»⁶⁶, что подчеркивает важность использования криминалистической характеристики в практике расследования.

Анализ судебно-следственной практики и исследований, посвященных рассмотрению криминалистической характеристики преступлений, а также содержательных особенностей частных методик, позволяет выделить в структуре криминалистической характеристики основные ее элементы в виде способа совершения преступления, обстановки преступления, личности преступника, личности потерпевшего и предмета посягательства⁶⁷.

Помимо основных можно выделить достаточно обширный круг дополнительных элементов криминалистической характеристики преступлений, таких как способ сокрытия преступления⁶⁸, типичные следы преступления и вероятные места их нахождения⁶⁹, особенности и источники формируемой

⁶⁴ Исаенко В. Н. Криминалистическая характеристика преступлений и ее разновидности // Криминалистика. 2014. № 1(14). С. 41.

⁶⁵ Драпкин Л. Я. Построение и проверка следственных версий : автореф. дис. ... канд. юрид. наук. Москва, 1972. С. 7.

⁶⁶ Об утверждении профессионального стандарта «Следователь-криминалист» : приказ Министерства труда и социальной защиты Российской Федерации от 23 марта 2015 г. № 183н // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_178094 (дата обращения: 08.02.2025).

⁶⁷ Криминалистика. Теоретический курс : монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. Уфа : НИИ ППГ. 2022. С. 593.

⁶⁸ Пантелеев И. Ф. Методика расследования преступлений. М. : Всесоюз. юрид. заоч. ин-т, 1975. С. 10.

⁶⁹ Бессонов А. А. Основы криминалистического учения об исследовании и использовании криминалистической характеристики преступлений : монография. М. : Юрлитинформ, 2016. С. 135.

информации⁷⁰, распространенность преступного деяния⁷¹, особенности выявления и обнаружения преступления⁷², обстоятельства, подлежащие выяснению при расследовании⁷³ и пр.

С учетом того, что учение о криминалистической характеристике преступления состоит из двух частей – общей (понятие, структура и взаимосвязи ее элементов) и особенной (криминалистических характеристик отдельных категорий преступлений), строящейся на основе анализа уголовных дел⁷⁴, становится возможным выявление структуры криминалистической характеристики преступлений в сфере компьютерной информации, актуальной на сегодняшний день.

Так, анализ 284 уголовных дел, 240 обезличенных отчетных форм по состоянию оперативной обстановки на территории обслуживания органа МВД России (Республика Башкортостан), а также 2500 приговоров по фактам совершения преступлений в сфере компьютерной информации (ст. ст. 272, 272.1, 273, 274, 274.1 УК РФ, за исключением ст. ст. 274.2, 274.3, 274.4, 274.5 УК РФ, по которым на момент исследования отсутствовала судебно-следственная практика), в большей степени которые были представлены преступлениями, квалифицируемыми по ст. ст. 272 УК РФ и 273 УК РФ, отчасти в совокупности со ст. 159.6 УК РФ⁷⁵, позволил выделить соответствующие текущему состоянию преступности в сфере компьютерной информации элементы их криминалистической характеристики.

На основе проведенного исследования, а также с учетом результатов анкетирования сотрудников органов дознания, следствия и оперативных подразделений, криминалистическую характеристику преступлений в сфере компьютерной информации предлагается изложить в совокупности следующих

⁷⁰ Танасевич В. Г. Теоретические основы методики расследования преступлений // Советское государство и право. 1976. № 6. С. 92

⁷¹ Ледащев В. А. Общие положения криминалистической методики. Волгоград : Министерство внутренних дел СССР, 1976. С. 12.

⁷² Герасимов И. Ф. Общие положения методики расследования преступлений / под ред. И. Ф. Герасимова и Л. Я. Драпкина. М. : Высш. шк., 1994. С. 330.

⁷³ Еркенов С. Е. Взаимодействие правоохранительных органов стран СНГ при раскрытии и расследовании транснациональных преступлений : дис. ... канд. юрид. наук. М., 1999. С. 28.

⁷⁴ Криминалистика. Теоретический курс. Указ. соч. С. 589.

⁷⁵ О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_434573 (дата обращения: 08.02.2025).

элементов: способ совершения преступления с описанием типичных следов преступления, способов их сокрытия, вероятных мест их нахождения и распространенности (серийности) преступного деяния; обстановка (место (среда), время совершения) преступления; личность преступника; личность потерпевшего и предмет посягательства.

Включение в элемент «способ совершения преступления» такого дополнения как «распространенность (серийность) преступного деяния» применительно к преступлениям в сфере компьютерной информации предполагается целесообразным (несмотря на то, что указанное обстоятельство носит по своей природе криминологический характер⁷⁶). Это подтверждается на практике необходимостью проверки схожести (серийности) эпизода с ранее выявленными преступными деяниями и обязательным включением сведений о способе и иных обстоятельствах совершения преступления в подсистемы программно-технического комплекса интегрированного банка данных федерального уровня (ИБД-Ф) Главного информационно-аналитического центра МВД России⁷⁷. Кроме того, серийность преступного деяния является одним из реквизитов для указания в статистической карточке преступления⁷⁸, а также отчетах оперативной обстановки на территории обслуживания органа МВД России, формируемых в Сервисе обеспечения деятельности дежурных частей системы информационно-аналитического обеспечения деятельности МВД России.

Распространенность преступного деяния выражается в установлении факта серийности преступления по учетам подсистемы интегрированного банка данных «Дистанционное мошенничество», например, на основе полученных сведений об использовании в преступной схеме одних и тех же уникальных идентификаторов, которые присваиваются каждому устройству, подключенному к сети (МАС-идентификаторов (от англ. «media access control» – управление доступом к среде передачи)) сетевых адаптеров или IP-адресов устройств, абонентских

⁷⁶ Криминалистика. Теоретический курс. Указ. соч. С. 590.

⁷⁷ Харисова З. И. О структурных элементах криминалистической характеристики преступлений в сфере компьютерной информации // Журнал прикладных исследований. 2025. № 9. 199-203.

⁷⁸ О едином учете преступлений : приказ Генеральной прокуратуры Российской Федерации № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_57951/2ff7a8c72de3994f30496a0ccb1ddafdaddd518 (дата обращения: 08.02.2025).

номеров или банковских реквизитов⁷⁹.

Кроме того, указанное дополнение может выступить основой для формирования нового криминалистического учета цифровых доказательств, что сопоставлено с одной из основных задач государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационно-телекоммуникационных технологий⁸⁰, заключающейся в хранении информации о лицах, совершивших противоправные действия с использованием сети связи общего пользования, в том числе информации об абонентских номерах и SIM-блках, используемых в целях совершения противоправных действий. Предлагаемое дополнение может в дальнейшем определить первоначальные принципы интеллектуализации процесса расследования преступлений в сфере компьютерной информации, а также иных видов преступных деяний. Стоит также отметить, что личность потерпевшего в ряде случаев будет рассматриваться во взаимосвязи с предметом посягательства.

Обстоятельства, подлежащие выяснению при расследовании уголовных дел, возбужденных по признакам преступлений в сфере компьютерной информации, в рамках обязанностей следователя предусматривают составление согласованного плана совместных следственных действий и оперативно-розыскных мероприятий с установленными сроками исполнения и конкретными версиями, составленными с учетом фактических обстоятельств совершенного преступления и обстоятельств, подлежащих доказыванию.

Вышеуказанные обстоятельства, как правило, закрепляются алгоритмами действий сотрудников правоохранительных органов по конкретному виду

⁷⁹ Материалы уголовного дела № 12301800043000085, возбужденного 04 февраля 2023 г. МВД по Республике Башкортостан (ОМВД России по г. Нефтекамску); Материалы уголовного дела № 12301690022000050, возбужденного 11 января 2023 г. УМВД России по Томской области (ОМВД РФ по Кировскому району г. Томска); Материалы уголовного дела № 12301140027000864, возбужденного 15 сентября 2023 г. УМВД Старооскольской Белгородской области; Материалы уголовного дела № 12301750007000030, возбужденного 25 января 2023 г. ГУ МВД России по Челябинской области.

⁸⁰ О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 01 апреля 2025 г. № 41-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_502182 (дата обращения: 01.06.2025); О реализации пилотного проекта по оперативному взаимодействию уполномоченных государственных органов и организаций и информационному обмену между ними при противодействии правонарушениям, совершаемым с использованием информационных технологий : распоряжение Правительства РФ от 28 мая 2025 г. № 1350-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_506509 (дата обращения: 30.05.2025).

преступления, что особенно важно в целях повышения эффективности установления криминалистически значимой информации, способствующей раскрытию совершенного преступного деяния.

Выбор методики расследования преступления в сфере компьютерной информации может быть обусловлен конкретным его видом, информационной средой (сферой), используемыми преступниками техническими средствами и иными особенностями совершения преступных деяний. В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ № 646 от 05 декабря 2016 г., под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, веб-сайтов в сети «Интернет», сетей связи, информационных технологий и субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием указанных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений⁸¹.

Соответственно, совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере, определяется как информационная угроза безопасности Российской Федерации. Состояние защищенности государства, общества и отдельно взятой личности от информационных угроз с обеспечением всех конституционных прав и свобод человека и гражданина, достойного качества и уровня жизни граждан, суверенитета, территориальной целостности и устойчивого социально-экономического развития страны, обороны и безопасности государства определяется как информационная безопасность.

В криминалистике отсутствует однозначное понимание, что является предметом преступного посягательства несмотря на то, что данный элемент криминалистической характеристики преступлений часто отмечается исследователями и в большинстве случаев в основу своего понимания закладывает уголовно-правовую характеристику объекта и предмета преступления⁸². Общим объектом преступлений в сфере компьютерной информации выступают

⁸¹ Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 05 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации : офиц. сайт. URL: <http://pravo.gov.ru> (дата обращения: 22.10.2025).

⁸² Кардашевская М. В. Предмет преступного посягательства как элемент криминалистической характеристики преступлений // Вестник Московского университета МВД России. № 7. 2019. С. 236.

общественные отношения в информационной сфере, обеспечивающие состояние защищенности личности, общества и государства от информационных угроз.

Исходя из широкого понимания предмета преступления и положений Доктрины информационной безопасности Российской Федерации, к общим предметам преступлений в сфере компьютерной информации следует отнести: компьютерную информацию; объекты информатизации; информационные системы; веб-сайты; сети связи; деятельность субъектов, связанную с формированием и обработкой информации, развитием и использованием информационных технологий, а также обеспечением информационной безопасности⁸³.

Указанное дает основание полагать, что предмет посягательства соотносится с потерпевшей стороной, но анализ материалов судебно-следственной практики показал, что возможны ситуации, когда при выявленном предмете посягательства невозможно установить личность потерпевшего.

В соответствии с УК РФ предметом посягательства в узком смысле является компьютерная информация в виде сведений (сообщений или данных), представленных в форме электрических сигналов, вне зависимости от средств их хранения, обработки и передачи. Она характеризуется возможностью фиксации на электронном носителе информации и передачи с помощью информационно-телекоммуникационных сетей.

Средством (орудием) совершения преступления рассматриваемого вида могут являться как средство вычислительной техники, так и программное обеспечение, с помощью которых преступники могут выявлять угрозы безопасности компьютерной информации (условия и факторы, создающие потенциальную или реально существующую опасность нарушения безопасности данных), либо уязвимости предмета посягательства (недостатки программного обеспечения, технических средств или информационных систем в целом, которые могут быть использованы для реализации угроз безопасности информации).

Стоит отметить, что в ряде современных исследований криминалистическая характеристика преступлений рассматривается как информационная модель⁸⁴ (содержащая сведения о взаимосвязанных криминалистически значимых признаках преступления определенного вида, построенная на основе анализа и

⁸³ Попов А. Н. Преступления в сфере компьютерной информации. Указ. соч. С. 23.

⁸⁴ Бессонов А. А. Основы криминалистического учения об исследовании и использовании криминалистической характеристики преступлений. Указ. соч. С. 30.

обобщения практики их раскрытия и предназначенная для формирования частных методик расследования) или типовая информационная модель⁸⁵ (информационная система, построенная на основе статистически обработанных данных уголовных дел по преступлениям определенного вида, позволяющая на основе выявленных между ее элементами взаимосвязей формировать новые источники криминалистически значимой информации).

Более того, применительно к преступлениям в сфере компьютерной информации, возможно формирование информационно-компьютерных моделей⁸⁶ (обобщение сведений о криминалистически значимых признаках конкретного вида преступления и их закономерных связях между собой на основе изучения больших массивов уголовных дел), а также цифровых криминалистических моделей (построение моделей преступлений на базе криминалистических характеристик в машиночитаемой форме, в которой сведения о значимых признаках и их взаимосвязях выражены математическими категориями) как основы криминалистической методики их расследования⁸⁷. Отдельно необходимо обозначить возможность построения указанных моделей лишь на основе имеющейся судебно-следственной практики.

Поскольку преступления в сфере компьютерной информации отличаются значительным своим многообразием и сложностью в определении единого подхода к их расследованию, соответственно, возникают противоречия по определению типового состава элементов криминалистической характеристики (модели) по каждому из видов противоправного деяния, что обусловлено сложностью выявления механизмов совершения «высокотехнологичных» преступлений, исследования технических средств, поиска, собирания цифровых доказательств и, отчасти, трудностями сбора и анализа судебной практики по указанной категории дел. Между тем, знание о модели в виде типовых наборов элементов криминалистической характеристики преступлений важно, поскольку дает возможность выдвигать достоверные криминалистические версии об обстоятельствах, подлежащих установлению и доказыванию в каждом конкретном

⁸⁵ Ищенко Е. П., Колдин В. Я. Типовая информационная модель преступления как основа методики расследования // Известия высших учебных заведений. 2006. № 6 (269). С. 137.

⁸⁶ Россинская Е. Р., Семикаленова А. И. Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа») // Вестник Томского государственного университета. Право, 2021. № 42. С. 69.

⁸⁷ Бессонов А. А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4 (13). С. 60.

случае. Элементы криминалистической характеристики рассматриваемой категории преступлений имеют существенное значение и требуют дальнейшего рассмотрения в рамках настоящего исследования для выявления между составляющими причинно-следственных связей. Необходимость их выделения обусловлена тем, что при наличии сформированных ранее наборов специфичных для конкретного вида преступления элементов, заложенных, например, в цифровую криминалистическую модель, следователь осуществит выстраивание криминалистических версий и подбор наиболее подходящей методики расследования со значительно меньшими трудовыми и временными затратами.

Таким образом, криминалистическая характеристика преступлений фактически представляет собой информационно-теоретическую базу для установления механизма расследуемых преступных деяний и создания типовых алгоритмов их расследования. Несмотря на то, что набор элементов криминалистической характеристики для различных видов преступлений одной родовой группы могут совпадать, отдельные криминалистически информативные для той или иной категорий преступления составные элементы могут быть неинформативными или малоинформативными для другой. По этой причине стремление к созданию универсальной модели криминалистической характеристики нецелесообразно⁸⁸.

В связи с изложенным выдвигается гипотеза о возможности формирования цифрового двойника⁸⁹ преступления в сфере компьютерной информации в виде его цифровой копии⁹⁰, позволяющей оптимизировать эффективность расследования. В качестве исходных данных для построения такого рода информационно-компьютерной модели будут использоваться элементы криминалистической характеристики рассматриваемых преступлений. Наиболее полно рассмотреть элементы криминалистической характеристики преступления возможно посредством анализа сложившейся судебной-следственной практики.

По этой причине в дальнейшем необходимо проведение структурно-содержательного анализа элементов криминалистических характеристик преступлений, совершаемых в сфере компьютерной информации.

⁸⁸ Косарев С. Ю. История и теория криминалистических методик расследования преступлений. СПб.: Юридический центр Пресс, 2008. С. 283.

⁸⁹ Tao F., Cheng J., Qi Q. Digital twin-driven product design, manufacturing and service with big data // International journal of advanced manufacturing technology. 2018. № 94. P. 3563.

⁹⁰ Ali S., Arcaini P., Arrieta A. Foundation models for the digital twins creation of cyber-physical systems // Leveraging applications of formal methods, verification and validation. № 15223. P. 10.

1.2. Криминалистическая модель преступлений в сфере компьютерной информации (структурно-содержательный анализ элементов криминалистической характеристики)

Подавляющее большинство определений криминалистической характеристики преступлений представляют ее как функциональную систему, в общем виде – систему данных, способствующих раскрытию и расследованию преступлений⁹¹, либо как научную абстракцию, отражающую систему взаимосвязанных и корреляционно зависимых элементов той или иной категории (группы) преступлений и способствующую определению основных направлений в расследовании общественно опасного деяния⁹².

Рассматривая криминалистическую характеристику конкретного преступления (отдельно взятого совершенного преступления), можно отметить, что она является самой низкой степенью абстракции, в связи с этим ее рассмотрение может быть необходимо лишь, например, для высокоорганизованных преступных деяний⁹³. Но изучение материалов уголовных дел по конкретным преступным деяниям, анализ и обобщение судебной и следственной практики позволяют формировать типовые криминалистические характеристики преступлений⁹⁴. Преступления в сфере компьютерной информации имеют общие особенности, характеризующие структуру их криминалистической характеристики⁹⁵. Между тем лишь перечисление элементов криминалистической характеристики преступного деяния не может в полной мере определять ее сути, требующей выявления взаимосвязей между ее составляющими.

По этой причине необходимо провести содержательный анализ элементов криминалистической характеристики преступлений в сфере компьютерной информации с точки зрения системно-структурного, а также кибернетического

⁹¹ Ищенко Е. П., Колдин В. Я. Типовая информационная модель преступления как основа методики расследования. Указ. соч. С. 133.

⁹² Каневский Л. Л. Разработка типовых криминалистических характеристик преступлений и их использование в процессе расследования // Российский юридический журнал. 2000. № 2 (26). С. 111.

⁹³ Головин А. Ю. Криминалистическая систематика : монография. М. : ЛексЭст, 2002. С. 130; Ермолович В. Ф. Криминалистическая характеристика преступлений. Минск : Амалфея. 2001. С. 225; Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М. : Норма Инфра-М, 2001. С. 221.

⁹⁴ Бессонов А. А. Частная теория криминалистической характеристики преступлений : 12.00.12 : дис. ... докт. юрид. наук. Москва, 2017. С. 17; Криминалистика : учебник / под ред. И. М. Комарова. М. : Юрлитинформ, 2023. С. 554.

⁹⁵ Россинская Е. Р. Избранное. М. : Норма, 2021. С. 585.

подходов. Результаты проводимого анализа смогут послужить основой для:

- раскрытия содержания элементов криминалистических характеристик преступлений в сфере компьютерной информации;
- описания зависимостей между элементами криминалистической характеристики преступлений в сфере компьютерной информации и объективных закономерностей, позволяющих оптимизировать дальнейшее расследование⁹⁶;
- формирования информационной модели⁹⁷ или цифрового двойника (от англ. «digital twin» – цифровой двойник) преступления в сфере компьютерной информации (виртуальной копии преступного деяния) на основе наиболее значимых элементов криминалистической характеристики.

Несмотря на традиционный подход указания процентного соотношения встречаемости того или иного элемента криминалистической характеристики преступления при изучении судебно-следственной практики указание соотношений распространенности составных элементов формируемых криминалистических характеристик преступлений в сфере компьютерной информации являлось нерепрезентативным, ввиду того, что за анализируемый период явно прослеживалась тенденция изменений способов и средств совершения преступных деяний, способов сокрытия следов преступной деятельности, личностных характеристик субъектов преступлений во времени, что обусловлено эволюцией преступности рассматриваемого вида в связи с развитием информационных технологий.

Проведенный анализ показал, что свойства выборочной совокупности (выборки материалов судебно-следственной практики) не отражали характеристику генеральной совокупности (рассматриваемых преступлений в целом) во времени. Определить выборку, которая в полной мере повторяет все имеющиеся особенности генеральной совокупности невозможно, по этой причине в рамках исследования представлены наиболее существенные характеристики генеральной совокупности. Выборка материалов судебно-следственной практики представляла собой случайно отобранные единицы генеральной совокупности, достаточные для того, чтобы в ней были выражены существенные черты изучаемого распределения.

⁹⁶ Курс криминалистики : сборник научных трудов : в 3 томах / под ред. О. Н. Коршуновой .: Т. 3 : Методика расследования преступлений против общественной безопасности, других видов и групп преступлений. М. : Юридический центр, 2024. С. 59.

⁹⁷ Волчецкая Т. С. Криминалистическая ситуалогия : монография. / под ред. Н. П. Яблокова. Московский гос. ун-т им. М. В. Ломоносова, Калининградский гос. ун-т. М. ; Калининград : КГУ, 1997. С. 18.

Репрезентативность выборки эмпирических данных обусловлена выборкой группы преступлений одного рода, в которой представлены подгруппы, важные для исследования (преступления в сфере компьютерной информации, по которым на момент исследования имелаась судебно-следственная практика). Изучение всей генеральной совокупности с указанием процентного соотношения встречаемости того или иного элемента криминалистической характеристики преступлений в сфере компьютерной информации является «эталонным» случаем и, безусловно, позволило бы получить более полную информацию об исследуемых объектах, но такой подход с точки зрения реализации ограничен, поскольку вся генеральная совокупность для исследования недоступна.

Структурно-содержательный анализ в первую очередь определялся структурой главы 28 УК РФ (по составам с имеющейся судебно-следственной практикой), а также содержанием таких определенных ранее элементов криминалистической характеристики преступлений в сфере компьютерной информации как: способ совершения преступного деяния с описанием способов сокрытия и типичных следов преступления, вероятных мест их нахождения, а также распространенности (серийности) преступного деяния; обстановка (место (среда), время совершения и пр. обстоятельства); личность преступника; личность потерпевшего и предмет посягательства.

В контексте проводимого структурно-содержательного анализа элементов криминалистической характеристики преступлений в сфере компьютерной информации под информацией о способе совершения преступления будет подразумеваться действие или бездействие при совершении преступления, в некоторых случаях сопряженного с подготовкой и (или) сокрытием преступления, обусловленных условиями внешней среды и психофизиологическими свойствами личности⁹⁸. Между способами совершения рассматриваемых преступлений и их видами не всегда удастся напрямую установить корреляционные или вероятностные связи, при этом для совершения разных видов преступлений часто используются одни и те же средства (программные, аппаратные, программно-аппаратные), информационно-компьютерное обеспечение⁹⁹. Знания способов совершения преступлений в цифровой среде и их классификации необходимы для установления лица, совершившего преступление, а также определения путей и средств его розыска и изобличения.

⁹⁸ Эксархопуло А. А. Криминалистика. Указ. соч. С. 676.

⁹⁹ Россинская Е. Р. Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений // Вестник Восточно-Сибирского института МВД России. 2021. № 2 (97). С. 192.

Под способом сокрытия преступления будут предполагаться действия, направленные на уничтожение или сокрытие следов преступного деяния, либо следов причастности лица к совершению преступления. Типичные следы преступления являются производными последствиями от способа его совершения и по преступлениям в сфере компьютерной информации имеют наиболее важное доказательственное значение. Выявление вероятных мест нахождения цифровых следов позволяет наиболее точно определить способ совершенного преступления. Классифицировать цифровые следы целесообразно по месту их нахождения¹⁰⁰, дополнительно можно учитывать процессуальный статус лица, выделяя следы на средствах совершения преступления, следы на технических средствах потерпевшего, которые могут включать, например, сведения в реестре операционной системы электронного устройства, в журналах расширений файлов, на электронных носителях информации, в конфигурационных и системных файлах функционирования программного обеспечения и пр.

Распространенность (серийность) преступного деяния позволяет определить схожесть эпизода с ранее выявленными преступными деяниями, в частности со способами их совершения, и служит основой для построения алгоритма следственных действий. Абсолютная повторяемость способов преступлений во всех их признаках полностью исключена, способы могут повторяться в случае, если сохраняется действие определенных факторов, их детерминирующих в виде мотива и цели преступления, обстановки его совершения, индивидуальных качеств личности преступника, особенностей личности потерпевшего и предмета преступного посягательства, а так как детерминирующие факторы изменяются и в количественном и в качественном отношении, то неизбежно изменяются и способы совершения преступлений, сохраняя, однако, некоторую совокупность повторяющихся признаков¹⁰¹.

Под обстановкой совершения преступления понимается система взаимодействующих между собой объектов, явлений и процессов (до и в момент совершения преступного деяния), характеризующих место (среду), время, вещественные и иные факторы объективной реальности, которые в свою очередь, определяют возможность, условия и обстоятельства совершения преступления¹⁰².

¹⁰⁰ Семенов Н. Н. Проблемы использования компьютерной техники при раскрытии, расследовании преступлений и доказыванию по уголовным делам // Тактико-методические особенности расследования преступлений. Казань. 2018. С. 140.

¹⁰¹ Зуйков Г. Г. «Модус операнди», кибернетика, поиск // Кибернетика и право. 1970. С. 50.

¹⁰² Яблоков Н. П. Обстановка совершения преступления как элемент его криминалистической характеристики // Криминалистическая характеристика преступления. М. : Издательство Всесоюзного института по изучению причин и разработке мер предупреждения преступности. 1984. С. 35.

Обстановка совершения преступления во многом определяет выбор способа и средств совершения преступления, влияя на его механизм, а также позволяет судить о личностных характеристиках преступника. С учетом того, что вид типичных оставляемых следов по преступлениям в сфере компьютерной информации является цифровым, целесообразно под местом совершения преступного деяния подразумевать «среду», которая может представлять собой киберпространство, метaproстранство, распределенные реестры (блокчейн), квантовую среду, а также гибридные инфраструктуры.

Под сведениями о личности преступника будет предполагаться система данных о лице, способствующих его поиску и изобличению¹⁰³. Знание личностных качеств преступника, как правило, может объяснить способ совершения преступления, характер совершенного деяния, формирование и способы сокрытия следов, а также мотивы и цели преступного деяния. Изучение личности потерпевшего играет не менее важную роль в расследовании преступлений, что обусловлено ее взаимосвязью с такими элементами криминалистической характеристики преступления как, например, личность преступника, место и время совершения преступления.

Предмет преступного посягательства характеризует его уязвимость (некую угрозу безопасности информации), которая не входит в состав элементов криминалистической характеристики преступления, но зачастую позволяет наметить пути поиска следов¹⁰⁴, несущих в себе криминалистически значимую информацию.

Функциональным предназначением криминалистической характеристики преступления является установление связей между ее элементами, при этом отображение взаимосвязей удобно осуществлять на объектно-ориентированном языке моделирования UML¹⁰⁵ (от англ. «unified modeling language» – унифицированный язык моделирования), например, в виде упрощенной диаграммы взаимодействий (последовательности действий)¹⁰⁶, позволяющей визуализировать сложные системы, явления или процессы.

¹⁰³ Ахмедшин Р. Л. Криминалистическая характеристика личности преступника : 12.00.09 : автореф. дис. ... докт. юрид. наук. Томск, 2006. С. 23.

¹⁰⁴ Шабанов В. Б., Ермолович В. Ф. Соотношение криминалистической характеристики преступлений со следственными ситуациями, предметом доказывания, версиями и задачами расследования преступления // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2012. № 1 (27). С. 82.

¹⁰⁵ Бойцов А. К., Колмогорова С. С. Практическое моделирование на UML : монография. Санкт-Петербург : Реноме, 2023. С.14.

¹⁰⁶ Kebande V. R., Karie N. M. A UML-based approach for analysing potential digital forensic evidence // International journal of electronic security and digital forensics. 2018. № 7 (4). P. 355.

Так, личность преступника как отражение его профессионализма, взаимосвязана со способом совершения преступного деяния, наличием или возможностью сокрытия следов преступления (в целях исключения серийности), с выбором личности потерпевшего и (или) места и времени воздействия на предмет преступного посягательства с выявлением его уязвимостей (угроз безопасности компьютерной информации). Обстановка совершения преступления, определяя место (среду) и время его совершения, взаимосвязана с предметом посягательства, и потерпевшим, со способом и средствами совершения преступления, выбор которых во многом определяют особенности появления (сокрытия) типичных следов в наиболее вероятных местах их расположения, что, в свою очередь, связано с наличием у преступника специальных навыков и умений, а также возможностью выявления распространенности преступного деяния.

Способ совершения преступления (для преднамеренных преступных деяний¹⁰⁷) обуславливает появление типичных следов в компьютерных системах ввиду использования различных средств и связан с обстановкой реализации преступного умысла (местом (средой), временем), особенностями личности преступника (его навыками и умениями), а также предметом посягательства (личностью потерпевшего), особенности и уязвимости которого предопределяют выбор приемов и средств совершения преступного деяния, неоднократное выявление которых может свидетельствовать о распространенности преступного деяния. Для непреднамеренных преступных деяний важным является наличие специфической связи потерпевшего с последствиями преступных действий, например, с бездействием или размером и характером нанесенного вреда.

Для удобства дальнейшего анализа целесообразно структурировать способы совершения преступления в сфере компьютерной информации, условно классифицировав их, например, по объекту воздействия, по доступу к объекту воздействия, уровню автоматизации и мотиву воздействия и т. д. Так, например, по объекту воздействия способы совершения преступлений можно подразделить в отношении: технических средств (компьютеров, мобильных средств связи, серверного или промышленного оборудования и пр.); информационных систем (незаконный доступ, нарушение целостности данных, подмена информации); сетей связи (перехват данных, блокировка каналов передачи, изменение маршрутизации трафика и пр.); конкретного пользователя или программного обеспечения (фишинг, эксплуатация уязвимостей, внедрение вредоносного кода и т. п.).

По доступу к объекту воздействия совершение преступления возможно удаленно (без физического контакта с объектом, например, удаленная DDoS-атака (от англ. «distributed denial of service» – распределенный отказ в

¹⁰⁷ Ермолович В. Ф. Криминалистическая характеристика преступлений. Указ. соч. С. 37.

обслуживании), эксплуатация уязвимостей ресурса, размещенного в сети «Интернет», взлом паролей и т. п.), локально (с физическим доступом к устройству, например, установкой вредоносного программного обеспечения на компьютер, несанкционированным копированием данных с носителя информации) или гибридно (сочетанием удаленного и локального воздействий). По уровню автоматизации воздействия можно отметить автоматизированные (с использованием программного обеспечения, ботнетов и пр.) и неавтоматизированные (использование методов, обеспечивающих уникальный подход к особенностям конкретного объекта) способы. По мотиву воздействия можно отметить способы: деструктивные (уничтожение данных, саботаж, нарушение работы системы и пр.); в отношении нарушения конфиденциальности данных (кража данных, перехват трафика, шпионаж и т. п.); в отношении экономической или политической дестабилизации (кибершпионаж и пр.).

Стоит также отметить, что выделяют полноструктурные способы совершения преступления, которые могут охватывать систему действий по подготовке, совершению и сокрытию преступного деяния, а также неполноструктурные способы, в которых отсутствуют действия по подготовке или сокрытию следов¹⁰⁸. По содержанию способы совершения преступления подразделяются на осуществляемые путем активных действий, бездействия или их комбинации¹⁰⁹. Типичными следами по преступлениям, совершаемым в сфере компьютерной информации, могут, например, выступить следы на носителях информации, в оперативной памяти, следы сетевой активности, следы в программном обеспечении и пр. Так, следы на носителях информации могут представлять собой: журналы файловых систем, метаданные (изменения в структуре каталогов и файлов системы (лог-файлы, временные метки, атрибуты доступа); фрагменты удаленных или модифицированных данных (системные журналы с протоколированием действий, связанных со входом в систему, запуском процессов, выявленных ошибок и пр.); журналы эксплуатируемого программного обеспечения (мониторинг процессов инфраструктуры объекта, реконструкция последовательности событий) и пр.

Следы в оперативной памяти могут содержать временные данные и артефакты: дампы памяти, содержащие сессии активных процессов, фрагменты исполняемых файлов и вредоносного программного обеспечения, загруженных в память, следы сессий удаленного доступа и пр. Следами сетевой активности могут признаваться данные об IP-идентификаторах, сетевой маршрутизации,

¹⁰⁸ Зуйков Г. Г. Криминалистическое учение о способе совершения преступления: автореф. дис. ... докт. юрид. наук. Москва, 1970. С. 10.

¹⁰⁹ Головин А. Ю. Криминалистическая систематика. Указ. соч. С. 128.

MAC-адресах и идентификации сетевого оборудования, протоколах передачи, а также журналы сетевого трафика и т. п. Следы в программном обеспечении могут представлять собой цифровые артефакты в системах мониторинга технических средств или иных информационных системах, компьютерах, журналах работы серверного оборудования, журналах аутентификации и изменений прав доступа, журналах эксплуатации криптографического программного обеспечения и т. д. Выявление и изучение криминалистически значимых особенностей личности потерпевшего, его поведения и предмета посягательства позволяют глубже разобраться в обстоятельствах преступления, его мотивах¹¹⁰.

Предмет преступного посягательства, преимущественно определяемый по преступлениям корыстной направленности, непосредственно связан с личностью потерпевшего и представляет особый интерес в связи с тем, что определяет непосредственную взаимосвязь потерпевшего с лицом, совершившим преступление, и, являясь целью преступной деятельности, определяет возможные приемы и средства, место и время совершения преступного деяния. Стоит отметить, что предмет преступного посягательства по преступлениям в сфере компьютерной информации может представлять собой следовоспринимающий объект (с точки зрения наличия в техническом средстве носителя информации), отражающий сведения о месте и времени совершения преступления, а также следообразующий объект (с точки зрения наличия в предмете преступного посягательства системного и прикладного программного обеспечения).

Таким образом, предварительно проведенный системный анализ взаимосвязанности предлагаемых элементов криминалистической характеристики преступлений в сфере компьютерной информации дает основания для рассмотрения их как основы для формирования информационной модели (цифрового двойника) преступления в сфере компьютерной информации на основе наиболее значимых элементов криминалистической характеристики, а также соответствующих частных методик их расследования. При надлежащем формировании системы исходных данных для криминалистической характеристики преступлений можно существенно продвинуться в понимании механизма совершения соответствующих преступных деяний¹¹¹, формирования алгоритмов их расследования, описания особенностей наиболее характерных для расследования этих преступлений следственных действий.

¹¹⁰ Каневский Л. Л. Криминалистические проблемы расследования и профилактики преступлений несовершеннолетних. Красноярск : Красноярский университет, 1991. С. 94; Masmoudi S. Unveiling the human factor in cybercrime and cybersecurity // *Cybercrime unveiled: technologies for analysing legal complexity*. 2025. V. 1181. P. 41.

¹¹¹ Волынский А. Ф. Криминалистика и криминалистическая деятельность. Избранное. М. : Юнити-Дана, 2019. С. 370.

1.2.1. Криминалистическая характеристика неправомерного доступа к компьютерной информации

Рассматривая неправомерный доступ к компьютерной информации (ст. 272 УК РФ) необходимо отметить, что под доступом к компьютерной информации понимается возможность ознакомиться с ней либо в дальнейшем ею воспользоваться в результате применения тех или иных средств и способов, что определяет наступление одного или нескольких последствий: уничтожение информации (в виде приведения ее (или ее части) в непригодное для использования по назначению состояние вне зависимости от возможности дальнейшего ее восстановления); блокирование информации (в виде создания условий, препятствующих в течение некоторого времени или на постоянной основе доступу к компьютерной информации субъекта, имеющего право на него, а также невозможности ее дальнейшего использования, в том числе ограничения или прекращения доступа к компьютеру или информационной системе и находящимся в них информационным ресурсам); модификация информации (в виде любых изменений компьютерной информации, в том числе внесения изменений в программное обеспечение и базы данных, в информационные ресурсы, размещаемые на электронных носителях информации); копирование информации (в виде неправомерного дублирования информации на другой носитель и воспроизведения ее в любой форме)¹¹².

В соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» неправомерным признается доступ к информации лица, который на момент доступа не обладает соответствующими правами на работу с данной информацией, компьютером или информационной системой, равно как и не имеет прав на использование средств и способов для ознакомления с информацией, в отношении которой приняты специальные меры по защите¹¹³ (охраняемая законом информация может характеризоваться специальным режимом ее правовой защиты и являться, например, служебной, коммерческой, нотариальной, государственной или иной тайной, а также объектами авторского права и смежных прав).

¹¹² Харисова З. И. Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации // Правовое государство: теория и практика. 2025. № 2. С. 97.

¹¹³ Комментарий к Уголовному кодексу РФ в 4 т. Том 3. Особенная часть. Раздел IX / В. М. Лебедев [и др.]. М. : Юрайт, 2024. С. 286.

Стоит отметить, что наиболее распространенной ситуацией в настоящее время, связанной с неправомерным доступом к компьютерной информации, является несанкционированный доступ к аккаунтам граждан на едином портале государственных и муниципальных услуг (справочно-информационный интернет-портал «Госуслуги»), который сопровождается копированием охраняемой законом информации и ее использованием в целях заполнения заявок на получение кредитных денежных средств и последующим распоряжением ими. Так, в результате несанкционированного доступа к аккаунту гражданина на едином портале государственных и муниципальных услуг преодолением системы защиты и копированием охраняемой законом информации на владельца аккаунта удаленно был оформлен потребительский кредит с последующим выводом и обналичиванием денежных средств неустановленными лицами, в результате чего гражданину был нанесен имущественный ущерб, при этом преступник в целях сокрытия следов преступного деяния использовал средство анонимизации в виде сервиса «VPN»¹¹⁴ (от англ. «virtual private network» – виртуальная частная сеть), обеспечивающего шифрование трафика и сокрытие реального IP-адреса.

Способ совершения преступления. Среди основных преднамеренных способов осуществления неправомерного доступа к компьютерной информации можно отметить: преодоление систем защиты в виде хищения учетных данных пользователей; использование несовершенства систем защиты информации; выявление уязвимостей программного обеспечения (эксплойтов (от англ. «exploit» – эксплуатировать)) и операционных систем; несанкционированное подключение к техническому средству и информационной системе, а также вспомогательному компьютерному оборудованию, внешним запоминающим устройствам и пр. в том числе удаленно или в случае системной поломки; фишинг (создание поддельных ресурсов или сообщений для несанкционированного получения данных) и т. п. Так, например, с целью исключения материальных затрат на приобретение лицензионного программного обеспечения у гражданина возник преступный умысел, направленный на неправомерный доступ к программе путем модификации и копирования компьютерной информации для нейтрализации встроенной системы защиты¹¹⁵. При реализации преступного умысла была выявлена уязвимость

¹¹⁴ Материалы уголовного дела № 12301800002000570, возбужденного 12 июня 2023 г. СО ОМВД России по Белорецкому району Республики Башкортостан.

¹¹⁵ Приговор по уголовному делу № 1-131/2022 // Первоуральский городской суд Свердловской области : офиц. сайт. URL: http://pervouralsky--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=409327185&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

программного обеспечения, определена возможность использования несовершенства систем защиты информации программного продукта, на основе системного оригинального файла программы был создан новый документ для модификации исполняемых файлов, что позволило нейтрализовать систему защиты оригинального программного продукта и несанкционированно запускать информационную систему без лицензии при отсутствии ключей аппаратной защиты.

Другим примером является умысел гражданина по модификации компьютерной информации и осуществлению неправомерного доступа к административному разделу управления интернет-магазином, а также изменению содержания стартовой страницы и установлению перенаправления на сторонний ресурс. Продолжая преступные действия, направленные на неправомерный доступ к конфиденциальным данным, принадлежащим индивидуальному предпринимателю, зная логин и пароль к его электронному почтовому ящику, гражданин осуществил доступ к содержимому электронной почты потерпевшего, где находилась охраняемая законом компьютерная информация. Имея умысел также и на блокирование доступа к почтовому ящику, осуществил неправомерный вход в административный раздел управления им и изменил пароль для осуществления доступа к регистрационной учетной записи, необходимой для использования электронной почты, после чего для правомерного пользователя доступ к указанному почтовому ящику был заблокирован¹¹⁶.

Процессы, возникшие в ходе случайных действий либо стечения обстоятельств, относят к непреднамеренным, это может быть, например: доступ к учетной записи иного пользователя из-за автосохранения пароля в браузере; работа на компьютере, доступ к которому имеется у нескольких пользователей (в офисе, коворкинге) с сохранением личных данных в системе. К программным способам можно отнести неправомерный доступ к компьютерной информации, осуществленный с использованием специализированного программного обеспечения. Доступ к информации с использованием непрограммных способов осуществляется посредством специальных технических средств, но не предполагает использование дополнительных приложений (например, установку аппаратных устройств, записывающих нажатия клавиш (кейлоггинг) и т. п.).

¹¹⁶ Приговор по уголовному делу № 1-977/2023 // Стерлитамакский городской суд Республики Башкортостан : офиц. сайт. URL: http://sterlitamaksky--bkr.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=134549564&case_uid=21cf7e70-e48d-462a-a09e-e84f634e8980&delo_id=1540006 (дата обращения: 08.02.2025).

В целом все способы неправомерного доступа к компьютерной информации можно подразделить на непосредственный доступ, удаленный и гибридный. В большинстве случаев при совершении указанных преступлений применяются различные комбинации перечисленных способов, функционирующих по различным алгоритмам¹¹⁷.

Способ совершения преступления в сфере компьютерной информации обусловлен в первую очередь использованием того или иного средства совершения преступления. Анализ уголовных дел позволил выявить основные средства совершения неправомерного доступа к компьютерной информации. При непосредственном доступе ими могут выступать носители информации, эксплуатируемые с техническими средствами, а при опосредованном доступе – сетевое оборудование и средства доступа в информационные системы (средства вычислительной техники, мобильные средства связи и пр.).

К основным средствам также относится различное программное обеспечение (например, сервисы «VPN», системы прокси-серверов, построенные на базе многослойного шифрования данных, вредоносные программы, способные к распространению в локальных информационных системах в целях выполнения какого-либо деструктивного действия (удаление, блокирование или изменение файлов), а также программное обеспечение, предназначенное для проведения тестов на проникновение и пр.).

К средствам хранения компьютерной информации относятся ее материальные носители¹¹⁸ – жесткие и оптические диски, USB-накопители, карты памяти и т. п., средством обработки компьютерной информации служит вычислительное устройство (процессор) технического средства. Каналы передачи информации могут быть проводными и беспроводными¹¹⁹.

Основными способами сокрытия следов неправомерного доступа к компьютерной информации являются: очищение журналов и шифрование событий в системе; удаление сведений о подключениях к компьютерам или информационным системам; использование программных средств анонимизации в целях подмены IP-адресов устройств (сервисы «VPN» и системы прокси-серверов); несанкционированное подключение к беспроводным точкам доступа;

¹¹⁷ Вехов В. Б. Компьютерные преступления. Способы совершения. Методики расследования. М.: Право и закон, 1996. С. 100.

¹¹⁸ Усов А. И. Судебная компьютерно-техническая экспертиза: становление, развитие, методическое обеспечение // Теория и практика судебной экспертизы. 2008. № 3 (11). С. 15.

¹¹⁹ Справочник следователя : научно-методическое пособие. Т. 2. М. : ФГКУ ВНИИ МВД России, 2023. С. 90.

использование беспроводных модемов с SIM-картами, оформленными на подставных лиц, с целью анонимизации абонентских номеров, а также VoIP-технологий (от англ. «voice over internet protocol» – протокол, обеспечивающий передачу речевого сигнала по сети «Интернет» или другим IP-сетям) и виртуальных (облачных) автоматических телефонных станций; задействование мессенджеров, обеспечивающих усиленное шифрование данных и пр. Так, гражданин, используя принадлежащий ему мобильный телефон с установленным VPN-приложением, позволяющим анонимизировать пользователя и скрывать его действительное местонахождение, по абонентскому номеру, логину и паролю (приобретенным в корыстных целях у неустановленного лица), привязанным к принадлежащей потерпевшему учетной записи «Единого портала государственных и муниципальных услуг», осуществил неправомерный доступ к охраняемой законом компьютерной информации, а именно, к персональным данным потерпевшего, после чего с учетной записи личного кабинета было сформировано и направлено электронное заявление на получение кредита, а также была осуществлена модификация сведений о реквизитах банковской карты для перечисления и дальнейшего вывода денежных средств¹²⁰.

Типичными следами неправомерного доступа к компьютерной информации в общем случае являются цифровые (установленное программное обеспечение, используемое для несанкционированного доступа, изменения в конфигурации операционной системы устройства, журналы подключений к компьютерам или информационным системам, модифицированные или заблокированные файлы данных и т. п.) и материальные следы на компьютерной периферии.

Следы по рассматриваемым преступным деяниям могут быть обнаружены в системном и прикладном программном обеспечении и в поименованных областях записей на носителях информации. Следы могут быть опосредованы с электронными файлами; базами данных; электронными ключами (подписями); идентификаторами в сети передачи данных (например, IP-адрес устройства или MAC-адрес его сетевой карты), IMEI-кодами мобильных средств связи (от англ. «international mobile equipment identity» – международный идентификатор мобильного оборудования), DNS-адресами; реестрами операционных систем;

¹²⁰ Приговор по уголовному делу № 1-8/2024 // Ленинский районный суд г. Саранска Республики Мордовия : офиц. сайт. URL: https://leninsky--mor.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=131817209&case_uid=d1943dd0-9e60-434d-ae7c-ad5096407646&delo_id=1540006 (дата обращения: 08.02.2025).

файлами подкачки и временными файлами, образующимися в операционной системе; сетевым трафиком; цифровыми финансовыми активами и электронными кошельками; IMS-, SMS- и MMS-сообщениями и пр.

Отдельно стоит отметить факторы, связанные с развитием генеративного искусственного интеллекта, метавселенных и квантовых алгоритмов, которые порождают относительно новые виды преступных деяний, связанных с неправомерным доступом к компьютерной информации (подмена данных, кража виртуальной собственности, идентификаторов личности, взлом ключей шифрования, перехват данных и т. п.).

По вышеуказанным преступным деяниям следы могут представлять собой сфальсифицированный мультимедиаконтент¹²¹, метаданные¹²² и конфигурации серверов, связанных с эксплуатацией метaprостранства (журналы функционирования программного обеспечения, обеспечивающего визуализацию трехмерных виртуальных пространств и работу децентрализованных сетей¹²³, конфигурационные файлы с настройками дополненной, виртуальной и расширенной реальностей, сетевые адреса взаимодействия цифровых аватаров и пр.) или квантовых компьютеров (реестры эксплуатации квантовых приложений и дампов квантовых состояний, протоколы квантовых связей¹²⁴ и пр.). Вероятными местами расположения типичных следов неправомерного доступа к компьютерной информации в цифровом виде являются носители информации, серверное оборудование и облачные хранилища, в том числе файлы и каталоги хранения данных, файлы конфигурации программ удаленного доступа и пр.

Распространенность преступного деяния выражается в установлении факта схожести эпизода на основе полученных сведений об использовании в преступной схеме способа совершения преступления. Так, например, признаками схожести по уголовным делам выступали идентичные реквизиты в виде: MAC- или IP-адресов устройств; абонентских номеров; вредоносных программ; IMEI-кодов задействованных мобильных средств связи; электронных адресов; банковских

¹²¹ Hashemi A., Shi W., Corriveau J. AI-generated or AI touch-up. Identifying AI contribution in text data // International journal of data science and analytics. 2024. V. 1. P.2.

¹²² Pachimatla D., Kilari R., Ranitha I. Advanced algorithms to detect and prevent the spread of manipulated images and videos using deep learning and AI // Proceedings of 5th international conference on recent trends in machine learning, IoT, smart cities and applications. 2025. V. 1182. P. 416.

¹²³ Qin H., Wang Y., Hui P. Identity, crimes, and law enforcement in the metaverse // Humanities and social sciences communications. 2025. № 12 (194). P. 2.

¹²⁴ Mihailescu M., Nita S., Marascu V. Quantum algorithms. Cham : Springer, 2025. P. 80.

реквизитов и т. п.¹²⁵.

Несмотря на имеющиеся проблемы реализации основных принципов теории криминалистической идентификации¹²⁶ по установлению связи между двумя объектами (идентифицируемым и идентифицирующим) посредством определения их идентичности или отсутствия таковой в процессе расследования преступного деяния¹²⁷, особенностей общей криминалистической теории распознавания¹²⁸, построенной на основе кибернетической теории распознавания образов¹²⁹ и криминалистической диагностики, заключающейся в идентификации материальных процессов, явлений, состояний материальных объектов и их комплексов, указанное дополнение в свете построения цифровых криминалистических моделей (моделей преступлений на базе криминалистических характеристик в машиночитаемой форме, в которой сведения о значимых признаках и их взаимосвязях выражены математическими категориями)¹³⁰ представляется весьма актуальным и ввиду тесной взаимосвязи с цифровыми признаками преступных деяний рассматриваемого вида позволяют наиболее просто осуществить идентификацию задействованных в преступлении объектов или диагностику протекающих информационных процессов, например, путем использования методов интеллектуального анализа и распознавания данных¹³¹,

¹²⁵ Материалы уголовного дела № 12301010018000015, возбужденного 09 января 2023 г. ГУ МВД России по Алтайскому краю (МО МВД России по г. Каменский); Материалы уголовного дела № 12201010040001465, возбужденного 20 июля 2022 г. ГУ МВД России по Алтайскому краю (УМВД России по г. Барнаулу); Материалы уголовного дела № 12201010041001894, возбужденного 28 сентября 2022 г. ГУ МВД России по Алтайскому краю (УМВД России по г. Барнаулу); Материалы уголовного дела № 12301500049001096, возбужденного 03 мая 2023 г. ГУ МВД России по Новосибирской области (УМВД России по г. Новосибирску); Материалы уголовного дела № 12301420029000604, возбужденного 07 сентября 2023 г. УМВД России по г. Липецку; Материалы уголовного дела № 12301800002001025, возбужденного 26 октября 2023 г. СО ОМВД России по Белорецкому району Республики Башкортостан; Материалы уголовного дела № 11701070014020098, возбужденного 10 марта 2017 г. ГУ МВД России по Ставропольскому краю (ОМВД России Благодарненский); Материалы уголовного дела № 11701070014020077, возбужденного 07 марта 2017 г. ГУ МВД России по Ставропольскому краю (ОМВД России Благодарненский).

¹²⁶ Потапов С. М. Принципы криминалистической идентификации // Советское государство и право. 1940. № 1. С. 80.

¹²⁷ Криминалистика. Теоретический курс. Указ. соч. С. 236.

¹²⁸ Драпкин Л. Я., Карагодин В. Н. Криминалистика. М. : Проспект, 2007. С. 32.

¹²⁹ Тюхтин В. С. Отражение, системы, кибернетика. Теория отражения в свете кибернетики и системного подхода. М. : Наука. 1972. С. 71.

¹³⁰ Бессонов А. А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности. Указ. соч. С. 60.

¹³¹ Татарникова Т. М. Интеллектуальный анализ данных : монография : Вологда : Инфра-Инженери, 2024. С. 8.

реализованных на основе технологий искусственного интеллекта и машинного обучения.

Обстановка совершения преступления. Обстановка совершения неправомерного доступа к компьютерной информации предполагает как непосредственный доступ к объекту посягательства (преимущественно в момент отсутствия обладателя защищаемой информации), так и удаленный с любой точки мира (при наличии подключения к сети «Интернет» или к локальной сети предприятия) и определяется спецификой работы с данными в электронном виде и использованием программно-аппаратных средств для их обработки, хранения и передачи.

Местом совершения указанного преступления являются как конкретные компьютеры, серверы или информационные системы (зачастую значительно удаленные друг от друга), так и локальные территории, учреждения и организации, в которых эксплуатируется объект преступления. В целях сокрытия физического расположения преступника удаленный доступ нередко осуществляется из общественных мест, предоставляющих сеть «Интернет» в порядке пользования услугами на базе организации.

В подавляющем большинстве случаев местом (средой) совершения неправомерного доступа к компьютерной информации является киберпространство ввиду его распространенности среди населения, реже – метaproстранство, блокчейн (распределенные реестры), либо гибридные инфраструктуры (распределенные облачные системы хранения данных и пр.) Таким образом, местом совершения рассматриваемого вида преступления является, как правило, место реализации преступного умысла в интернет-пространстве – место, где фактически располагалось компьютерное оборудование, посредством которого реализован преступный план.

Согласно ч. 2 ст. 9 УК РФ временем совершения преступления признается время окончания преступного деяния вне зависимости от момента наступления последствий. Время совершения рассматриваемого вида преступлений, несмотря на протоколирование действий в системе, не всегда устанавливается точно, поскольку их совершение часто связано с задействованием различных компьютеров, программного обеспечения, информационных систем и пр., реестры функционирования которых бывает довольно сложно сопоставить. Кроме того, работа указанных средств связана со временем, установленным в его системе, которое может быть легко изменено преступником в целях искажения типичных следов.

Таким образом, анализ обстановки совершения преступления, представленной в качестве самостоятельного элемента криминалистической характеристики, позволяет следователю получить информацию об обстоятельствах и условиях, предшествовавших преступлению, о том, что в обстановке способствовало или препятствовало его совершению, каким образом обстановка повлияла на выбор способов, орудий и средств совершения преступления, а также личности потерпевшего и др.¹³². Стоит отметить, что, например, несанкционированный доступ к аккаунту на едином портале государственных и муниципальных услуг, как правило, происходил в вечернее время, либо в выходные дни. Таким образом преступники пытались застать потенциальную жертву со сниженным уровнем критического мышления (расслабленным, спящим и пр.)¹³³.

Личность преступника. Сведения о преступнике, сопоставленные с данными о способе и обстановке совершения преступления, позволяют сформировать новые сведения, способствующие его поиску и изобличению¹³⁴. Как правило, лицо, осуществляющее неправомерный доступ к компьютерной информации, имеет высшее или среднее инженерно-техническое либо экономическое образование, обладает устойчивыми навыками работы с техническими средствами и программным обеспечением. Совершаемые им преступления часто носят серийный, многоэпизодный характер и сопровождаются тщательными действиями по сокрытию следов преступной деятельности. Помимо указанной категории все чаще встречаются несовершеннолетние, действующие по заранее определенным алгоритмам, не требующим специальных знаний в области информационных технологий или обеспечения информационной безопасности. Так, наблюдается рост количества вовлеченных несовершеннолетних участников (+ 225,2 % – за последние пять лет, + 55,2 % – за 2024 год)¹³⁵ в организованные преступные группы или преступные сообщества (преступные организации), содействию которому служит активно распространяющееся дропперство (от англ. «drop» – сбрасывать).

¹³² Яблоков Н. П. Обстановка совершения преступления как элемент его криминалистической характеристики . Указ. соч. С. 35.

¹³³ Кибермошенничество: портрет пострадавшего // Центральный банк Российской Федерации (Банк России) : офиц. сайт. URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024 (дата обращения: 28.03.2025).

¹³⁴ Ахмедшин Р. Л. Криминалистическая характеристика личности преступника. Указ. соч. С. 23.

¹³⁵ Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. Указ. соч. С. 61.

Негативная тенденция объясняется уязвимостью этой социальной группы, обладающей ограниченными навыками работы с цифровыми технологиями и недостаточным уровнем правосознания, отсутствием критической оценки последствий участия в преступной деятельности (в том числе при совершении преступлений в сфере компьютерной информации), широкой распространенностью веб-сервисов и площадок, обеспечивающих анонимное вербование несовершеннолетних (тематические чаты и сообщества, игровые платформы, социальные сети и пр.), а также желанием легкого заработка при минимальных трудозатратах. Кроме того, на развитие такого рода негативного явления влияет развитие нового вида бизнеса, заключающегося в вербовке и последующей продаже дроп-пользователей, создании фирм дропповодов, сотрудничающих с организованной преступностью и рекрутирующих дропперов для дальнейшего их перераспределения по заказчикам, занимающимся противоправной деятельностью.

Так, подросток приобрел в сети «Интернет» базу данных о гражданах, которые не использовали зарегистрированные на них абонентские номера. Используя указанные сведения, действуя согласно приобретенным инструкциям, он покупал «пустые» SIM-карты (без привязки к контактному номеру), с возможностью саморегистрации карты и ее восстановления¹³⁶. Указанные манипуляции позволяли несовершеннолетнему осуществлять неправомерный доступ к компьютерной информации, размещенной на едином портале государственных и муниципальных услуг (ныне квалифицируется как организация деятельности по незаконному обороту SIM-карт (ст. 274.4 УК РФ), неправомерный оборот аккаунтов и учетных данных (ст. 274.5 УК РФ)).

Несовершеннолетние при этом выступают не только в качестве исполнителей преступлений, но и «средством» совершения преступного деяния в руках взрослых участников организованных преступных групп (так называемые «неразводные» участники нелегальных схем и «разводные» соответственно¹³⁷),

¹³⁶ Приговор по уголовному делу № 1-46/2025// Семилукский районный суд г. Воронежа : офиц. сайт. URL: https://semiluksky--vrn.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=19061884&case_uid=be7f959c-cdc2-4dbb-9c38-b7215a05b923&delo_id=1540006 (дата обращения: 14.05.2025).

¹³⁷ Аналитический обзор «Инструменты противодействия кибермошенничеству: анализ системы вывода денежных средств, похищенных у граждан» // ПАО Сбербанк : офиц. сайт. URL: https://www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhnyh_sredstv (дата обращения: 27.05.2025).

выступая в качестве дропов («транзитов», «заливщиков», «обнальщиков»¹³⁸ и пр. лиц), т. е. лиц, например, оформляющих на себя счета, SIM-карты для последующего обналичивания похищенных средств, сознательно или неосознанно предоставляют доступ к оформленным на них электронным средствам платежа.

Стоит отметить результаты анализа материалов уголовных дел, которые показали, что действия дропперов в ряде случаев могут сопутствовать мошенничеству (ст. 159 УК РФ), легализации (отмыванию) денежных средств или иного имущества, полученных другими лицами преступным путем (ст. 174 УК РФ), неправомерному обороту аккаунтов и учетных данных (ст. 274.5 УК РФ) или неправомерному обороту средств платежей (ст. 187 УК РФ), при этом они зачастую сопряжены с задействованием в преступной схеме различных информационных технологий и технических средств и могут отчасти сопутствовать неправомерному доступу к компьютерной информации (ст. 272 УК РФ). Так, по материалам возбужденного Главным управлением МВД России по Нижегородской области уголовного дела о дропперстве, гражданин получил в свое личное пользование доступ к электронному платежному сервису, оформленному на его несовершеннолетнюю знакомую. В течение нескольких дней гражданин использовал полученные данные для неправомерного доступа к компьютерной информации и перевода на счет несовершеннолетней денежных средств, похищенных преступниками у третьих лиц, а затем выводил их на сторонние счета¹³⁹.

Особенностью личности преступника, совершающего преступление в сфере компьютерной информации, является его возраст в пределах от 16 до 45 лет¹⁴⁰, также отмечается, что около 90 % лиц, совершающих указанные деяния, мужского пола¹⁴¹.

¹³⁸ Дропперы: связующее звено преступной цепи [Электронный ресурс] // Национальный исследовательский университет «Высшая школа экономики» : офиц. сайт. URL: <https://daily.hse.ru/post/zizn-dropper-a-pomenyat-krossovki-na-svobodu> (дата обращения: 27.05.2025).

¹³⁹ Приговор по уголовному делу № 1-86/2025 // Тоншаевский районный суд Нижегородской области : офиц. сайт. URL: https://tonshaevsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=46728556&case_uid=a1bcdad7-e8c2-4fa0-be37-9515948dce42&delo_id=1540006 (дата обращения: 30.10.2025).

¹⁴⁰ ИТ-справочник следователя : монография / под ред. С. В. Зуева. М.: Юрлитинформ. 2019. С. 77.

¹⁴¹ Holt T. J., Bossler A. M., Seigfried-Spellar K. C. Cybercrime and digital forensics. introduction. Abingdon : Routledge, 2018. P. 75.

Вместе с тем, деление преступников на возрастные категории носит весьма условный характер¹⁴², по этой причине в дальнейшем эта особенность учитываться не будет. Однако стоит отметить, что взрослый преступник, как правило, грамотно владеет комплексом манипулятивных приемов и техник воздействия на жертву с целью неправомерного доступа к конфиденциальной информации, методами социальной инженерии, а также совокупностью знаний в области социологии и психологии, которая позволяет управлять поведением людей, играя на их эмоциях, чувствах, страхах и рефлексках (под предлогом инвестирования, предоставления легкого и удаленного заработка, выигрыша денежных средств и сохранения их на счете), прогнозируя их возможное поведение исходя из складывающейся обстановки.

Анализ уголовных дел показал, что преступники часто использовали принцип доверия, построенного на знании, тщательно готовились к взаимодействию с конкретным лицом, собирая разведывательную информацию из открытых источников или ресурсов, имеющихся у них в распоряжении, персонализируя ее под предмет неправомерного доступа. Так, будучи специалистом по взысканию задолженности, гражданка, согласно назначенным правам в информационной системе по должностной инструкции, имела доступ к сведениям по должникам¹⁴³. Установив доверительный контакт с потерпевшим, формально выяснила причины неоплаты задолженности, путем обмана и злоупотребления доверием клиента организации похитила денежные средства, сообщив потерпевшему несоответствующую действительности информацию о том, что целесообразнее направлять платежи по погашению задолженности в обход банка, непосредственно на ее личную банковскую карту, при этом заведомо зная, что переведенные на указанную карту денежные средства она на погашение задолженности по кредитному договору не направит, а обратит в свою пользу, при этом с целью замены сведений о должнике осуществила неправомерный доступ к охраняемой законом компьютерной информации, что повлекло ее модификацию без разрешения на то собственника (законного владельца) системы.

¹⁴² Хисамова З. И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. 2018. № 9. С. 44.

¹⁴³ Приговор по уголовному делу № 1-233-36/2020 // Ленинский районный суд г. Мурманска : офиц. сайт. URL: http://lensud--krs.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=156511389&case_uid=01f90cd7-fe7b-4b82-9d03-01b4818dfb03&delo_id=1540006 (дата обращения: 08.02.2025).

Основными мотивами совершения неправомерного доступа к компьютерной информации выступают корыстные побуждения (получение материальной выгоды), личная неприязнь к собственнику информации, вымогательство или мошенничество, хулиганство, вандализм (разрушение информационных систем, атаки на технические средства и пр.), шпионаж (например, получение сведений экономической направленности, данных о личной жизни и пр.).

Личность потерпевшего и предмет посягательства. Предметом неправомерного доступа к компьютерной информации являются охраняемые законом сведения (под которыми понимаются данные о лицах, предметах, фактах, событиях, явлениях и процессах), находящиеся на носителе информации, в компьютере, системе компьютеров или их сети¹⁴⁴ в форме электрических сигналов. Нематериальный характер компьютерной информации не может выступать веским аргументом в пользу отрицания возможности ее рассмотрения в качестве предмета неправомерного доступа по смыслу ст. 272 УК РФ¹⁴⁵.

Потерпевший, как правило, является владельцем (пользователем) технического средства или информационной системы, в отношении которых осуществлен неправомерный доступ к компьютерной информации, лицом, сведения о котором обрабатываются в информационной системе, либо лицом, правам и законным интересам которого причинен вред определенного характера.

Потерпевших по преступлениям, связанным с неправомерным доступом к компьютерной информации, можно также разделить на категории в зависимости от принадлежности к физическим или юридическим лицам. Типичной жертвой среди физических лиц является пользователь сети «Интернет», который не обладает знаниями в области информационной безопасности, активный пользователь интернет-сервисов, в частности, банковских, в возрасте от 25 до 64 лет, а также коммерческие организации, не обеспечивающие усиленные меры по защите эксплуатируемых ими ресурсов в сети «Интернет».

Так, из-за разногласий с представителем работодателя гражданка осуществила неправомерный доступ к охраняемой законом компьютерной информации на сайте организации, имея возможность доступа к сетевым ресурсам, удалила с официального сайта сведения об оказываемых организацией услугах, после чего совершила вышеуказанные действия на официальной странице

¹⁴⁴ Клепицкий И. А. Комментарий к Уголовному кодексу Российской Федерации (постатейный). М. : РИОР ИНФРА-М, 2019. С. 556.

¹⁴⁵ Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография. М. : ИНФРА-М, 2022. С. 184.

организации в социальной сети «ВКонтакте» (произвела изменение информации, переименовала страницу, осуществила изменение наименования аккаунта и логотипа организации, ограничила доступ к странице, отвязала абонентский номер организации, привязав номер, оформленный на нее, создала в социальной сети аналогичную группу с иным сетевым адресом), таким образом, осуществила модификацию компьютерной информации, что потенциально могло нанести как репутационный так и экономический ущерб организации¹⁴⁶.

Исходя из анализа сложившейся за последние несколько лет следственной и судебной практики необходимо отметить отличительные особенности личности потерпевшего. Как правило, основными чувствами и эмоциями, которые испытывают потенциальные жертвы, являются любопытство, жадность, жалость или страх, способные отключить объективное восприятие действительности, критическое мышление и логику.

Дополняют перечисленные такие факторы как безотлагательность действий, диктуемых преступником, чувство раздражения или оказание давления собственным авторитетом, что в совокупности усиливает манипуляционный эффект. В протоколах допроса потерпевших часто фигурируют фразы «Все было как в тумане», «сам(а) не понял(а), как все произошло», «сделал(а) все на автомате» и пр. Таким образом, в ряде случаев осуществляется вовлечение в совершение преступления с применением психологических манипуляций, склоняющих, например, к разглашению уникального кода для осуществления несанкционированного доступа к ресурсу или к самостоятельной загрузке программного обеспечения, позволяющего удаленно управлять устройством жертвы.

Характерной особенностью потерпевших является их бездействие или неохотное желание сообщать о преступлении в правоохранительные органы, что обуславливается предположением о низкой вероятности раскрытия преступления. Потерпевшие часто не могут предоставить минимально необходимые данные и доказательства для создания полноценной картины расследования (параметры входа в сеть, учетные данные и пр.)¹⁴⁷, что является следствием пока еще низкого уровня просвещенности населения в области информационно-

¹⁴⁶ Приговор по уголовному делу № 1-250/2024 // Советский районный суд г. Томска : офиц. сайт. URL: https://sovetsky--tms.sudrf.ru/modules.php?name=sud_delo&srv_num=1&nameop=doc&number=11138974&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

¹⁴⁷ Харисова З. И. Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» // Вестник Уфимского юридического института МВД России. 2019. № 3 (85). С. 95.

телекоммуникационных технологий.

Часто потерпевший использует условно бесплатное программное обеспечение или программы, в которых настроен обход контроля лицензий, что зачастую сопровождается внедрением в них дополнительного функционала для несанкционированного доступа к устройству пользователя.

Стоит также отметить, что исследование уголовных дел показало массовость и идентичность совершаемых преступлений рассматриваемого вида, которые редко организуются единолично. Часто правоохранительные органы имеют дело с повторяющимися, детально подготовленными преступлениями со сложным и многоступенчатым механизмом, что может осуществляться только организованными преступными группами¹⁴⁸, включающими: организатора преступной группы; специалистов в области информационных технологий и программирования; лиц, обладающих компетенциями в области компьютерных технологий, эксплуатации компьютеров и иных технических средств, а также электронных кошельков с целью последующего перевода на них денежных средств; лиц, осуществляющих снятие наличных денежных средств со счетов или в банкоматах¹⁴⁹.

Потерпевшими среди юридических лиц обычно являются организации финансового сектора, преимущественно занимающиеся электронной коммерцией, оказывающие телекоммуникационные услуги или услуги образования.

Кроме того, крупные компании и корпорации не желают сообщать в правоохранительные органы о совершенных преступлениях в связи с действующей репутационной политикой, боязни раскрытия механизма обеспечения информационной безопасности и функционирования систем защиты информации на предприятии¹⁵⁰.

¹⁴⁸ Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. Указ. соч. С. 63.

¹⁴⁹ Антонян Е. А., Россинская Е. Р., Клещина Е. Н. Обзор правоприменительной практики по противодействию киберпреступлений. М. : Консорциум «Инновационная юриспруденция», 2024. С. 85.

¹⁵⁰ Россинская Е. Р. Криминалистика. М. : Норма ИНФРА-М, 2021. С. 444.

1.2.2. Криминалистическая характеристика незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а равно создания и (или) обеспечения функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения

Дополнение в декабре 2024 года УК РФ статьей 272.1¹⁵¹, устанавливающей ответственность за незаконные использование, хранение, передачу и сбор информации, содержащей персональные данные, а также создание и обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и распространения, обусловлено тем, что совершенствование технологий и современные потребности общества, подвергшегося цифровизации, делают необходимой автоматизированную обработку значительных по объему массивов личных данных граждан.

Формируемые государственными органами и коммерческими организациями базы данных с указанными сведениями становятся специфическим предметом преступных посягательств, что подтверждает сложившаяся международная ситуация, отчасти связанная с деятельностью транснациональных организованных преступных групп, нацеленных на хищение персональных данных, их неправомерное использование и распространение. Введение новой статьи в главу 28 УК РФ в первую очередь было связано с существенным ростом противоправных действий в отношении персональных данных¹⁵², фактами незаконного использования конфиденциальной информации при совершении преступлений в сфере компьютерной информации, а также тем, что наказание, предусмотренное законом за такого рода преступления, было несопоставимо их потенциальным общественно опасным последствиям. Так, только из финансовых организаций за 2024 год объем утечек персональных данных составил 410 млн. строк, что более чем в 2,5 раза больше объема утечек, выявленных в 2023 году¹⁵³. Указанные сведения преимущественно содержали информацию об учетных данных клиентов,

¹⁵¹ О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 30 ноября 2024 г. № 421-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_491931/#dst100011 (дата обращения: 28.03.2025).

¹⁵² Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 года и ожидаемые тенденции ее развития. Указ. соч. С. 56.

¹⁵³ Аналитический отчет «Кибератаки на финансовый сектор в 2024 году» // Акционерное общество «Солар секьюрити» : офиц. сайт. URL: <https://rt-solar.ru/analytics/reports/5206> (дата обращения: 28.03.2025).

их адресах, контактных номерах, электронных адресах, кредитной истории и т. п., что использовалось для дальнейшего совершения различного рода преступлений и мошенничеств. Поскольку рост противоправных деяний в отношении персональных данных является значимым фактором самовоспроизводства киберпреступлений целесообразно рассмотрение возможностей оптимизации процесса расследования преступлений, связанных с незаконным использованием, передачей, сбором и хранением компьютерной информации, содержащей персональные данные, в частности, изучение элементов, входящих в их криминалистическую характеристику¹⁵⁴.

Стоит отметить, что обоснование структуры криминалистической характеристики преступлений может быть исключительно на основе эмпирических данных, по этой причине строится лишь общая (вероятностная) криминалистическая характеристика на основе теоретико-прогностического подхода, что обусловлено отсутствием на текущий момент судебной практики по применению данной новеллы в достаточном количестве. Ввиду того, что следственная и судебная практика по ст. 272.1 УК РФ на сегодняшний день лишь начала формироваться, был проведен дополнительный анализ смежных по составу уголовных дел¹⁵⁵, например, в соответствии со ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», а также ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», исключительно в отношении персональных данных, который позволил выявить вероятностные элементы криминалистической характеристики рассматриваемых преступных деяний. Это объясняется тем, что отсутствие практики применения указанной нормы (в достаточном количестве) может осложнить проведение анализа взаимосвязанности элементов криминалистической характеристики преступления, что, соответственно, снизит точность формируемой в пятой главе настоящей работы информационной модели.

Под персональными данными подразумевается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, то есть субъекту персональных данных¹⁵⁶.

¹⁵⁴ Харисова З. И. Криминалистическая характеристика незаконного использования, передачи, сбора и хранения компьютерной информации, содержащей персональные данные // Сибирские уголовно-процессуальные и криминалистические чтения. 2025. № 2. С. 98.

¹⁵⁵ Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Указ. соч. С. 39.

¹⁵⁶ О персональных данных : Федеральный закон № 152-ФЗ от 27 июля 2006 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_61801 (дата обращения: 08.02.2025).

К указанным данным, например, могут относиться: фамилия, имя и отчество субъекта персональных данных (физического лица); дата и место его рождения; реквизиты документов; контактный телефон и адрес электронной почты (в связке с определяемым субъектом); семейное и социальное положение; образование; профессия; сведения о доходах и пр. информация. Любое действие (операция) или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, определяется как обработка таких данных¹⁵⁷.

Под специальными персональными данными понимают данные, касающиеся расовой и национальной принадлежности, политических, религиозных либо философских убеждений, состояния здоровья субъекта персональных данных, его интимной жизни, а также данные о судимости¹⁵⁸. Биометрическими персональными данными являются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность. В соответствии с ч. 2 ст. 272.1 УК РФ за совершение неправомерных действий в отношении специальных и биометрических персональных данных предусмотрена повышенная уголовная ответственность. Под трансграничным перемещением носителей информации понимается совершение действий по ввозу на территорию РФ и (или) вывозу с ее территории носителя, на который осуществлены запись и хранение такой информации, под трансграничной передачей компьютерной информации понимают передачу персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу¹⁵⁹.

Под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272.1 УК РФ, понимается возможность неправомерного доступа к персональным данным, возникшего в результате выполняемой работы (по трудовому, гражданско-правовому договору и пр.) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует персональные данные и средства их обращения.

¹⁵⁷ Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» : комментарий. М. : Статут, 2017. С. 11.

¹⁵⁸ Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р. Защита персональных данных в организации : монография. М. : Флинта, 2021. С. 58.

¹⁵⁹ Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет : монография / под ред. А. С. Дупан. М. : Изд. дом Высшей школы экономики, 2018. С. 35.

Создание информационного ресурса представляет собой деятельность, направленную на разработку веб-сервиса, либо информационной системы, заведомо предназначенных для незаконного хранения и передачи компьютерной информации, содержащей персональные данные, полученных незаконным путем. Лицо может быть подвергнуто уголовному преследованию за вышеуказанные действия только при условии, что оно достоверно знало об их направленности в плане функционирования веб-ресурса или информационной системы, заведомо предназначенных для незаконной обработки компьютерной информации, содержащей персональные данные. Действие настоящей статьи не распространяется на случаи обработки рассматриваемых данных лицами исключительно для личных и семейных нужд. Выявление незаконного способа завладения персональными данными в электронном виде и незаконных действий, связанных с их распространением, является ключевым условием наступления ответственности, предусмотренной ст. 272.1 УК РФ.

Способ совершения преступления. Среди основных преднамеренных способов незаконного использования и (или) передачи, сбора и (или) хранения персональных данных, создания и (или) обеспечения функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения можно отметить: преодоление систем защиты в виде хищения учетных данных пользователей с целью получения персональных данных; использование несовершенств информационных систем персональных данных; выявление уязвимостей программного обеспечения и операционных систем, эксплуатирующих информационные системы персональных данных; несанкционированное подключение к техническим средствам, а также вспомогательному компьютерному оборудованию, эксплуатирующего систему; сбор и дальнейшее распространение данных, в связи с утечками персональных данных¹⁶⁰; приобретение баз данных, содержащих персональные данные; неправомерный доступ к средствам обработки персональных данных, их хранения или иного вмешательства в их функционирование; организация и обеспечение функционирования программного обеспечения, веб-ресурсов и информационных систем, предназначенных для незаконной обработки персональных данных (распространения, предоставления, доступа); фишинг¹⁶¹ (создание поддельных

¹⁶⁰ Сервис проверки данных на предмет скомпрометированности // Национальный координационный центр по компьютерным инцидентам Федеральной службы государственной статистики : офиц. сайт. URL: <https://chk.safe-surf.ru> (дата обращения 30.03.2025).

¹⁶¹ Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. Т. 14. № 5. С. 703.

(фишинговых) ресурсов, документов или сообщений для несанкционированного сбора персональных данных); веб-скрейпинг (от англ. «web scraping» – автоматизированный сбор данных с веб-ресурсов или социальных сетей); взлом и незаконный сбор персональных данных, размещенных в облачных системах хранения данных; доксинг (от англ. «doxing» и сокращения «docs» – сбор и распространение личной информации о человеке без его согласия); трансграничное перемещение носителей информации (ввоз на территорию РФ или вывоз за пределы страны) носителей, на которые осуществлена запись и хранение персональных данных); незаконная передача защищаемых персональных данных на территорию иностранного государства.

Примером незаконного сбора, хранения и распространения персональных данных может служить уголовное дело, согласно материалам которого преступники, предвидя неизбежность незаконного копирования и распространения данных, из корыстной заинтересованности, а именно, в стремлении незаконно обогатиться с целью предоставления сторонним лицам конфиденциальных сведений о гражданах, создали информационный ресурс в сети «Интернет» (обеспечив его функционирование), заведомо предназначенный для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные граждан¹⁶².

В качестве примера несанкционированного подключения непосредственно к информационным системам персональных данных можно привести уголовное дело в отношении работника организации, который действуя в нарушение должностной инструкции, используя свое служебное положение и возможность доступа к сведениям, содержащимся в информационной системе, использовал личные учетные данные (достоверно зная порядок и условия внесения изменений в базу данных организации, предусмотренные внутренними документами), осуществлял неправомерный доступ к информации, принадлежащей организации и содержащей персональные данные граждан, неоднократно модифицируя базу данных системы в личных целях¹⁶³.

Процессы, возникшие в ходе случайных действий либо стечения обстоятельств, относят к непреднамеренным.

¹⁶² Приговор по уголовному делу № 1-239/2025 // Ленинский районный суд г. Владимира : офиц. сайт. URL: https://leninsky--wld.sudrf.ru/modules.php?name=sud_delo&name_op=r_juid&vnkod=33RS0001&srv_num=1&delo_id=1540006&case_type=0&judicial_uid=77RS0023-02-2025-010692-87 (дата обращения: 20.10.2025).

¹⁶³ Приговор по уголовному делу № 1-103/2024 // Октябрьский городской суд Республики Башкортостан : офиц. сайт. URL: http://oktabrsky--bkr.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=147445045&case_uid=aec2f93c-2992-4d83-99a9-dc95e9804546&del_o_id=154_0006 (дата обращения: 08.02.2025).

К неумышленным способам незаконного использования, передачи, сбора и хранения персональных данных, а также создания и обеспечения функционирования ресурсов для их незаконного распространения можно отнести незащищенную передачу данных (например, через незащищенные каналы связи без шифрования или несертифицированное программное обеспечение); использование общедоступных облачных хранилищ персональных данных; ошибки администрирования информационных систем персональных данных (неправильная настройка доступа без разграничения ролей и пр.); потеря или кража технического средства или его компонента (например, ноутбука или электронного носителя информации с персональными данными); использование веб-аналитики и трекеров действий пользователей веб-ресурсов без их согласия. Так, при непосредственном доступе ими могут выступать носители информации, эксплуатируемые с техническими средствами, а при опосредованном доступе – сетевое оборудование и средства доступа к информационной системе персональных данных (средства вычислительной техники, мобильные средства связи и пр.).

К основным средствам также относится: программное обеспечение (например, сервисы «VPN», обеспечивающие шифрование трафика и сокрытие реального IP-адреса преступника, системы прокси-серверов и пр.), в том числе криптографическое и вредоносное, способное к распространению в локальных информационных системах и служащих в целях выполнения какого-либо деструктивного действия (удаление, блокирование или изменение файлов) или несанкционированного копирования данных; программное обеспечение для веб-парсинга в виде настраиваемых скриптов для кражи данных из социальных сетей и подобных ресурсов и скрытого наблюдения, сбора персональных данных с компьютеров и мобильных устройств, способного перехватывать совокупность действий пользователей (нажатия клавиш, записей звонков и сбора конфиденциальных данных); сетевые снифферы (анализатор сетевого трафика, содержащего персональные данные); поисковые системы, позволяющие находить подключенные к сети устройства и сервисы; теневые маркетплейсы для распространения персональных данных и пр.

Примером задействования различных технических средств и программ при совершении рассматриваемого преступного деяния может выступить уголовное дело в отношении гражданина, использующего принадлежащий ему мобильный телефон с предустановленным на нем VPN-сервисом и осуществившего

неправомерный сбор персональных данных в корыстных целях¹⁶⁴. Согласно материалам, преступник приобрел в сети «Интернет» данные для авторизации пользователя на «Едином портале государственных и муниципальных услуг» (справочно-информационном интернет-портале «Госуслуги»), осуществил неправомерный доступ к охраняемой законом компьютерной информации, а именно, к персональным данным потерпевшего. С учетной записи личного кабинета пользователя было направлено заявление на получение заемных денежных средств, при заполнении которого преступник использовал имеющиеся в учетной записи личного кабинета потерпевшего персональные данные (фамилию, имя и отчество, контактный телефон, адрес электронного почтового ящика, адрес проживания, реквизиты документа, удостоверяющего личность, ИНН, СНИЛС).

К средствам хранения компьютерной информации в виде персональных данных относятся ее материальные носители (жесткие и оптические диски, USB-накопители, карты памяти и т. п.), средствами обработки персональных данных в целом служит вычислительное устройство (процессор) компьютера. Каналы передачи информации могут быть проводными и беспроводными.

Основными способами сокрытия следов незаконного использования и (или) передачи, сбора и (или) хранения персональных данных, создания и (или) обеспечения функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения, являются: использование средств анонимизации и систем прокси-серверов, которые позволяют устанавливать анонимные сетевые соединения с туннелированием; очищение журналов и шифрование событий в системе; удаление сведений о подключениях к компьютеру или информационной системе персональных данных; использование чужих, временных или и одноразовых учетных записей для доступа к персональным данным; использование программных средств анонимизации в целях подмены IP-адресов устройств и абонентских номеров, размещение ресурсов персональных данных для их последующего распространения в неиндексируемой глубокой сети (от англ. «deep web» – глубокий «Интернет») и сети даркнет (от англ. «dark web» – темный «Интернет»); корректировка даты и времени доступа к персональным данным для дальнейшего незаконного их распространения и пр.

Типичными следами неправомерного доступа к компьютерной информации в общем случае являются: цифровые (установленное программное обеспечение,

¹⁶⁴ Приговор по уголовному делу № 1-8/2024 // Ленинский районный суд г. Саранска Республики Мордовия : офиц. сайт. URL: https://leninsky--mor.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=131817209&case_uid=d1943dd0-9e60-434d-ae7c-ad5096407646&delo_id=1540006 (дата обращения: 08.02.2025).

используемое для незаконной обработки или хранения персональных данных, изменения в конфигурации операционной системы устройства, журналы подключений к компьютеру или информационной системе персональных данных, модифицированные или заблокированные файлы данных и т. п.), а также материальные следы на компьютерной периферии.

Типичные следы по рассматриваемым преступлениям могут быть обнаружены в системном и прикладном программном обеспечении и в поименованных областях записей на носителях информации (например, на носителях серверного оборудования с размещаемыми на нем ресурсами информационной системы персональных данных). Так, по материалам уголовного дела, для доступа к информационному ресурсу в сети «Интернет», заведомо предназначенному для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные граждан, использовалась специализированная программная оболочка через веб-форму и API-интерфейс (от англ. «application programming interface» – набор инструкций для установления взаимодействия различных приложений и сервисов)¹⁶⁵.

Цифровые следы при этом могут опосредованы с электронными файлами; компьютерами, информационными системами, мобильными средствами связи; базами данных; электронными ключами (подписями); файлами подкачки и временными файлами, образующимися в процессе функционирования операционной системы; сетевым трафиком; идентификаторами в сети передачи данных (например, IP-адреса устройств или MAC-адреса их сетевых карт), DNS-адресами; реестрами операционных систем и журналов событий эксплуатации информационной системы персональных данных; цифровыми финансовыми активами и электронными кошельками; используемыми при приобретении баз данных с персональными данными и пр. Отдельно стоит отметить ресурсы, предназначенные для поиска персональных данных по открытым источникам (OSINT-разведка (от англ. «open source intelligence – разведка по открытым источникам¹⁶⁶)) в индексируемой сети «Интернет»,

¹⁶⁵ Приговор по уголовному делу № 1-239/2025 // Ленинский районный суд г. Владимира : офиц. сайт. URL: https://leninsky--wld.sudrf.ru/modules.php?name=sud_delo&name_op=r_juid&vnkod=33RS0001&srv_num=1&delo_id=1540006&case_type=0&judicial_uid=77RS0023-02-2025-010692-87 (дата обращения: 20.10.2025).

¹⁶⁶ Белей А. В. Необходимость анализа трендов киберпреступлений и осуществления OSINT для эффективного проведения СКТЭ // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции. М. : Российский государственный университет правосудия, 2021. С. 98.

неиндексируемой глубокой сети и даркнете, а также по ресурсам Telegram-ботов (аккаунтам в кроссплатформенном мессенджере «Telegram», которые программируются на автоматическое совершение действий, например, связанных с незаконным сбором и обработкой персональных данных). Кроме того, развитие метавселенных порождает такие виды преступных деяний, как подмена личных данных, кража цифровых идентификаторов личности и т. п. По вышеуказанным преступным деяниям следы могут представлять собой, например, сфальсифицированные биометрические данные, метаданные и конфигурации серверов, связанных с эксплуатацией метапространства (журналы функционирования программ, обеспечивающих визуализацию виртуальных пространств и аутентификацию по биометрическим данным, реестры эксплуатации децентрализованных сетей, конфигурации с настройками протоколов передачи данных, сетевые адреса взаимодействия цифровых аватаров и пр.).

Вероятными местами расположения типичных следов незаконной обработки, хранения или распространения персональных данных в цифровом виде являются носители информации, серверное оборудование дата-центров и облачные хранилища, в том числе файлы и каталоги хранения данных, файлы конфигурации программ удаленного доступа и пр. Так из приговора по уголовному делу, связанного с созданием информационных ресурсов, предназначенных для незаконного хранения и распространения информации, содержащей персональные данные с помощью Telegram-бота, следует, что у основателя запрещенного ресурса были изъяты технические средства с изобличающей электронной перепиской, а также серверное оборудование дата-центра с накопителями общим объемом 40 терабайт данных¹⁶⁷.

Распространенность преступного деяния выражается в установлении факта схожести эпизода на основе полученных сведений об использовании в преступной схеме способа совершения преступления. Так, признаками схожести могут выступить идентичные реквизиты в виде: любых идентифицирующих конкретного гражданина персональных данных, в том числе биометрических; абонентских номеров; программного обеспечения и технических средств, используемых для совершения атак на информационную систему персональных данных или компьютеры, обрабатывающие персональные данные; банковских реквизитов и т. п. Также необходимо отметить массовость утечек данных, при которых число пострадавших лиц могут измеряться миллионами записей.

¹⁶⁷ Приговор по уголовному делу № 3/1-0338/2025 // Официальный портал судов общей юрисдикции города Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/rs/tverskoj/services/cases/criminal-materials/details/5187dbb0-b6fb-11f0-8e85-6d57f7d43af6> (дата обращения: 01.11.2025).

Обстановка совершения преступления. Незаконное использование и (или) передача, сбор и (или) хранение персональных данных, создание и (или) обеспечение функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения предполагает как непосредственный доступ к персональным данным (преимущественно в момент отсутствия обладателя или пользователя, имеющего на доступ к защищаемой информации законные права), так и удаленный с любой точки мира (при наличии подключения к сети «Интернет» или к локальной сети предприятия), которые определяются спецификой работы с указанными данными в электронном виде и предполагают использование программно-аппаратных средств, либо информационных систем персональных данных, обеспечивающих обработку, хранение и передачу конфиденциальных сведений. Так, работник организации сформировал преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации (сведениям о факте обращения потерпевшего за оказанием медицинской помощи в медицинские учреждения, состоянии его здоровья, поставленных диагнозах, а также иных сведений, полученных при медицинских обследованиях и лечении, содержащихся в информационной системе медицинской организации). С целью реализации задуманного работник организации без служебной необходимости и вопреки исполняемым служебным обязанностям, с целью неправомерного доступа к конфиденциальным сведениям в виде персональных данных, в момент отсутствия стороннего пользователя, имеющего на доступ к защищаемой информации законные права, вошел под учетной записью коллеги (не осведомленного о преступном характере предпринимаемых действий), в результате чего получил неограниченный доступ к персональным данным и сведениям о пациентах медицинских учреждений, составляющим врачебную тайну, нарушив этим права граждан на неприкосновенность частной жизни¹⁶⁸.

Местами совершения указанного преступления являются: компьютеры, серверы или информационные системы персональных данных (зачастую значительно удаленные друг от друга), так и локальные территории, учреждения и организации, в которых эксплуатируются системы; социальные сети и мессенджеры; фишинговые сайты; теневые торговые площадки и форумы, где продаются базы данных, содержащие персональные данные; IoT-устройства (от

¹⁶⁸ Приговор по уголовному делу № 1-243/2024 // Оренбургский районный суд Оренбургской области : офиц. сайт. URL: https://orenburgsky--orb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=265996474&case_uid=b8b16dc1-0cd8-4f1e-b828-2e411e9f587d&delo_id=1540006 (дата обращения: 08.02.2025).

англ. «internet of things (IoT)» – Интернет вещей) и серверы-хранилища видеоданных; незащищенные беспроводные сети.

В целях сокрытия физического расположения преступника удаленный доступ нередко осуществляется из общественных мест, предоставляющих сеть «Интернет» в порядке пользования услугами на базе организации. В подавляющем большинстве случаев местом (средой) совершения рассматриваемого преступления является киберпространство ввиду его распространенности среди населения, реже – метaproстранство, блокчейн (распределенные реестры), либо гибридные инфраструктуры (распределенные облачные системы хранения данных и пр.). Временем совершения преступления признается время окончания преступного деяния вне зависимости от момента наступления последствий. Время доступа к компьютерам, программному обеспечению или информационной системе персональных данных, хранящим конфиденциальные данные, может быть изменено преступником в целях искажения типичных следов.

Личность преступника. Как правило, лицо, осуществляющее незаконные использование, передачу, сбор или хранение персональных данных, обладает глубокими знаниями в области информационных технологий, включая сетевую безопасность, методы обхода систем защиты информационной системы персональных данных. Указанные лица стабильно отслеживают методы защиты данных, мониторят уязвимости программного обеспечения, адаптируя имеющиеся знания к новым условиям функционирования программ или конкретным жертвам, часто пренебрегают правовыми и этическими нормами, не учитывая последствия своих действий для пострадавших и общества в целом. Многие из них обладают навыками социальной инженерии, позволяющими обманом получать доступ к конфиденциальной информации от пользователей или сотрудников организаций.

Анализ уголовных дел также показывает, что преступники часто используют информацию из открытых источников, а также сведения, ставшие известными в результате утечки данных из баз данных различных веб-сервисов¹⁶⁹. Отличительной особенностью является то, что они не проявляют сочувствия к жертвам преступлений, рассматривая их лишь как средства достижения собственных целей, как правило, имеют высшее или среднее инженерно-техническое образование и (или) обладает устойчивыми навыками работы с техническими средствами и программным обеспечением. Совершаемые ими преступления часто носят серийный характер и сопровождаются тщательными

¹⁶⁹ Приговор по уголовному делу № 3/1-0338/2025 // Официальный портал судов общей юрисдикции города Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/rs/tverskoj/services/cases/criminal-materials/details/5187dbb0-b6fb-11f0-8e85-6d57f7d43af6> (дата обращения: 01.11.2025).

действиями по сокрытию следов преступной деятельности. Отдельной категорией являются лица, имеющие доступ к персональным данным граждан в связи с исполнением ими служебных обязанностей по месту работы, которые оказывают услуги информирования иных лиц. Основными мотивами совершения указанного преступления выступают корыстные побуждения в виде получения материальной выгоды, получаемой посредством продажи полученных персональных данных¹⁷⁰, вымогательство или мошенничество, а также личная неприязнь к собственнику информации, шпионаж (например, получение сведений, связанной с личной жизнью) и пр. Так, в материалах одного из изученных приговоров были представлены сведения по факту незаконного сбора и передачи сотрудником больницы информации, содержащей персональные данные пациента, в том числе об обращениях за медицинской помощью и диагнозе¹⁷¹. Находясь в кабинете врача, будучи лицом, не имеющим доступа к данным, содержащимся в информационной системе персональных данных, эксплуатируемой в организации, сфотографировал на камеру мобильного телефона конфиденциальные сведения с экрана монитора компьютера, незаконно совершив сбор информации, отнесенной к категории персональных данных пациента, к которому обвиняемый испытывал личную неприязнь. После чего работник распространил информацию об обращениях пациента за медицинской помощью и диагнозе путем направления изготовленного фотоизображения третьим лицам в сервис мгновенного обмена сообщениями.

Личность потерпевшего и предмет посягательства. Предметом рассматриваемого преступления является компьютерная информация, содержащая персональные данные, полученная незаконным путем, включая неправомерный доступ к средствам обработки или хранения данных, вмешательство в функционирование таких средств и прочие незаконные способы. Персональные данные в данном контексте включают любую информацию, относящуюся к определенному или определяемому физическому лицу.

Особо выделяются при этом данные о несовершеннолетних лицах, специальные категории персональных данных (сведения о расовой или этнической принадлежности, политических взглядах, состоянии здоровья, интимной жизни и пр.) и биометрические данные.

¹⁷⁰ Приговор по уголовному делу № 10-17703/2025 // Официальный портал судов общей юрисдикции города Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/mgs/services/cases/appeal-criminal/details/03273280-782c-11f0-bc99-8d8541b34621> (дата обращения: 01.09.2025).

¹⁷¹ Приговор по уголовному делу № 1-154-0006/2025 // Артемовский районный суд Свердловской области : офиц. сайт. URL: https://artemovsky--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=r&delo_id=1540006 (дата обращения: 08.02.2025).

Потерпевший – физическое лицо, к которому прямо или косвенно относятся персональные данные, либо организация, в которой функционирует информационная система персональных данных, в отношении которых осуществлены незаконное использование и (или) передача, сбор и (или) хранение персональных данных, создание и (или) обеспечение функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения. Потерпевших по данным преступлениям можно также разделить на категории в зависимости от принадлежности к физическим или юридическим лицам. Исходя из анализа сложившейся за последние несколько лет следственной и судебной практики, связанной со сбором, хранением, использованием и распространением информации о частной жизни лица без его согласия необходимо отметить отличительные особенности личности потерпевшего по рассматриваемому виду преступления. Потерпевшим, как правило, является физическое лицо, конкретный гражданин, чьи данные были собраны или распространены без его согласия, это могут быть, например, клиенты банков, пациенты медицинских учреждений, работники организаций, а также публичные лица, чьи данные представляют интерес для злоумышленников.

Довольно часто потерпевший сам предоставляет свои персональные данные на фишинговых ресурсах, что объясняется отсутствием знаний в области защиты рассматриваемых данных. Таким образом, частым признаком, выявляемым в ходе следствия, является пассивная роль потерпевшего при совершении преступления, так, потерпевший часто не подозревает о незаконном сборе персональных данных до момента их использования. Ключевым признаком также является то, что субъект персональных данных не давал согласия на обработку сведений о нем, однако в результате преступного деяния ему причинен материальный или репутационный ущерб. Характерной особенностью потерпевших является их бездействие или неохотное желание сообщать о факте преступного деяния в правоохранительные органы. Кроме того, потерпевшие зачастую не могут предоставить минимально необходимые данные и электронные доказательства для создания картины расследования. Юридические лица часто не желают сообщать в правоохранительные органы об утечках данных из эксплуатируемых ими информационных систем персональных данных в связи с действующей репутационной политикой. Судебная практика по незаконному использованию и (или) передаче, сбору и (или) хранению персональных данных, созданию и (или) обеспечению функционирования ресурсов для их незаконного хранения и (или) распространения показывает, что потерпевшими по такого рода преступлениям могут быть лица любого возраста, профессии и социального статуса.

1.2.3. Криминалистическая характеристика создания, использования и распространения вредоносных компьютерных программ

Вредоносное программное обеспечение все чаще становится инструментом преступников для осуществления несанкционированного доступа к охраняемой законом информации, кражи персональных данных граждан, вымогательства, шпионажа, атак на государственные структуры. В условиях повсеместной цифровизации создание, использование и распространение вредоносного программного обеспечения может нанести значительный ущерб экономической жизни общества, например, при внедрении в банковские приложения¹⁷², а в отдельных случаях причинить вред здоровью различной тяжести и смерти людей, например, при внедрении в информационные системы персональных данных, эксплуатируемые в медицинских учреждениях и т. п.

Вредоносное программное обеспечение – форма представления совокупности данных и команд, обеспечивающих функционирование компьютера, либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации¹⁷³. Способом совершения данного преступления является действие, выраженное в виде создания вредоносного программного обеспечения, а равно использования или распространения такого программного обеспечения либо иной компьютерной информации. Под созданием вредоносных программ подразумевается результат деятельности, выразившейся в представлении в объективной форме совокупности данных и команд, предназначенных для функционирования информационно-телекоммуникационной сети либо компьютера с целью уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также с целью нарушения работы указанной сети. Действия, направленные на создание вредоносной программы, не доведенные до конца по причинам, не зависящим от воли виновного, могут быть квалифицированы как покушение на преступление.

¹⁷² Харисова З. И. Криминалистическая характеристика создания, использования и распространения вредоносных компьютерных программ // Вестник Балтийского федерального университета им. И. Канта. Серия: гуманитарные и общественные науки. 2025. № 2. С. 20.

¹⁷³ Классификация и типы вредоносного программного обеспечения // Акционерное общество «Лаборатория Касперского» : офиц. сайт. URL: <https://www.kaspersky.ru/resource-center/threats/malware-classifications> (дата обращения: 18.03.2025).

Распространение предполагает как возмездную, так и безвозмездную передачу программного обеспечения либо вредоносной информации или электронного носителя информации с его содержанием. Использование программ либо вредоносной информации имеет место при их внедрении в компьютер или информационную систему независимо от того, повлекло ли это последствия, поскольку преступление окончено в момент совершения соответствующих действий.

Рассматриваемое преступление имеет некоторые общие черты с несанкционированным доступом к компьютерной информации. Сложность разграничения этих составов преступлений заключается в том, что и неправомерный доступ к компьютерной информации, и создание, использование и распространение вредоносного программного обеспечения ведут к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нейтрализации средств защиты информации. Между тем они имеют много отличий. Так, предметом создания, использования и распространения вредоносных программ является любая информация, содержащаяся на электронном носителе информации или в информационно-телекоммуникационных сетях, предметом преступления, предусмотренного ст. 272 УК РФ, является только та информация, которая охраняется законом. Следует иметь в виду, что, когда вредоносное программное обеспечение использовалось для осуществления неправомерного доступа к компьютерной информации и это повлекло наступление последствий, предусмотренных ч. 1 ст. 272 УК РФ (что встречается достаточно часто), действия лица подлежат квалификации по совокупности преступлений, предусмотренных соответствующими частями статей 272 и 273 УК РФ.

Способ совершения преступления. Среди основных способов создания вредоносного программного обеспечения можно отметить: написание исходного кода на языке программирования с использованием вредоносных алгоритмов; модификацию легального программного обеспечения¹⁷⁴ с внедрением вредоносного функционала в виде бэкдоров (от англ. «backdoor» – лазейка); использование специализированных сервисов в виде автоматизированных МaaS-конструкторов (от англ. «malware-as-a-service (MaaS)» – вредоносное программное обеспечение, предоставляемое в виде услуги), позволяющих

¹⁷⁴ Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования. Указ. соч. С. 702.

создавать программы без глубоких знаний в области информационных технологий; создание новой вредоносной версии программного проекта с открытым исходным кодом путем форкинга (от англ. «forking» – ветвление); создание программного обеспечения, которое использует уязвимости в легальном программном обеспечении для распространения вредоносных функций в виде эксплойта (от англ. «exploit» – эксплуатировать); внедрение буткитов (от англ. «boot» – загрузка и «kit» – набор инструментов – комплекс вредоносного программного обеспечения, которое изменяет сигнатуру исходного кода для уклонения от обнаружения антивирусами); генерация адаптивного вредоносного кода с использованием алгоритмов искусственного интеллекта и пр. Ввиду того, что непосредственное создание вредоносных программ требует знаний в области программирования, кибербезопасности и эксплуатации уязвимостей, довольно часто преступники прибегают к приобретению готовых вредоносных продуктов на теневых площадках сети даркнет.

Среди основных способов использования вредоносного программного обеспечения можно выделить: сбор конфиденциальных данных в целях кибершпионажа; шифрование данных; создание ботнетов для заражения компьютеров (например, для организации DDoS-атак, несанкционированного копирования компьютерной информации и пр.); рассылку спама или криптоджекинг (майнинг криптовалют); SQL-инъекции; компрометацию систем безопасности (установка бэкдоров для несанкционированного доступа и пр.); создание ресурсов с использованием вредоносных скриптов; деструктивное воздействие вредоносного программного обеспечения на информацию или техническое средство (уничтожение данных, вывод из строя информационной инфраструктуры); нейтрализацию средств защиты информации; обход лицензий программного обеспечения и антивирусов; воздействие вредоносного программного обеспечения на объекты критической информационной инфраструктуры РФ; распространение программного обеспечения с возможностями VPN-прокси-сервера и создания бот-сетей из зараженных ею компьютеров с сокрытием IP-адресов¹⁷⁵; сканирование информационных систем и эксплуатация уязвимостей¹⁷⁶ и пр. Так, гражданин использовал компьютерную программу, заведомо предназначенную для несанкционированного копирования

¹⁷⁵ Антонян Е. А., Россинская Е. Р., Клещина Е. Н. Обзор правоприменительной практики по противодействию киберпреступлений. Указ. соч. С. 31.

¹⁷⁶ Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. Указ. соч. С. 56.

компьютерной информации, из корыстной заинтересованности установив ее на свой личный компьютер, предварительно скачав ее с информационного ресурса в сети «Интернет». Ознакомившись с правилами функционирования указанной вредоносной программы приступил к реализации плана, который заключался в несанкционированном копировании на собственное средство вычислительной техники охраняемой законом компьютерной информации, принадлежащей третьим лицам и содержащую аутентификационные данные, персональные данные пользователей, а также иную техническую информацию о пользовательской системе. В этих целях гражданин разместил для скачивания в открытом доступе в сети «Интернет» файл с вредоносной программой под видом компьютерной игры, мотивируя к скачиванию указанного программного обеспечения сопутствующим видеообзором к прохождению игры. В результате пользователи, скачивающие замаскированную под компьютерную игру вирусную программу, подвергались утечке личных данных, которые незаконно копировались и передавались на персональный компьютер преступника. Несанкционированно скопированную компьютерную информацию, добытую в результате использования вредоносной компьютерной программы, гражданин за денежное вознаграждение передавал неустановленным пользователям информационного ресурса противоправной направленности в сети «Интернет». Денежные средства от продажи получаемой конфиденциальной информации субъект преступления получал на виртуальный счет в личном аккаунте информационного ресурса противоправной направленности в сети «Интернет». В результате исследования компьютерной программы, согласно заключению эксперта, установлено, что программа обладала возможностями по несанкционированному копированию компьютерной информации на удаленный сервер, а результаты ее работы могли быть использованы для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, а также нейтрализации средств защиты компьютерной информации¹⁷⁷.

Способы распространения вредоносного программного обеспечения зависят от целей преступника и технических возможностей жертвы и в большинстве своем представляют собой распространение вредоносных ссылок и программ на веб-ресурсах, в файлообменных пиринговых сетях, торрент-трекерах, сети блокчейн, а

¹⁷⁷ Приговор по уголовному делу № 1-44/2024 // Даниловский районный суд Ярославской области : офиц. сайт. URL: http://danilovsky-jrs.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=137975232&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

также электронных узлах и локальных информационно-вычислительных сетях¹⁷⁸, в виде вложений через мессенджеры, электронную почту и социальные сети; заражение устройств через недоработки в программном обеспечении и операционных системах устройств, принадлежащих жертве (например возможно воздействие на уязвимость нулевого дня (от англ. «zero-day» уязвимость в программном обеспечении, против которой еще не разработаны защитные механизмы и не были выпущены обновления безопасности) и т. п.; манипулирование пользователями применением методов социальной инженерии с целью побуждения их скачать и запустить вредоносное программное обеспечение; взлом протоколов безопасности для загрузки вредоносного кода; заражение носителей информации и IoT-устройств; использование вредоносного программного обеспечения для кражи лицензий, учетных данных, платежной информации банковских карт и пр.

Примером вышеуказанного может служить уголовное дело по обвинению гражданина в создании и распространении вредоносного программного обеспечения: из корыстной заинтересованности, действуя с прямым умыслом, субъект преступления разработал программный продукт, относящийся к категории компьютерных программ, обладающих признаками вредоносного программного обеспечения и предназначенных для использования в качестве веб-ресурсов и компонентов фишинговых сайтов, с целью дальнейшего несанкционированного копирования компьютерной и платежной информации банковских карт пользователей в обход средств защиты информации¹⁷⁹. Стоит отметить особую распространенность случаев нейтрализации средств защиты информации пользователей задействованием вредоносного программного обеспечения¹⁸⁰.

¹⁷⁸ Приговор по уголовному делу № 1-608/2023 // Советский районный суд г. Томска : офиц. сайт. URL: http://sovetsky--tms.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=11134764&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

¹⁷⁹ Приговор по уголовному делу № 1-637/2023 // Гагаринский районный суд г. Севастополя : офиц. сайт. URL: https://gagarinskiy--sev.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=51710604&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025); .

¹⁸⁰ Материалы уголовного дела № 12201711493000919, возбужденного 05 октября 2022 г. УМВД России по Ямало-Ненецкому (АО ОМВД России по г. Новому Уренгою); Приговор по уголовному делу № 1-250/2022 // Центральный районный суд г. Симферополя Республики Крым : офиц. сайт. URL: http://centr-simph--krm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=99109845&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

Наиболее популярные места распространения вредоносного программного обеспечения – различные веб-ресурсы, социальные сети и мессенджеры. Так, гражданин из корыстной заинтересованности создал «легендированный» (поддельный под оригинал) веб-интерфейс сайта, на котором пользователи сети «Интернет» сталкивались с хищением личных данных (полагая, что посещают ресурс с одноименным и оригинальным названием, допуская ошибку при наборе букв в названии сайта, где в интерфейсе ресурса использовалось вредоносное программное обеспечение, позволяющее устранять предусмотренную правообладателем защиту от несанкционированного доступа к компьютерной информации и копировать компьютерную информацию пользователей сети «Интернет» без ведома и против воли владельцев), а именно с неправомерным сбором: информации о программном и аппаратном обеспечении компьютера, включая список установленного на нем программного обеспечения, список запущенных процессов и браузеров; учетных данных пользователей; сведений о центральном процессоре, оперативной памяти, видеоадаптере, а также служебных данных, содержащихся в файлах, используемых при работе программного обеспечения; содержимого файлов, используемых частью программного обеспечения для хранения в качестве кошельков; пользовательских, служебных данных, содержащихся в файлах, используемых при работе браузеров (включающие учетные данные, используемые на сетевых ресурсах (адрес сайта, логин и пароль), данные автозаполнения для различных сайтов, данные об используемых банковских картах (имя владельца, месяц и год окончания обслуживания, номер))¹⁸¹.

Процессы, возникшие в ходе случайных действий либо при стечении обстоятельств, относят к непреднамеренным, это, например: использование разработчиками легального программного обеспечения открытых библиотек и баз данных, содержащих вредоносный код или критические уязвимости; внедрение вредоносного кода в проекты с открытым исходным кодом; создание прототипов автоматизированных программ для тестирования различных сервисов, которые случайно выходят из-под контроля, что довольно часто встречается при генерации кода с использованием искусственного интеллекта и т. п. Кроме того, вредоносные

¹⁸¹ Материалы уголовного дела № 11901320001060334, возбужденного 31 июля 2019 г. ГУ МВД России по Кемеровской области (УМВД России по г. Кемерово ОП «Заводский»); Приговор по уголовному делу № 1-188/2025 // Приволжский районный суд г. Казани Республики Татарстан : офиц. сайт. URL: https://privolzhsky--tat.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=365473880&case_uid=5978fa7b-f7ce-4e95-8479-7a42883090fe&delo_id=1540006 (дата обращения: 08.02.2025).

программы могут использоваться непреднамеренно, например, пользователем или администратором информационной системы. Так, довольно часто встречается ситуация, когда в отсутствие действенных средств защиты информации пользователи скачивают и запускают на первый взгляд легальное, но зараженное программное обеспечение, не подозревая о его вредоносной активности, что часто объясняется использованием нелегальных версий программ, распространяемых на безвозмездной основе.

Анализ уголовных дел позволил выявить основные средства создания, использования и распространения вредоносного программного обеспечения. При непосредственном доступе ими могут выступать носители информации, эксплуатируемые с техническими средствами, а при опосредованном доступе – сетевое оборудование, средства доступа в информационные системы (средства вычислительной техники, мобильные средства связи и пр.), различное программное обеспечение (например, кейлоггеры (от англ. «key» – клавиша и «logger» – регистрирующее устройство в виде клавиатурного шпиона), руткиты (от англ. «rootkit» – набор программных средств в виде исполняемых файлов, скриптов и пр., обеспечивающих маскировку объектов, управление и сбор данных), трояны (от англ. «trojan» – троянская вирусная программа, проникающая в компьютер под видом легального программного обеспечения) и пр.), способное к распространению в локальных информационных системах и служащих в целях выполнения какого-либо деструктивного действия (удаление, блокирование или изменение файлов) и пр.¹⁸².

В целом к средствам хранения вредоносного программного обеспечения относятся материальные носители: жесткие и оптические диски, USB-накопители, карты памяти и т. п., средством их обработки служит вычислительное устройство (процессор) технического средства. Средства разработки вредоносного программного обеспечения могут включать в себя: компиляторы и интерпретаторы (языки программирования, используемые для написания исходного кода); программное обеспечение в виде фреймворков для тестирования эксплойтов и бэкдоров; конструкторы вредоносного программного обеспечения, в том числе функционирующие на основе искусственного интеллекта, программное

¹⁸² Материалы уголовного дела № 12401250033000526, возбужденного 04 июня 2024 г. УМВД России по Иркутской области (МУ МВД России Иркутское ОП №5); Приговор по уголовному делу № 01-0285/2024 // Официальный портал судов общей юрисдикции г. Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/rs/lyublinskij/services/cases/criminal/details/29d72bc0-fb9c-11ec-956b-a9e3851a82ca> (дата обращения: 08.02.2025).

обеспечение для шифрования и маскировки вредоносного кода.

Средствами использования вредоносного программного обеспечения являются, например, управляемые группы зараженных устройств, используемые для DDoS-атак, спама и криптоджекинга (ботнет-сети), а также инструменты, обеспечивающие полный доступ к зараженному устройству; программы-шифровальщики и вымогатели, используемые для блокировки данных и вымогательства. К средствам распространения вредоносного программного обеспечения преимущественно относятся зараженные компьютеры (носители информации), сети передачи данных, веб-ресурсы и пр. хранилища данных.

Минимизировать риск раскрытия преступником своей личности и источников происхождения вредоносного программного обеспечения позволяют следующие методы сокрытия следов: использование анонимных сетей (например, «Tor», «VPN» или децентрализованной одноранговой сети «I2P» (от англ. «invisible internet project» – проект «Невидимый интернет») и пр.) с целью сокрытия IP-адреса или MAC-идентификатора средства совершения преступления и анонимных (фиктивных) учетных записей для внедрения программного обеспечения в информационные системы или в целях обсуждения и дальнейшего распространения вредоносных программ. Для исключения отслеживания банковских операций используются цифровые активы; шифрование исходного кода вредоносного программного обеспечения, обфускация (запутывание алгоритмов и маскировка вредоносных функций) для затруднения анализа; создание динамически изменяемых версий программ для обхода детектирования антивирусами; маскировка вредоносного программного обеспечения под легальные программы, входящие в состав операционной системы.

Для сокрытия следов разработки вредоносного программного обеспечения, как правило, используются изолированные виртуальные машины¹⁸³. При успешном внедрении вредоносных программ преступник переходит к мерам по сокрытию своей деятельности в зараженном устройстве, так, например, осуществляется маскировка вредоносных процессов и сетевой активности в операционной системе, обход или отключение антивирусных систем; манипуляция атрибутами создания, изменения и доступа к файлам (изменение временных меток файлов жертвы); использование самоуничтожаемых вредоносных программ после выполнения задачи; очистка системных лог-файлов и следов активности и пр.

¹⁸³ Белей А. В., Томская С. И. Компьютерное криминалистическое исследование вредоносного программного обеспечения // Правовая информатика. 2023. № 2. С. 103.

Типичными следами создания, использования и распространения вредоносного программного обеспечения в общем случае являются: следы установленных программ с признаками вредоносного функционала, изменения в конфигурации операционной системы устройства, журналах подключений к компьютерам или информационным системам, удаленные, модифицированные или заблокированные файлы данных и т. п.) и материальные следы на компьютерной периферии¹⁸⁴. К такого рода следам также относятся, например, артефакты в исходном коде программного обеспечения (метаданные файлов, идентифицирующих разработчика, дату компиляции, используемые библиотеки, сигнатуры компиляторов и сред разработки, а также использование типичных функций из открытых репозиторий или выявляемых ранее атак); IP-адреса и доменные имена серверов управления программным обеспечением; параметры задействованных виртуальных машин и обращения к серверам; временные файлы данных, содержащие информацию о запуске вредоносного кода; журналы системных событий; следы использования вредоносного программного обеспечения в файловой системе, оперативной памяти, сетевом трафике; следы распространения вредоносного программного обеспечения в сети «Интернет», в фишинговых электронных рассылках (структура заголовков писем, IP-адреса отправителей, SMTP-серверы исходящей почты (от англ. «simple mail transfer protocol» – простой протокол передачи почты) и пр.), сообщениях мессенджеров (фишинговые ссылки), вредоносных вложениях (документы с макросами, исполняемые файлы и пр.)) в компрометированных веб-сайтах и облачных сервисах, торрент-трекерах.

Таким образом, типичные следы при создании, использовании и распространении вредоносных программ можно обнаружить в программном обеспечении и в поименованных областях записей на носителях информации, при этом следы могут быть опосредованы с: электронными файлами; базами данных; идентификаторами в сети передачи данных (IP-адрес устройства или MAC-адрес его сетевой карты), IMEI-кодами мобильных устройств, DNS-адресами; реестрами операционных систем; сетевым трафиком; цифровыми финансовыми активами и электронными кошельками; IMS-, SMS- и MMS-сообщениями и т. п.

Вероятными местами расположения типичных следов создания, использования и распространения вредоносного программного обеспечения в цифровом виде являются носители информации различных устройств, облачные

¹⁸⁴ Материалы уголовного дела № 12401920053000057, возбужденного 16 января 2024 г. МВД по Республике Татарстан (УМВД России по городу Казани).

хранилища данных, в том числе файлы и каталоги хранения данных, файлы конфигурации программ удаленного доступа и пр.

Распространенность преступного деяния выражается в установлении факта схожести преступного деяния, например, на основе полученных сведений об использовании в преступной схеме способа совершения преступления, тиражирования вредоносного программного обеспечения. Так, например, признаками схожести по рассматриваемым деяниям могут выступить отдельные техники и тактики, которые обнаруживаются на основе наборов матриц баз данных угроз безопасности информации «Mitre Att&ck»¹⁸⁵ (от англ. «adversarial tactics, techniques & common knowledge» – тактики, техники и общеизвестные факты о злоумышленниках), представляющих собой основанные на реально существующих наблюдениях базы данных инцидентов безопасности или, например, идентичные контрольные суммы¹⁸⁶ программного обеспечения, а также реквизиты в виде MAC-идентификаторов или IP-адресов устройств, IMEI-кодов задействованных при распространении вредоносных программ мобильных средств связи; электронных адресов и т. п. Стоит также отметить, что с учетом развития технологий возможно создание и распространение вредоносного программного обеспечения с использованием технологий искусственного интеллекта с возможностью автоматической адаптации к системам защиты, использования методов машинного обучения для поиска уязвимостей в легальном программном обеспечении, генерации кода для обхода антивирусных сигнатур, а также интеграции их в мультимедиа контент.

Обстановка совершения преступления. Преступления, связанные с созданием, использованием и распространением вредоносного программного обеспечения, как правило, совершаются в условиях анонимности, с применением эффективных методов сокрытия цифровых следов неправомерных воздействий. Обстановка совершения рассматриваемого преступления предполагает как непосредственный доступ к объекту посягательства (преимущественно в момент отсутствия потенциальной жертвы), так и удаленный (при наличии подключения к сети «Интернет») и предполагает использование программно-аппаратных средств.

Местом совершения указанного преступления являются как конкретные компьютеры, серверы или информационные системы, так и локальные территории,

¹⁸⁵ База данных угроз безопасности информации «Mitre Att&ck» // Некоммерческая организация «Mitre»: офиц. сайт. URL: <https://attack.mitre.org> (дата обращения: 28.10.2025).

¹⁸⁶ Белей А. В., Томская С. И. Компьютерное криминалистическое исследование вредоносного программного обеспечения. Указ. соч. С. 105.

учреждения и организации, в которых эксплуатируется объект воздействия, либо критическая информационная инфраструктура. Довольно часто местом совершения преступления является локация, где физически располагается средство совершения преступления (компьютеры и серверное оборудование, в том числе арендованные), облачные хранилища, а также веб-сайты и ресурсы сети даркнет. В подавляющем большинстве случаев местом (средой) использования и распространения вредоносных компьютерных программ является киберпространство ввиду его распространенности среди населения, реже – метакосмос, блокчейн (распределенные реестры), либо гибридные инфраструктуры (распределенные облачные системы хранения данных и пр.).

Таким образом, местом совершения рассматриваемого вида преступления является, как правило, место реализации преступного умысла в интернет-пространстве – локация, где фактически располагалось компьютерное оборудование, посредством которого реализован преступный план, которая не ограничивается городом, территорией или конкретной страной, поскольку зачастую рассматриваемый вид преступлений носит трансграничный характер.

Временем совершения преступления признается время окончания преступного деяния вне зависимости от момента наступления последствий. Время создания вредоносного программного обеспечения не всегда устанавливается точно, поскольку их совершение часто связано с задействованием различных компьютеров, программного обеспечения, информационных систем и пр. Кроме того, работа указанных средств связана со временем, установленным в его системе, которое может быть легко изменено преступником в целях искажения типичных следов. Момент «внедрения» или распространения вредоносного программного обеспечения установить легче, поскольку его можно зафиксировать использованием средств защиты информации, например, антивирусных программ. В целом, время не оказывает особого влияния на выбор способа совершения или сокрытия рассматриваемых преступлений. Так, например, лицо, обвинялось в создании вредоносной компьютерной программы, предназначенной для несанкционированной модификации компьютерной информации о количестве нефтепродуктов, отпускаемых клиентам заправочной станции, и внедрении вредоносной программы в технологическое оборудование организации с последующим хищением нефтепродуктов, приобретаемых клиентами станции (путем их частичного недолива), и извлечением при этом материального дохода в результате сбыта похищенного. Однако, исходя из материалов уголовного дела, точная дата, а также время создания и внедрения вредоносных программ в технологическое оборудование организации, несмотря на наличие журналов

аудита, установлены не были¹⁸⁷.

Создание, использование и распространение вредоносного программного обеспечения ограничено временными рамками и в зависимости от специфики конкретного случая может возникнуть необходимость определения времени создания программного обеспечения или времени наступления вредоносных последствий. Разработка вредоносных программ может занять довольно длительное время, а процесс распространения или внедрения в систему отдельно взятого пользователя – считанные секунды.

Личность преступника. Как правило, лицо, разрабатывающее, использующее и распространяющее вредоносное программное обеспечение, имеет высшее или среднее инженерно-техническое¹⁸⁸ образование и (или) обладает навыками программирования и системного администрирования сетей, а также знаниями в области информационных технологий, сетевой безопасности, криптографии, реверс-инжиниринга, в сфере оборота электронных средств платежей, банковской деятельности и международных платежных систем, национальной платежной системы Российской Федерации. Совершаемые ими преступления часто носят серийный характер ввиду массовости распространения идентичного программного обеспечения¹⁸⁹ и сопровождаются тщательными действиями по сокрытию следов преступной деятельности. Анализ уголовных дел показывает, что преступники часто являются бывшими сотрудниками компаний, обладающими инсайдерской информацией, тщательно готовятся к атаке конкретного лица или объекта. Основными мотивами создания, использования и распространения вредоносного программного обеспечения выступают корыстные побуждения (получение материальной выгоды), личная неприязнь к объекту воздействия, вымогательство¹⁹⁰ или мошенничество, хулиганство, вандализм (разрушение информационных систем, атаки на технические средства, стремление

¹⁸⁷ Приговор по уголовному делу № 1-288/2024 // Промышленный районный суд г. Ставрополя : офиц. сайт. URL: https://promyshlenny--stv.sudrf.ru/modules.php?name=sud_delo&srv_%20num=1&name_op=doc&number=425524525&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

¹⁸⁸ Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования : монография / под ред. Е. В. Смахина, Р. Д. Шарапова, В. И. Морозова. Тюмень : Издательство Тюменского государственного университета, 2021. С. 219.

¹⁸⁹ Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования. Указ. соч. С. 703.

¹⁹⁰ Белей А. В., Томская С. И. Компьютерное криминалистическое исследование вредоносного программного обеспечения. Указ. соч. С. 110.

манипулировать системами и пр.), шпионаж (например, получение сведений экономической направленности, личной жизни и пр.) и пр. Помимо указанной категории часто встречаются несовершеннолетние, действующие по заранее определенным алгоритмам, не требующим специальных знаний, преимущественно для распространения фишинговых ресурсов, вредоносного программного обеспечения.

Личность потерпевшего и предмет посягательства. Предметом рассматриваемого преступления является вредоносное программное обеспечение, а также иная компьютерная информация, обрабатываемая на компьютерах или в информационных системах, не являющаяся программой, но способная нанести вредоносное воздействие. Потерпевший, как правило, является владельцем (пользователем) объекта, в отношении которого использовалось вредоносное программное обеспечение, либо лицом, правам и законным интересам которого причинен вред. Потерпевшим является физическое или юридическое лицо, которым причинен вред в результате преступного деяния, связанного с распространением вредоносного программного обеспечения.

Типичной жертвой среди физических лиц является пользователь сети «Интернет», который не обладает специальными знаниями в области кибербезопасности, активный пользователь интернет-сервисов, в частности, финансовых или сотрудник государственных органов (специалист в области информационных технологий, системный администратор), ставший мишенью атаки, направленной на получение доступа к служебной информационной системе.

Среди юридических лиц типичными пострадавшими являются коммерческие компании, производственные предприятия, образовательные и научные учреждения, средства массовой информации. Все чаще объектом воздействия становится критическая информационная инфраструктура Российской Федерации. Также потерпевшими признаются государственные органы власти, силовые структуры, нередко – медицинские учреждения.

Психологическими и поведенческими чертами и иными особенностями личности потерпевших от рассматриваемых деяний являются: недостаточная цифровая грамотность, излишняя доверчивость, высокая активность в цифровом пространстве, наличие критически значимой информации, отказ от использования антивирусных программ, использование слабой защиты данных авторизации, а также использование устаревшего программного обеспечения пр.

1.2.4. Криминалистическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

В связи с нарастающей необходимостью обработки и анализа значительного количества цифровых данных повсеместно вводится в эксплуатацию все большее количество различных информационно-телекоммуникационных сетей, которые существенным образом влияют на общественные отношения. Выход из строя указанных сетей или оборудования, обеспечивающего их функционирование, может привести к утечкам конфиденциальных сведений, разрушению информационных систем и иным последствиям¹⁹¹. По этой причине законодателем установлена уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Под правилами эксплуатации глобальных и иных информационно-телекоммуникационных сетей понимаются нормативные акты, регламентирующие работу соответствующей сети, например, Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»¹⁹², Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»¹⁹³ и иные документы, регламентирующие порядок создания и подключения к сети «Интернет», локальные инструкции и рекомендации по работе, разработанные предприятиями-изготовителями компьютеры и технические средства и т. п. Нарушение правил эксплуатации может быть совершено как умышленно, так и по неосторожности. Лицо может предвидеть уничтожение, блокирование, модификацию либо копирование компьютерной информации в результате нарушения им правил эксплуатации, но без достаточных к тому оснований самонадеянно рассчитывать на предотвращение последствий, либо не

¹⁹¹ Харисова З. И. Криминалистическая модель нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Философия права. 2025. № 2 (113). С. 181.

¹⁹² Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 г. № 17 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_147084 (дата обращения: 08.02.2025).

¹⁹³ О связи : Федеральный закон № 126-ФЗ от 07 июля 2003 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_43224 (дата обращения: 16.11.2025).

предполагать о них, хотя при необходимой внимательности и предусмотрительности должно было и могло их предвидеть. Субъектом данного преступления является лицо, которое в силу должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и обязано соблюдать установленные для них правила эксплуатации¹⁹⁴.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей необходимо отличать от преступления, предусмотренного ст. 272 УК РФ. При неправомерном доступе к охраняемой законом компьютерной информации виновный действует несанкционированно. Ответственность по ст. 274 УК РФ наступает только в том случае, если в результате этих действий причиняется крупный ущерб. Для привлечения к ответственности по ст. 272 УК РФ причинение такового не требуется, достаточно установить сам факт уничтожения, блокирования, модификации либо копирования компьютерной информации.

Способ совершения преступления. К противоправным действиям по рассматриваемому виду преступления можно отнести, например: предоставление посторонним лицам прав доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации и информационно-телекоммуникационным сетям; разглашение учетных данных (логина и пароля для доступа к информационным системам или информационно-телекоммуникационным сетям); нарушение запрета на подключение оконечного оборудования к сети «Интернет»; использование нелицензионного программного обеспечения; несанкционированная модификация программного обеспечения, настроек оборудования или информационно-телекоммуникационных сетей; отключение средств защиты информации и пр. Так, работники организации, действуя умышленно, из корыстной заинтересованности, обладая специальными познаниями в сфере компьютерной информации, договорились об использовании вычислительных мощностей компьютерного оборудования и локальной вычислительной сети организации, предназначенных для обработки информации уровня конфиденциальности «для служебного пользования», «персональные

¹⁹⁴ Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий : науч.-практ. пособие / под ред. А. Л. Аристархова, К. В. Камчатова. М. : Университет прокуратуры Российской Федерации, 2023. С. 17.

данные» и «коммерческая тайна», в целях майнинга криптовалюты и ее последующего обращения в свою пользу вопреки служебным интересам организации, тем самым нарушив запрет на подключение окончного оборудования к сети «Интернет»¹⁹⁵.

Учитывая многообразие способов совершения рассматриваемых преступления можно отметить наиболее распространенные из них: нарушение правил, направленных на обеспечение конфиденциальности информации (несанкционированный доступ к средствам хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (например, преодолением средств защиты информации с целью получения доступа к конфиденциальной информации без надлежащих прав, что может осуществляться с использованием методов социальной инженерии, эксплуатации уязвимостей и пр.), перехват обрабатываемой в них информации (например, перехват сетевого трафика или доступ к каналу связи), разглашение конфиденциальной информации и пр.); нарушение правил, направленных на обеспечение целостности информации (внесение изменений в охраняемую законом информацию (искажение, блокирование или удаление информации, хранящейся или обрабатываемой в информационно-телекоммуникационных сетях) или деструктивное воздействие на информационные системы и технические средства (вывод из строя информационной инфраструктуры)); нарушение правил, направленных на обеспечение доступности информации (совершение атак, приводящих к парализации работы средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (DoS и DDoS-атаки на информационные ресурсы)); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в целом (внесение изменений в состав, конструкцию, конфигурацию и условия размещения основных технических средств и информационных систем, проведение изменений, которые могут снизить уровень защищенности информации, подключение нештатных блоков и устройств; неправомерное изменение настроек оборудования (маршрутизаторов, коммутаторов, функционирующего на объектах программного обеспечения), неправильная эксплуатация информационных систем (использование

¹⁹⁵ Приговор по уголовному делу № 1-149/2019 // Саровский городской суд Нижегородской области : офиц. сайт. URL: https://sarovsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=104015501&case_uid=a2519d1d-d5f3-45c8-a536-2386e9b88b75&delo_id=1540006 (дата обращения: 08.02.2025).

нелицензионного программного обеспечения, отказ от обновлений, ошибки в настройке средств защиты информации; несанкционированное тестирование безопасности и воздействие вредоносного программного обеспечения; компрометация систем безопасности; нарушение политики контроля доступа; (использование сканеров уязвимостей без разрешения владельца системы); игнорирование признаков атак); использование вычислительных мощностей информационно-телекоммуникационных сетей в целях криптоджекинга и пр.

Процессы, возникшие в ходе случайных действий, относят к непреднамеренным. Непреднамеренность может выражаться бездействием в отношении проверок используемых средств хранения или передачи информации на наличие вредоносного программного обеспечения, игнорирование требований по использованию средств защиты информации при обработке информации; невыполнение обязательных процедур по резервному копированию данных, передача прав пользования информационной системой, а также отклонение от регламента обработки или передачи информации в информационно-телекоммуникационных сетях сотрудником организации ввиду его некомпетентности или халатности и т. п. В целом средствами совершения рассматриваемого преступления являются средства хранения, обработки или передачи охраняемой компьютерной информации и информационно-телекоммуникационных сетей, компьютеры и эксплуатируемые с ними и без них материальные носители: жесткие диски; USB-накопители; карты памяти и пр.

Анализ уголовных дел позволил также выявить такие наиболее распространенные средства, как сетевое (маршрутизаторы, коммутаторы и пр.) и серверное оборудование, мобильные устройства и средства доступа в информационные системы (средства вычислительной техники, средства защиты информации, электронные ключи пр.), виртуальные машины, облачные сервисы, а также различное программное обеспечение (например для клонирования данных, блокирования или их модификации), в том числе вредоносное (тройные программы, программы-шифровальщики, снифферы, сканеры уязвимостей, фишинговые наборы и пр.), средства защиты информации (антивирусное программное обеспечение, брандмауэры, системы обнаружения вторжений, системы аутентификации) для подключения к корпоративной сети в обход систем защиты, персональные средства аутентификации (электронные цифровые подписи, учетные записи, API-ключи), а также аппаратные инструменты (оборудование для перехвата информации (аппаратные снифферы для захвата сетевого трафика и закладки для удаленного контроля и пр.), создания помех в работе систем

(генераторы электромагнитных импульсов), съемные носители информации в виде USB-накопителей, внешних жестких дисков и иные физические устройства, например, Wi-Fi-адаптеры, одноплатные микрокомпьютеры и пр.).

Так, гражданин, обладающий техническими познаниями в области использования вредоносных компьютерных программ в операционных системах терминалов самообслуживания кредитно-финансовых учреждений, использовал электронные носители информации с вредоносной программой, обеспечивающей тайное хищение денежных средств, посредством неправомерного доступа к компьютерной информации и несанкционированного подключения к устройству самообслуживания, принадлежащего банку. Для нарушения правил эксплуатации данного устройства самообслуживания, как средства хранения, обработки и передачи компьютерной информации, с целью вывода его из рабочего состояния путем скрытного уничтожения, блокирования, копирования, модификации компьютерной информации на этом устройстве и последующего хищения из него наличных денежных средств, скопировал в операционную систему указанного устройства вредоносную компьютерную программу¹⁹⁶.

При нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей преимущественно используются следующие методы сокрытия следов: маскировка следов в файловой системе и на носителях информации; фальсификация временных меток в журналах событий; использование методов анонимизации с целью сокрытия IP-адреса или MAC-идентификатора средства совершения преступления; неправомерное использование чужой учетной записи в целях недопущения компрометации данных, внедрения шифровального программного обеспечения в информационные системы; деактивация средств защиты информации и прочих защитных механизмов информационно-телекоммуникационных сетей или информационных систем; обход систем контроля доступа и пр.

Типичными следами нарушений правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в общем случае являются: следы установленного программного обеспечения, в том числе с признаками вредоносного функционала;

¹⁹⁶ Приговор по уголовному делу № 1-105/2016 // Кировградский городской суд Свердловской области : офиц. сайт. URL: http://kirovgradsky--cvd.sudrf.ru/modules.php?name=sud_delo&srvnum=1&name_op=doc&number=17566285&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

изменения в конфигурации операционной системы устройства, сведения в журналах подключений к компьютерам или информационным системам и в реестрах событий, протоколирующих входы в систему и изменения привилегий доступа к информационным системам или информационно-телекоммуникационным сетям, а также действия в межсетевых экранах информационных систем; перечни удаленных, модифицированных или заблокированных данных и т. п.; материальные следы на компьютерной периферии.

К следам нарушений правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей можно отнести, например, IP-адреса и доменные имена серверов управления программным обеспечением; параметры задействованных виртуальных машин и обращений к серверам; временные файлы данных, содержащие информацию о запуске программного обеспечения или информационных систем; сведения в журналах системных событий; следы использования программ в файловой системе и в оперативной памяти (временные данные о процессах, активных соединениях и исполняемых файлах), сетевом трафике.

Таким образом, типичные следы по рассматриваемым преступлениям могут быть обнаружены в прикладном программном обеспечении и поименованных областях записей на носителях информации, при этом следы могут быть опосредованы с электронными файлами; базами данных информационных систем; идентификаторами передачи данных в информационно-телекоммуникационных сетях (IP-адрес устройства или MAC-адрес его сетевой карты), DNS-адресами; реестрами операционных систем; сетевым трафиком и т. п.

Вероятными местами расположения типичных следов нарушений правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в цифровом виде являются носители информации различных устройств, облачные хранилища данных, в том числе файлы и каталоги хранения данных, файлы конфигурации программ удаленного доступа и пр.

Распространенность преступления выражается в установлении факта схожести преступного деяния, например, на основе сведений, полученных государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) Национального координационного центра по компьютерным инцидентам (осуществляет координацию деятельности сил субъектов системы по вопросам реагирования на компьютерные инциденты, а

также международный обмен информацией о них)¹⁹⁷ об использовании в преступной схеме конкретного способа совершения преступления. Стоит отметить положительную тенденцию, выражающуюся в возможности подключения к вышеуказанной системе организаций, не являющихся субъектами критической информационной инфраструктуры РФ¹⁹⁸.

Однако на сегодняшний день подразделения МВД России и Следственного комитета РФ не имеют прямого доступа к средствам ГосСОПКА, системам Центра взаимодействия и реагирования Департамента информационной безопасности Банка России (ФинЦЕРТ) и иным сервисам Национального координационного центра по компьютерным инцидентам¹⁹⁹, по этой причине не всегда владеют оперативной информацией по совершаемым инцидентам.

Признаками схожести по рассматриваемым деяниям также могут выступить отдельные техники и тактики, которые могут быть обнаружены на основе наборов матриц, представляющих собой основанные на реально существующих наблюдениях баз данных инцидентов безопасности²⁰⁰, а также реквизитов в виде MAC-идентификаторов или IP-адресов устройств, электронных адресов и т. п.

С учетом развития технологий возможно нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей с возможностью автоматической адаптации к системам защиты, использования методов машинного обучения для поиска уязвимостей в легальном программном обеспечении²⁰¹, генерации кода для

¹⁹⁷ Единый территориально распределенный комплекс «Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ГосСОПКА) // Национальный координационный центр по компьютерным инцидентам – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : офиц. сайт. URL: <https://gossopka.ru> (дата обращения: 07.05.2025).

¹⁹⁸ О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» : Федеральный закон от 07 апреля 2025 г. № 58-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_502581 (дата обращения: 07.04.2025).

¹⁹⁹ Михайлова И. А., Лимарь А. С., Гилаев Р. И. О деятельности правоохранительных органов по противодействию преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий // Вестник экономики, права и социологии. 2024. № 2. С. 112.

²⁰⁰ ГОСТ Р 59709–2022 Защита информации. Управление компьютерными инцидентами. Термины и определения; дата введения: 01 февраля 2023 г. М.: Российский институт стандартизации, 2022. С. 2.

²⁰¹ Arevalo-Herrera J., Camargo J., Martinez J. Assessing SDN controller vulnerabilities: a survey on attack typologies, detection mechanisms, controller selection, and dataset application in machine learning // Wireless personal communications. 2025. V. 140. P. 740.

обхода антивирусных сигнатур и пр. Использование генеративного искусственного интеллекта способствует персонализации фишинговых атак под конкретного сотрудника, в частности, возможна генерация поддельных биометрических данных²⁰², используемых для авторизации в информационных системах или подложных документов и электронных ключей доступа.

Обстановка совершения преступления. Преступления, связанные с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, как правило, совершаются в условиях анонимности, с применением эффективных методов сокрытия цифровых следов неправомерных воздействий.

Обстановка совершения рассматриваемого преступления предполагает как непосредственный доступ к объекту посягательства (преимущественно в момент отсутствия свидетелей), так и удаленный (при наличии подключения к сети «Интернет» или к локальной сети объекта) и предполагает использование программно-аппаратных средств.

Местом совершения указанного преступления являются как конкретные компьютеры, серверы или информационные системы, так и локальные территории, учреждения и организации, в которых эксплуатируется объект воздействия. Довольно часто местом совершения преступления является локация, где физически располагается средство совершения преступления (компьютеры и серверное оборудование, в том числе арендованные), облачные хранилища, а также веб-сайты.

В подавляющем большинстве случаев местом (средой) нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей является киберпространство или локальная сеть организации.

Таким образом, местом совершения рассматриваемого вида преступления является, как правило, место реализации преступного умысла по месту расположения средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей или локация, где фактически располагалось оборудование, посредством которого реализован преступный план.

²⁰² Jenkins J., Roy K. Exploring deep convolutional generative adversarial networks (DCGAN) in biometric systems: a survey study // Discover artificial intelligence. 2024. V.4 (42). P. 2.

Временем совершения преступления признается время окончания преступного деяния вне зависимости от момента наступления последствий. Время факта нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей устанавливается достаточно точно, поскольку их совершение часто связано с задействованием различных компьютеров и программного обеспечения, входящих в информационные системы, функционирование которых протоколируется реестрами событий. Однако работа указанных средств и информационных систем связана со временем, установленным в их системе, которое в ряде случаев может быть изменено преступником в целях искажения следов.

Личность преступника. Как правило, лицо, совершающее рассматриваемое преступление, является сотрудником организации, в которой выявлено нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, имеющим высшее или среднее инженерно-техническое или профильное, соответствующее деятельности организации, образование, обладающим знаниями в области информационных технологий, обеспечения информационной безопасности организации, функционирования информационных систем. Так, в материалах одного из изученных уголовных дел работник, занимающий должность системного администратора отдела технической поддержки организации, имел умысел нарушения правил эксплуатации средств хранения, передачи охраняемой компьютерной информации путем копирования компьютерной информации и использования средств авторизации. Имея в силу исполняемых обязанностей доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, скопировал ее на USB-носитель из базы данных организации (не менее 40 000 записей пользовательских данных) и передал третьему лицу²⁰³.

Часто правоохранительные органы имеют дело с повторяющимися, детально подготовленными преступлениями со сложным и многоступенчатым механизмом, что может осуществляться только организованными преступными группами, включающими: организатора преступной группы; специалистов в области информационных технологий и программирования; лиц, обладающих

²⁰³ Приговор по уголовному делу № 10-15427 // Официальный портал судов общей юрисдикции г. Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/mgs/cases/docs/content/4ce5f02c-a4ae-45ae-a0a1-8a539cb978c5> (дата обращения: 08.02.2025).

компетенциями в области компьютерных технологий, эксплуатации компьютеров и иных технических средств, а также электронных кошельков с целью последующего перевода на них денежных средств; лиц, осуществляющих снятие наличных денежных средств со счетов или в банкоматах²⁰⁴.

Анализ уголовных дел показывает, что преступники часто являются действующими или бывшими сотрудниками компаний, обладающими инсайдерской информацией, тщательно готовятся к атаке конкретного лица или объекта.

Основными мотивами нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей выступают вандализм (воздействия на информационные системы, атаки на технические средства, стремление манипулировать системами и пр.), шпионаж (например, получение сведений экономической направленности), корыстные побуждения.

Так, работники научно-исследовательского института заранее договорились о совместном совершении преступления и разработали план: действуя умышленно, из корыстной заинтересованности, используя свое служебное положение, приискали имеющиеся незадействованные в работе гибридные системы, коммутаторы, серверы, пригодные для криптоджекинга (в целях извлечения материальной выгоды), которые под видом осуществления научно-исследовательских работ задействовали в процесс майнинга криптовалюты, а полученную прибыль делили между собой²⁰⁵. Собранное вычислительное оборудование было подключено к GSM-модему, что подразумевает подключение нештатных технических средств и организацию канала передачи данных между узлами вычислительного сегмента и сети «Интернет», представляя угрозу наступления тяжких последствий в виде утечки охраняемой законом информации.

²⁰⁴ Антонян Е. А., Россинская Е. Р., Клещина Е. Н. Указ. соч. С. 85.

²⁰⁵ Приговор по уголовному делу № 1-167/2019 // Саровский городской суд Нижегородской области : офиц. сайт. URL: https://sarovsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=104015975&case_uid=d45ac732-0fab-45e1-b969-34e877aad8dd&delo_id=1540006 (дата обращения: 08.02.2025).

Личность потерпевшего и предмет посягательства.

Предметом рассматриваемого преступления может выступать непосредственно охраняемая компьютерная информация, обрабатываемая с использованием средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в соответствии с неким регламентом либо сами средства хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационные сети и окончное оборудование²⁰⁶.

Самой распространенной в России информационно-телекоммуникационной сетью является сеть «Интернет», помимо которой, например, также имеются: Единая система информационно-аналитического обеспечения деятельности МВД России; Единая сеть электросвязи Российской Федерации; мультисервисная транспортная сеть связи Министерства обороны Российской Федерации и т. п.

Потерпевшими по рассматриваемому преступлению являются юридические лица или государственные структуры, которым причинен вред в результате преступного деяния. Часто потерпевшими оказываются коммерческие компании, производственные предприятия, образовательные и научные учреждения, средства массовой информации. Также потерпевшими признаются государственные органы власти, силовые структуры, нередко – медицинские учреждения.

По рассматриваемой категории дел в обязательном порядке подлежит установлению локальный нормативный акт в организации, регулирующий вопросы работы со средствами хранения, обработки или передачи охраняемой компьютерной информации и информационно-телекоммуникационных сетей (правила доступа к компьютерной информации, инструкции работы пользователей в информационных системах, регламенты по защите информации).

²⁰⁶ Стяжкина С. А. Уголовно-правовые особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник Удмуртского университета. Серия Экономика и право. 2021. №. 31 (3). С. 491.

1.2.5. Криминалистическая характеристика неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Одной из приоритетных на сегодняшний день задач для организаций, работающих в ключевых отраслях экономики, является защита объектов критической информационной инфраструктуры РФ, активное использование которых обусловлено переходом к информационному обществу. Обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры государства является одним из приоритетных направлений реализации национальных интересов страны и положений Доктрины информационной безопасности Российской Федерации²⁰⁷.

К объектам критической информационной инфраструктуры относят информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления субъектов критической информационной инфраструктуры, к которым относятся государственные органы и учреждения, юридические лица и индивидуальные предприниматели, которым указанные объекты принадлежат на праве собственности (аренды) или на ином законном основании.

Субъекты критической информационной инфраструктуры РФ являются владельцами либо эксплуатантами вышеуказанных объектов, функционирующих в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, сбой в которых могут привести к тяжелым социальным, политическим, экологическим и прочим последствиям²⁰⁸.

²⁰⁷ Харисова З. И. Информационно-компьютерная криминалистическая модель преступления в сфере компьютерной информации на примере неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Право и государство: теория и практика. 2025. № 9. С. 509.

²⁰⁸ О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 г. № 187-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_220885 (дата обращения: 07.04.2025).

Относимость объекта к критическому определяется исходя из его включения в реестр значимых объектов критической информационной инфраструктуры РФ²⁰⁹.

Состав преступления по статье 274.1. УК РФ в основе своей является специальным по отношению к иным статьям 28 главы УК РФ, выделенным по особой предметной области совершения преступления, т. е. критической информационной инфраструктуре РФ. Ответственность за создание, распространение и (или) использование программного обеспечения либо иной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты информации установлена ч. 1 ст. 274.1 УК РФ²¹⁰. В ч. 2 ст. 274.1 УК РФ предусмотрена ответственность за неправомерный доступ к охраняемым данным, содержащимся в критической информационной инфраструктуре РФ, в том числе с использованием программного обеспечения либо иной информации, которая заведомо предназначена для неправомерного воздействия на критическую информационную инфраструктуру РФ, или иных вредоносных компьютерных программ, если это повлекло причинение вреда инфраструктуре²¹¹. Диспозиция ч. 3 ст. 274.1 УК РФ включает противоправные деяния как в форме активного действия, так и бездействия в отношении соблюдения правил эксплуатации и нарушения правил доступа к объектам критической информационной инфраструктуры РФ. Обязательным признаком рассматриваемых преступлений является наступление общественно опасных последствий – причинения вреда критической информационной инфраструктуры РФ и тяжких последствий, имеющих значение для безопасности данной инфраструктуры. В соответствии со ст. 151 УПК РФ уголовные дела о преступлениях, предусмотренных статьей 274.1 УК РФ, преимущественно рассматриваются следователями органов ФСБ России, однако, предварительное

²⁰⁹ Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 06 декабря 2017 г. № 227 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_290538/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518 (дата обращения: 22.01.2025).

²¹⁰ Есаков Г. А. Комментарий к Уголовному кодексу Российской Федерации (постатейный). М. : Проспект, 2021. С. 182.

²¹¹ Дунин В. С., Скрипко П. Б. Инфокоммуникационные технологии и средства обеспечения информационной безопасности в деятельности подразделений, участвующих в раскрытии и расследовании преступлений в сфере информационно-коммуникационных технологий. Хабаровск : РИО ДВЮИ МВД России, 2019. С. 54.

следствие может производиться также следователями органа, выявившего эти преступления.

По содержанию ст. 274.1 УК РФ представляет собой объединение трех традиционных для отечественного законодательства форм преступного посягательства на безопасность компьютерной информации в виде неправомерного доступа к ней, создания и распространение вредоносного программного обеспечения, а также нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации в отношении объекта критической информационной инфраструктуры РФ²¹².

Способ совершения преступления. К действиям по рассматриваемому виду преступления можно отнести, например: неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ; нарушение правил доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, например, в виде предоставления посторонним лицам прав пользования информационными системами; несанкционированное изменение настроек оборудования; отключение средств защиты информации и программного обеспечения для резервирования данных; несанкционированное подключение к оборудованию или информационной системе, входящим в состав объекта критической информационной инфраструктуры РФ; модификация, блокирование или уничтожение компьютерной информации путем несанкционированного доступа к объекту критической информационной инфраструктуры РФ или внесение в информационную систему недостоверной информации, что нарушает целостность входящих в его состав систем, в результате чего информация, циркулирующая в нем, перестает соответствовать критериям ее достоверности, актуальности, целостности и полноты; использование веб-сервисов, размещенных в сети «Интернет», предназначенных для нагрузочного тестирования ресурсов объекта критической информационной инфраструктуры РФ (использование вредоносного программного обеспечения, позволяющего сканировать открытые порты оборудования); приостановление функционирования объекта или доступа других пользователей к информационной системе объекта; причинение вреда объекту, его физическое разрушение или вмешательство в работу серверных и вычислительных мощностей (разгон процессоров, перегрев оборудования, изменение параметров систем охлаждения); перехват сетевого трафика (сниффинг)

²¹² Русскиевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. Указ. соч. С. 237.

с целью получения критически важной информации; подмена программного кода в автоматизированных системах управления; использование «закладок» на аппаратном уровне (модифицированные микросхемы, предустановленные уязвимости в программном обеспечении); компрометация систем безопасности; игнорирование признаков атак функционирующих в составе объекта критической информационной инфраструктуры РФ систем обнаружений вторжений и пр.

Так, группа лиц по предварительному сговору в нарушение процедуры регистрации услуг, производили действия, связанные с привязкой банковских карт к абонентским номерам сотовой связи поставщика услуг без правовых на то оснований (без клиентских заявлений). В результате неправомерных действий организации был причинен вред как субъекту критической информационной инфраструктуры РФ, по причине того, что была нарушена целостность и актуальность содержащихся в ней данных, были созданы условия, при которых субъект критической информационной инфраструктуры РФ вынужден был приостановить работу своего сервиса на территории Российской Федерации и принять меры по восстановлению информации вследствие несанкционированного доступа к ней, что нанесло вред имиджу организации²¹³.

Способ реализации воздействия на объект критической информационной инфраструктуры РФ может быть удаленным, локальным или гибридным. По уровню автоматизации воздействия – автоматизированные (например, с использованием программного обеспечения, ботнетов и пр.) и неавтоматизированные. Также можно отметить отдельно аппаратные способы (перехват сетевого трафика, обход средств защиты информации, установленных на объектах, копирование конфиденциальных данных, хранящихся на объекте, изменение параметров загрузки операционной системы) и программные способы (неправомерное сканирование сетевых портов и сервисов, а также тестирование на предмет уязвимостей объектов критической информационной инфраструктуры РФ, шифрование, маскировка данных).

Неправомерное воздействие на критическую информационную инфраструктуру РФ может совершаться в форме как активных действий, либо бездействия в отношении соблюдения указанных регламентами правил доступа и эксплуатации. Непреднамеренность может выражаться бездействием в отношении

²¹³ Приговор по уголовному делу № 1-171/2023 // Вахитовский районный суд г. Казани : офиц. сайт. URL: https://vahitovsky--tat.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=236195779&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

соблюдения требований по использованию средств защиты информации при обработке информации; невыполнением обязательных процедур по резервному копированию данных, а также отклонения от регламента обработки или передачи информации на объекте критической информационной инфраструктуры РФ сотрудником организации и пр.

В целом средствами совершения рассматриваемого преступления являются непосредственно средства хранения, обработки или передачи охраняемой компьютерной информации, а также информационные системы, функционирующие на объекте критической информационной инфраструктуры РФ, компьютеры и эксплуатируемые с ними и без них материальные носители (жесткие и оптические диски, USB-накопители, карты памяти).

Анализ уголовных дел позволил также выявить такие распространенные средства неправомерного воздействия на критическую информационную инфраструктуру РФ как сетевое (маршрутизаторы, коммутаторы и т. п.) и серверное оборудование, мобильные устройства и средства доступа в информационные системы (средства вычислительной техники, средства защиты информации, электронные ключи пр.), виртуальные машины, облачные сервисы, а также различное программное обеспечение (например для клонирования данных, блокирования или модификации), в том числе вредоносное (троянские программы, программы-шифровальщики, снифферы, сканеры уязвимостей, фишинговые наборы и пр.), средства защиты информации (антивирусное программное обеспечение, брандмауэры); системы обнаружения вторжений на объекте критической информационной инфраструктуры РФ, а также персональные средства аутентификации (электронные цифровые подписи, учетные записи, API-ключи). Так, работник, выполняя трудовые обязанности и обладая информацией, что сотрудниками службы безопасности предприятия проводится служебная проверка, в рамках которой он проверяется на причастность к хищению жестких дисков и комплектующих к компьютерной технике, находясь по месту постоянного проживания, умышленно и незаконно осуществил удаленное подключение к информационным ресурсам предприятия, после чего уничтожил (удалил) папку «Служебные расследования» и заблокировал работу программного обеспечения, обеспечивающего управление резервным копированием и восстановлением данных, что отрицательно отразилось на выполнении работы по обеспечению экономической и информационной безопасности предприятия, являющегося субъектом критической информационной инфраструктуры РФ, тем

самым причинил вред критической информационной инфраструктуре РФ²¹⁴.

Аппаратно-технические средства неправомерного воздействия на критическую информационную инфраструктуру РФ включают устройства, непосредственно используемые для атаки на объект или обеспечивающие сокрытие цифровых следов. Это могут быть компьютеры и серверное оборудование, корпоративные мобильные устройства и иные специализированные устройства в виде датчиков, IoT-устройств, контроллеров и носителей информации. Программные средства играют ключевую роль при неправомерном воздействии на объект критической информационной инфраструктуры РФ, обеспечивая удаленный доступ, маскировку действий и повреждение входящих в него систем. К ним можно отнести вредоносное программное обеспечение (руткиты, троянские программы, программы-шифровальщики, ботнеты), инструменты для тестирования на проникновение, программы, используемые для маскировки преступных действий, сервисы «VPN», прокси-серверы, а также криптографические средства.

Типичными следами неправомерного воздействия на критическую информационную инфраструктуру РФ являются: журналы событий в системе и реестры сетевых подключений; IP-адреса и MAC-идентификаторы используемых устройств; IMEI-код или IMSI-код (от англ. «international mobile subscriber identity» – международный идентификатор мобильного абонента в сотовой связи) корпоративных мобильных средств связи; журналы соединений, изменений в прошивках устройств, входящих в инфраструктуру объекта; серийные номера носителей информации. Косвенными признаками неправомерного воздействия на критическую информационную инфраструктуру РФ могут являться рост потребления вычислительных ресурсов информационных систем, эксплуатируемых на объекте, а также материальные следы на компьютерной периферии.

Следы на носителях информации могут представлять собой журналы файловых систем и метаданных с отображением лог-файлов, временных меток, атрибутов доступа и пр., фрагменты удаленных или модифицированных данных (системные журналы с протоколированием действий, связанных со входом в

²¹⁴ Приговор по уголовному делу № 1-45/2022 // Ковровский городской суд Владимирской области : офиц. сайт. URL: http://kovrovsky--wld.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=120430332&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

систему, запуском процессов, выявленных ошибок и пр.), журналы эксплуатируемого программного обеспечения (мониторинг процессов инфраструктуры объекта, реконструкция последовательности событий).

Примером выявления следов неправомерного воздействия на критическую информационную инфраструктуру РФ в системных журналах может выступить уголовное дело по обвинению в неправомерном доступе к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ и нарушении правил доступа к охраняемой компьютерной информации, повлекших причинение вреда критической информационной инфраструктуре РФ: работник организации внес в информационную базу данных Министерства здравоохранения РФ заведомо ложные сведения о проведенной фиктивной вакцинации, что повлекло модификацию компьютерной информации, содержащейся в системе, являющейся значимым объектом критической информационной инфраструктуры РФ и нарушило целостность системы, в результате чего информация, циркулирующая в системе, перестала соответствовать критериям ее достоверности, актуальности, целостности и полноты, при этом факт модификации компьютерной информации, содержащейся в системе организации, был выявлен в результате анализа системных журналов с протоколированием действий работника, связанных с авторизацией в системе и предпринимаемых им манипуляций²¹⁵.

Так, по материалам уголовного дела было установлено, что работник организации с функционирующими объектами критической информационной инфраструктуры РФ, создал и распространил компьютерную программу, заведомо предназначенную для неправомерного воздействия на программный комплекс, несанкционированной модификации и нейтрализации средств защиты компьютерной информации, используемой для процедуры тестирования работников организации (на предмет знаний нормативных актов). Обладая специальными познаниями в области программирования, используя принадлежащий ему носитель информации, скопировал программный модуль и изменил структуру его системных настроек (в командной строке модуля программного комплекса прописал команду о выдаче положительного значения

²¹⁵ Приговор по уголовному делу № 1-480/2024 // Вахитовский районный суд г. Казани : офиц. сайт. URL: https://vahitovsky--tat.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=370408556&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

вне зависимости от правильности ввода значений), что позволило в дальнейшем тестируемым работникам получать положительный результат вне зависимости от правильности даваемых ими ответов. В дальнейшем работник организации разместил модифицированную программу в открытом доступе в сети «Интернет» для возмездного скачивания заинтересованными лицами на ранее созданном им сайте. В представленных на исследование в рамках судебной компьютерной экспертизы системных блоках, флэш-карте и ноутбуке имелось программное обеспечение, которое функционировало как программа с возможностью выдачи положительного результата тестирования вне зависимости от правильности ввода значений. На накопителях (жестких магнитных дисках), представленных на исследование компьютеров, имелись сведения о посещении ресурсов сети «Интернет», а также сведения о сохраненных логинах для доступа к веб-сайту с размещенной для возмездной реализации модифицированной программы. На накопителе мобильного средства связи, принадлежащего работнику, имелись сведения о переписке с пользователями-приобретателями программы в мессенджерах²¹⁶.

Следы в оперативной памяти технического средства на объекте критической информационной инфраструктуры РФ могут отображать временные данные и артефакты, содержащие сессии активных процессов, фрагменты исполняемых файлов или вредоносного программного обеспечения, загруженных в память, следы сессий удаленного доступа и пр.

Следы, связанные с функционированием программного обеспечения, могут быть представлены в системах мониторинга объекта, в журналах работы серверного оборудования, журналах аутентификации и изменений прав доступа, реестрах эксплуатации криптографических средств.

Типичными местами расположения следов при неправомерном воздействии на критическую информационную инфраструктуру РФ являются, соответственно: электронные или машинные носители информации; файловая система и метаданные; оперативная память; пакеты сетевого трафика; журналы событий программного обеспечения, межсетевых экранов, прокси-серверов и DNS-запросов; журналы работы специализированных систем управления, системы мониторинга компьютерных инцидентов (журналы, протоколирующие

²¹⁶ Приговор по уголовному делу № 1-15/2023 // Тимашевский районный суд Краснодарского края : офиц. сайт. URL: http://timashevsky--krd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=363864441&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

аномальные события в работе оборудования, ошибки, сбои, параметры нагрузки, а также журналы записей об административных операциях, конфигурационных изменениях, взаимодействии пользователей с системой и пр.); виртуальные машины и облачные среды; электронные цифровые подписи; сертификаты и криптографические ключи; журналы событий антивирусных систем.

При неправомерном воздействии на критическую информационную инфраструктуру РФ преимущественно используются следующие методы сокрытия следов: маскировка следов в журналах файловых систем и на носителях информации; фальсификация временных меток в реестрах событий; использование методов анонимизации с целью сокрытия IP-адреса или MAC-идентификатора средства совершения преступления; неправомерное использование чужой учетной записи в целях недопущения компрометации личных данных; внедрение шифровального программного обеспечения в информационные системы; деактивация средств защиты информации и прочих защитных механизмов информационно-телекоммуникационных сетей или информационных систем; обход систем контроля доступа и пр.

Таким образом, типичные следы неправомерного воздействия на критическую информационную инфраструктуру РФ могут быть обнаружены в системном и прикладном программном обеспечении и в поименованных областях записей на носителях информации. Следы могут быть опосредованы с электронными файлами, базами данных информационных систем, идентификаторами устройств и передачи данных (IP-адрес устройства или MAC-адрес его сетевой карты), DNS-адресами, реестрами операционных систем, сетевым трафиком и т. п.

Распространенность неправомерного воздействия на критическую информационную инфраструктуру РФ определяется установлением факта схожести преступного деяния на основе сведений, полученных государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) Национального координационного центра по компьютерным инцидентам о произошедшем на объекте инциденте информационной безопасности.

Признаками схожести по рассматриваемым деяниям могут выступить, например, IP-адрес, доменное имя, URL-адрес, атакованная сетевая служба и порт или протокол ресурса, вредоносное программное обеспечение, описание

используемых уязвимостей, хеш-сумма вредоносного модуля²¹⁷.

Помимо указанных признаками схожести также могут выступить угрозы из состава отечественного банка данных угроз безопасности информации²¹⁸, а также техники и тактики, обнаруженные на основе наборов матриц, представляющих собой основанные на реально существующих наблюдениях баз данных инцидентов безопасности, а также реквизитов в виде MAC-идентификаторов или IP-адресов устройств, электронных адресов и т. п. Стоит отметить, что наличие специализированной системы реагирования на компьютерные инциденты предполагает алгоритмизация действий по управлению ими, что является хорошим примером централизованного реагирования на инциденты безопасности²¹⁹. Перспективными способами неправомерного воздействия на критическую информационную инфраструктуру РФ с учетом развития информационных технологий могут выступить: компрометация защищенных каналов связи путем взлома асимметричных криптографических алгоритмов²²⁰; применение машинного обучения для поиска уязвимостей²²¹; внедрение аномалий в системы, представляющие из себя цифровые двойники объектов²²² критической

²¹⁷ Регламент взаимодействия Национального координационного центра по компьютерным инцидентам и владельцев информационных ресурсов Российской Федерации при информировании ФСБ России о компьютерных инцидентах, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак // Национальный координационный центр по компьютерным инцидентам : офиц. сайт. URL: <https://www.cert.gov.ru/materialy/organizatsiya-vzaimodeystviya/reglament-vzaimodeystviya-nktski-i-vladeltsev-informatsionnykh-resursov-rossiyskoy-federatsii-pri-in> (дата обращения: 31.01.2025).

²¹⁸ Банк данных угроз безопасности информации // Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю : офиц. сайт. URL: <https://bdu.fstec.ru/threat>. (дата обращения: 31.01.2025); Янгаева М. О., Шепель Н. В. Актуальные способы неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 4 (68). С.185.

²¹⁹ Методические рекомендации по разработке плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации // Национальный координационный центр по компьютерным инцидентам – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : офиц. сайт. URL: <https://gossopka.ru/upload/iblock/a9f/3va55amvsxqelhuo1oufo9y6998nbtwzMetodicheskie-rekomendatsii-po-razrabotke-Plana-reagirovaniya.pdf> (дата обращения: 31.01.2025).

²²⁰ Sengupta A., Kumar P., Sahani A. Ensuring the privacy of digital forensic reports using searchable symmetric encryption // *Advances in digital forensics*. 2025. V. 724. P. 30.

²²¹ Ahmad S., Haque M. Machine learning approaches in cybersecurity to enhance security in future network technologies // *Springer nature computer science*. 2025. № 6. P. 301.

²²² Metwally W., Ibrahim V. The role of the data analytics and digital twin for establishing intelligent city // *Proceedings of the ICSDI*. 2025. Springer, Singapore. V. 3. P. 295.

информационной инфраструктуры РФ с целью деструктивного воздействия на них.

Использование генеративного искусственного интеллекта способствует персонализации фишинговых атак под конкретного сотрудника, в частности, возможна генерация поддельных биометрических данных²²³, используемых для авторизации в информационной системе объекта критической информационной инфраструктуры РФ или подложных документов и электронных ключей доступа.

Обстановка совершения преступления. Как правило, обстановкой, способствующей совершению криминальной деятельности в отношении объекта критической информационной инфраструктуры РФ, является недостаточность мер по обеспечению информационной безопасности и защиты информации во входящих в него информационных системах и подсистемах²²⁴.

Обстановка совершения неправомерного воздействия на критическую информационную инфраструктуру РФ предполагает как непосредственный доступ к объекту посягательства (преимущественно в момент отсутствия сотрудников), так и удаленный (при наличии подключения к сети «Интернет» или к локальной сети объекта) и предполагает использование программно-аппаратных средств.

Местом совершения рассматриваемого вида преступления является место реализации преступного умысла по расположению объекта критической информационной инфраструктуры РФ или локация, где фактически располагалось оборудование, посредством которого реализован преступный план.

Временем совершения преступления признается время окончания преступного деяния вне зависимости от момента наступления последствий. Время факта неправомерного воздействия на критическую информационную инфраструктуру РФ устанавливается достаточно точно, поскольку все инциденты безопасности, как правило, протоколируются системами обнаружения вторжений.

Личность преступника. Неправомерное воздействие на объект критической информационной инфраструктуры РФ в большинстве случаев совершается работниками (сотрудниками) организаций, предприятий, учреждений, которые используют для их совершения свое служебное положение. Известны случаи, когда преступник ранее являлся сотрудником объекта. Преступления, совершаемые внешними субъектами, часто организуются в составе группировки, также

²²³ Mahima A., Monica M., Neha S. Deepfake image, video and audio detection // Computing technologies for sustainable development. 2025. V. 2361. P. 30.

²²⁴ Голубев Ф. А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации // Право и политика. 2020. № 10. С. 57.

возможны диверсии, спонсируемые иностранными государствами.

Анализ уголовных дел показывает, что преступники, как правило, имеют высшее или среднее инженерно-техническое или профильное, соответствующее деятельности организации, образование, обладают знаниями в области информационных технологий, обеспечения информационной безопасности систем на объектах критической информационной инфраструктуры РФ и их функционирования, предоставления услуг связи, доступа в сеть «Интернет», кабельного и спутникового телевизионного вещания, цифровых сервисов и мобильных приложений, финансовых услуг и сервисов электронной коммерции. Основными мотивами неправомерного воздействия на объект критической информационной инфраструктуры РФ выступают вандализм (разрушение информационных систем, атаки на технические средства, стремление манипулировать системами и пр.), разглашение конфиденциальных сведений, дискредитация деловой репутации субъекта критической информационной инфраструктуры РФ, корыстные побуждения (получение материальной выгоды), шантаж, шпионаж (например, получение сведений стратегической направленности) и пр.

Так, по уголовному делу в отношении работника, осуществившего неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, и причинившего ей вред в результате нарушения свойств информационной безопасности (целостности и конфиденциальности содержащейся в информационной системе организации), а также в результате нарушения работоспособности системы и ее перегруженности, указывается, что описанными действиями был причинен ущерб деловой репутации организации, а также разглашены конфиденциальные сведения о пользователях-клиентах²²⁵. Примером мотива преступника, выраженного шантажом, является уголовное дело, в материалах которого имеется информация о наличии у гражданина достаточных знаний и практических навыков в области компьютерной информации и работы с компьютерным обеспечением, а также корыстных требований материального характера за прекращение совершаемых им вредоносных компьютерных атак на сайты, являющиеся объектами критической

²²⁵ Приговор по уголовному делу № 1-142/2022 Саяногорский городской суд Республики Хакасия : офиц. сайт. URL: http://saianogorsky--hak.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=53520798&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

информационной инфраструктуры РФ²²⁶.

Личность потерпевшего и предмет посягательства. Предметом рассматриваемого состава преступления является охраняемая законом компьютерная информация, содержащаяся в критической информационной инфраструктуре РФ²²⁷ или программное обеспечение, заведомо предназначенное для совершения компьютерных атак на объект²²⁸.

Чаще всего воздействию подвержены абонентские базы данных операторов мобильной связи и интернет-провайдеров, либо банковские или служебные базы данных, при нарушении правил эксплуатации различных информационных систем и доступа к ним²²⁹, например, в отношении систем, эксплуатируемых в медицинских учреждениях, на промышленных и иных объектах. Существенными проблемами для потерпевших по факту неправомерного воздействия на объект критической информационной инфраструктуры РФ является наступление общественно опасных последствий в виде модификации содержащейся в информационных системах компьютерной информации, утечек конфиденциальных данных, а также необходимости проведения дополнительных внеплановых мероприятий по оценке защищенности систем, актуализации циркулирующих в них данных. Потерпевших можно связать с владельцем (пользователем) объекта, в отношении которого допущено неправомерное воздействие. Ими являются юридические лица или государственные структуры, которым причинен вред в результате рассматриваемого преступного деяния. Часто потерпевшими оказываются медицинские учреждения, поставщики услуг связи и сети «Интернет», производственные предприятия, а также научные учреждения.

По рассматриваемой категории дел в обязательном порядке подлежит установлению локальный нормативный акт в организации, регулирующий вопросы работы на объекте критической информационной инфраструктуры РФ (правила доступа к компьютерной информации, правила обработки конфиденциальных

²²⁶ Приговор по уголовному делу № 1-237/2022 Харабалинский районный суд Астраханской области : офиц. сайт. URL: http://harabalinsky--ast.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=182264936&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

²²⁷ Ермолаев Н. В. К вопросу о разграничении преступлений в сфере компьютерной информации, предусмотренных статьей 272 и ч. 2 ст. 274.1 уголовного кодекса РФ // Вестник Дальневосточного юридического института МВД России. 2024. № 2 (67). С. 43.

²²⁸ Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. Указ. соч. С. 238.

²²⁹ Евдокимов К. Н. Вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 168.

данных, инструкции работы пользователей в системах, регламенты защиты информации). Целесообразно также рассмотрение документов, подтверждающих служебное положение лица (приказы о назначении на должность, копия трудовой книжки, должностной регламент, правовые и нормативные акты, регулирующие деятельность и поведение субъекта, табель рабочего времени)²³⁰.

В заключение необходимо отметить ряд особенностей формирования криминалистической характеристики преступлений в сфере компьютерной информации, в том числе с точки зрения теоретико-прогностического подхода, а также ее использования в целях формирования цифровой модели преступного деяния. Обоснование дополнения структуры криминалистической характеристики преступлений может быть исключительно на основе эмпирических данных.

По этой причине для ряда преступных деяний, относящихся к преступлениям в сфере компьютерной информации, таких как нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ), незаконное использование абонентских терминалов и виртуальных телефонных станций (ст. 274.3 УК РФ) и организация деятельности по незаконному обороту SIM-карт (ст. 274.4 УК РФ), неправомерному обороту аккаунтов и учетных данных (ст. 274.5 УК РФ) может строиться лишь общая (вероятностная) криминалистическая характеристика на основе теоретико-прогностического подхода, что обусловлено отсутствием на момент исследования следственной и судебной практики по применению данных норм.

В то же время, например, отсутствие судебной практики по ст. 274.2 УК РФ с момента ее включения в 2022 году в УК РФ может свидетельствовать либо о высокой степени уголовно-правовой охраны рассматриваемых процессов, либо о недостаточной правоприменительной активности в данной сфере. Кроме того, временное отсутствие следственной практики за определенный период времени зачастую связано с нововведениями в законодательстве, что применимо в настоящий момент к ст. ст. 274.3, 274.4 и 274.5 УК РФ.

При явной необходимости уголовно-правовой охраны киберпространства от информационных посягательств имеются исследования, которые подчеркивают

²³⁰ Голубев Ф. А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации. Указ. соч. С. 54.

отсутствие обоснованности и оправданности введения в УК РФ рассматриваемой статьи²³¹. Так, при условии отнесения объекта преступления к объектам критической информационной инфраструктуры РФ, деяния по нарушению правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования могут быть квалифицированы как по ч. 3 ст. 274.1 УК РФ, а в случае, если объект не категоризован как критическая информационная инфраструктура – по ст. 274 УК РФ. По этой причине элементы криминалистической характеристики рассматриваемого преступления частично могут повторять составляющие характеристики преступлений по ст. ст. 274 и 274.1 УК РФ, что, отчасти обусловлено их родовой принадлежностью

Таким образом, отсутствие практики применения указанных выше норм осложняет проведение анализа взаимосвязанности элементов криминалистической характеристики преступлений в сфере компьютерной информации даже на теоретическом уровне, либо приводит к невозможности осуществления такого анализа и, закономерно, может снизить точность формируемой информационной модели (цифрового двойника преступления²³²), а также внести погрешности, связанные с отсутствием алгоритмов расследования перечисленных преступных деяний. По этой причине выявление элементов криминалистической характеристики преступлений по ст. ст. 274.2, 274.3, 274.4 и 274.5 УК РФ на данный момент нецелесообразно, но необходимо в дальнейшем по мере появления практики их расследования. Проведенный анализ показал, что большинство преступлений в сфере компьютерной информации могут совершаться одними и теми же способами, с использованием одних и тех же средств, которые во многом оставляют схожие следы. Однако объединение информационных моделей по различным видам преступлений нецелесообразно, несмотря, например, на единый

²³¹ Дремлюга Р. И. Проблемы уголовно-правовой регламентации ответственности за преступления, предусмотренные ст. 274.2 УК РФ // Труды Института государства и права Российской академии наук. 2024. Т. 19. № 1. С. 166; Дроздецкая А. С. Некоторые проблемы законодательной конструкции состава преступления, предусмотренного статьей 274.2 Уголовного кодекса Российской Федерации // Следственная деятельность: проблемы, их решение, перспективы развития : материалы VII Всероссийской научно-практической конференции. Москва : Московская академия Следственного комитета Российской Федерации, 2024. С. 130.

²³² Homaei M., Mogollon-Gutierrez O., Sancho J. A review of digital twins and their application in cybersecurity based on artificial intelligence // Artificial intelligence review. 2024. V. 57. № 201. P. 3.

для всех преступлений, объединенных главой 28 УК РФ, комплекс способов сокрытия следов в виде использования средств анонимизации (сервисов «VPN» и прокси-серверов)²³³ и т. п., поскольку чем уже уровень обобщения преступлений, тем конкретнее по ним данные и выше практическая ценность такой характеристики при расследовании. В целом, сформированный комплекс элементов криминалистической характеристики преступлений в сфере компьютерной информации может приобрести практическое значение лишь в случае выявления между его составляющими корреляционных связей и зависимостей, носящих закономерный характер²³⁴.

В заключение также стоит отметить, что современные технологии, основанные на методах обработки больших данных, математической статистики, искусственного интеллекта и алгоритмах машинного обучения, могут предоставить возможность построения типовых криминалистических характеристик преступлений в виде цифровых моделей²³⁵, отображаемых в машиночитаемой форме и представленных сведениями о криминалистически значимых признаках и их корреляционных и вероятностных связях между математическими категориями, уравнениями или неравенствами. Модели такого рода могут использоваться как для получения знаний о преступлениях различных видов и использования их следователями, так и для разработки специального программного обеспечения, сопровождающего следственную и судебно-экспертную деятельность.

Для построения цифровой модели преступления между элементами криминалистической характеристики преступлений необходимо выделить корреляционных и вероятностных связей, что удобнее всего осуществлять с применением математических методов и алгоритмов машинного обучения (глава 5). При составлении криминалистических характеристик для наглядности могут использоваться схемы, отражающие элементы, связи системы расследуемого преступления или криминалистические формулы. Как показал проведенный структурно-содержательный анализ, элементы криминалистических характеристик преступлений в сфере компьютерной информации по содержанию могут в некоторой степени совпадать, но отличаться частностями, которые существенно позволяют повысить точность алгоритма работы моделей и выдачи

²³³ Антонян Е. А., Россинская Е. Р., Клещина Е. Н. Обзор правоприменительной практики по противодействию киберпреступлений. Указ. соч. С. 72.

²³⁴ Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. Указ. соч. С. 222.

²³⁵ Криминалистика : учебник / под ред. И. М. Комарова. Указ. соч. С. 557.

ими результатов. Это объясняется тем, что при обучении систем на основе искусственного интеллекта используются наборы данных (обучающие датасеты)²³⁶, которые содержат сведения с результатами решения поставленных задач, при этом отбираются наиболее значимые для выдачи результата признаки.

Качество алгоритма зависит от данных, на которых он обучен, что говорит о важности разнообразия в наборе обучающих данных²³⁷. В общем случае алгоритмы искусственного интеллекта используют обучающий набор в качестве входных данных, который содержит совокупность переменных в виде значимых признаков. Каждый обучающий пример в датасете содержит переменную результата (метку), которая отражает верное решение. Чем больше и разнообразнее набор обучающих данных (за исключением эффекта переобучения), тем лучше она распознает закономерности в них и тем точнее она выдает решения²³⁸. Соответственно, интеллектуальное программное технико-криминалистическое средство, используемое, например, для формирования методики расследования преступлений в сфере компьютерной информации, обученное на выборочном²³⁹ наборе данных, включающем элементы криминалистической характеристики одного вида преступления, выдаст результат с погрешностью для преступления, отличного от обучающего.

В свою очередь, криминалистическое средство, обученное на наборе данных, включающем элементы криминалистической характеристики нескольких видов преступлений, входящих в одну группу, выдаст результат с большей точностью, поскольку будет учитывать значимость (веса) признаков для выдачи результата. Это связано со спецификой каждого из рассмотренных составов, входящих в 28 главу УК РФ, в частности, со способами и используемыми средствами совершения преступлений, цифровыми следами преступлений и способами их сокрытия. Выделение элементов криминалистических характеристик преступлений в сфере компьютерной информации выступает важнейшим этапом для машинного обучения, который требует значительных усилий, связанных с получением данных для моделирования, извлечением и компоновкой наиболее значимых признаков. Кроме того, элементы криминалистических характеристик могут выступить

²³⁶ Постолиит А. В. Основы искусственного интеллекта в примерах на Python. СПб. : БХВ-Петербург, 2024. С. 230.

²³⁷ Анирад К., Сиддха Г., Мехер К. Искусственный интеллект и компьютерное зрение. Реальные проекты на Python, Keras и TensorFlow. СПб.: Питер, 2023. С. 249.

²³⁸ Хултен Дж. Разработка интеллектуальных систем. М. : ДМК Пресс, 2019. С. 219.

²³⁹ Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Указ. соч. С. 24.

основой для структурирования обучающего датасета²⁴⁰, позволяющего получить более полную информационную модель преступного деяния, что будет способствовать формированию более точного алгоритма его расследования.

Детализация способов совершения преступлений, в свою очередь, сформирует основу для построения цифровой модели преступления в сфере компьютерной информации (цифрового двойника преступления), которая позволит моделировать полную структуру преступной деятельности (подготовка, совершение и сокрытие преступления), а также ход его расследования в цифровом виде, на основе предварительно обученных алгоритмов искусственного интеллекта, при этом анализируя взаимосвязи путем сопоставления способов совершения преступлений (тактик) со средствами совершения преступлений (техниками), оставляющими цифровые следы.

Типовая криминалистическая характеристика преступления способствует установлению ретроспективной модели произошедшего события и позволяет оценивать полноту исходной информации о преступном деянии, определять признаки преступления, выдвигать следственные версии и планировать следственные действия и, что наиболее важно по преступлениям в сфере компьютерной информации, выявлять наиболее эффективные криминалистические средства для собирания (обнаружения, фиксации и изъятия), исследования и оценки следов криминального деяния²⁴¹, которые преимущественно являются программными (глава 2).

Прикладным значением типовых криминалистических характеристик преступлений в сфере компьютерной информации является возможность их использования при формировании частных криминалистических методик расследования, создании новых криминалистических учетов на основе формируемых баз данных цифровых доказательств, а также разработки специализированного программного обеспечения в виде систем поддержки принятия решений, применяемых, например, при выдвижении следственных версий и планировании расследования (глава 3).

Цифровой двойник преступления в данном контексте будет представлять собой виртуальную модель, отражающую состояние и динамику реального преступления в сфере компьютерной информации, позволяющую исследовать различные сценарии его совершения, выявлять закономерности между элементами его криминалистической характеристики, формировать алгоритм расследования

²⁴⁰ Стивен С. Наука о данных. СПб. : Диалектика, 2020. С. 39.

²⁴¹ Криминалистическая методика : учебник для вузов / под ред. А. И. Бастрыкина. М. : Юрайт. 2025. С. 18.

преступного деяния, выдавать вероятность его раскрытия. В связи с этим необходимо предусмотреть систему кодирования (в значении упорядочивания, как одного из видов работ в области инженерии знаний, присвоения кодов) указанных элементов с целью возможности представления криминалистически значимых признаков в машиночитаемой форме (глава 4).

Таким образом, криминалистическая характеристика преступлений является составляющим элементом криминалистической методики. Проведенный структурный анализ служит основой для систематизации преступных деяний указанного вида, однако, выявление причин их возникновения с целью попытки принятия предупреждающих мер возможно путем объединения структурно-содержательного и системно-исторического подхода. Совмещение этих методов позволит выявить основные закономерности формирования и эволюции правовых норм в указанной сфере, спрогнозировать новые формы противоправной деятельности с учетом технологических трендов и, как следствие, разработать концептуальные основы совершенствования существующих криминалистических методик расследования (глава 5).

В соответствии с Концепцией государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-телекоммуникационных технологий, необходимо отметить, что рост числа преступлений в рассматриваемой области обусловлен не только широкой распространенностью и развитием технологий, но и виктимным поведением потерпевших, низким уровнем финансовой и правовой грамотности населения, возможностью анонимного доступа преступников к сети «Интернет» и пр. факторами. Ежегодное увеличение количества потерпевших от преступлений в сфере компьютерной информации, ущерб, причиненный киберпреступлениями в размере 200 млрд руб. (+ 36,0 % по сравнению с 2023 годом), который составляет 32,4 % от общей суммы материального ущерба, причиненного всеми преступлениями в 2024 году²⁴², ставит закономерным вопрос о выявлении наиболее эффективных методов и средств, используемых в противодействии указанному виду преступлений. Актуальность проводимого исследования подтверждает также стабильная трансформация структуры рассматриваемого вида преступных деяний и ее содержания, что приводит к необходимости исследования генезиса преступлений, совершаемых в сфере компьютерной информации, их детерминант, а также оценки влияния на них внешних факторов с определением сценария их развития.

²⁴² Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. Указ. соч. С. 59.

1.3. Генезис преступлений, совершаемых в сфере компьютерной информации, и их детерминанты

Современный этап общественного развития характеризуется переходом к информационному обществу. Развитие кибернетики, разработка и совершенствование технических устройств, внедрение информационно-телекоммуникационных технологий в большинство сфер жизнедеятельности человека привели к глобальной информатизации, обусловленной необходимостью обработки, хранения и анализа значительных объемов цифровых данных. Информационные технологии, являясь потенциальным инструментом содействия общественному прогрессу, одновременно создают широкие возможности для противоправной деятельности. Их использование преступниками способствует не только диверсификации преступных проявлений и эскалации их масштабов, но и деструктивному воздействию на общество, государство и его институты, а также коммерческие организации.

В контексте снижения потенциала использования информационно-телекоммуникационных технологий в целях совершения преступлений представляется необходимым исследование генезиса преступлений, совершаемых в сфере компьютерной информации. Использование системно-исторического подхода при анализе позволит рассмотреть не только этапы его развития, но и современное состояние, а также возможные направления его трансформации с целью выявления наиболее перспективных (прогностических или предиктивных моделей)²⁴³ (от англ. «predictive analytics» – предсказательная аналитика) методов предотвращения противоправных деяний, принятия предупреждающих мер, направленных на сокращение как существующих, так и потенциально возможных преступлений.

Современное право направлено на урегулирование вновь появляющихся форм отношений практически всех сфер деятельности человека, где объектами, субъектами, а порой и средствами все чаще выступают высокие технологии, что закономерно формирует новый вид права, именуемый высокотехнологичным и представляющим собой логистичный, наукоемкий и технологичный регулятор общественных отношений, который не только контролирует вновь возникающие отношения, связанные с высокими технологиями, но и активно использует их в

²⁴³ Edwards, J. Mastering cybersecurity strategies, technologies and best practices. New York : APress Media (Springer Nature), 2024. P. 581.

правоприменении²⁴⁴. Возникновение новых субъектов права, объектов регулирования и высокотехнологичных средств совершения преступлений в основном вынуждает законодателей принимать меры по разработке нормативных правовых актов, регулирующих новые правоотношения. Однако хорошей практикой является рассмотрение генезиса того или иного явления и его основных детерминант в целях выявления наиболее перспективных методов предотвращения нежелательных последствий в будущем, что возможно при проведении анализа с использованием системного подхода²⁴⁵.

Наиболее распространенными разновидностями системного подхода в науке, которыми активно пользуются в естествознании, являются: системно-элементный (выявление элементов, входящих в исследуемую систему); системно-структурный (выявление взаимосвязей между составляющими систему элементами); системно-функциональный (выявление функций, выполняемых системой); системно-коммуникационный (определение взаимосвязей между входящими в систему элементами и внешней средой) и системно-исторический (исследование генезиса системы и ее динамики как изучение пройденных этапов ее развития, современного состояния, а также возможных перспектив развития)²⁴⁶.

Под генезисом в науке понимается описание происхождения, возникновения, становления и развития различных природных, социальных и иных явлений²⁴⁷.

Изучение генезиса преступлений, совершаемых в сфере компьютерной информации, как феномена правовой действительности с точки зрения системно-исторического подхода позволит получить дополнительные сведения не только о природе юридических приемов создания, реализации и толкования норм права, но и сформулировать текущие и потенциально возможные формы рассматриваемого вида преступных деяний в будущем.

Рассматривая основные составляющие ядра пятого индустриального технологического уклада (1980–2020 г.г.) наибольшее внимание следует уделить таким областям науки, как электроника и прикладная информатика, регулирующим процесс изучения информационных технологий, телекоммуникаций, методов

²⁴⁴ Пучков О. А. Право в зеркале высоких технологий: сравнительный анализ тенденций правового развития // Правовое государство: теория и практика. 2024. № 2. С. 168.

²⁴⁵ Харисова З. И. Генезис преступности в сфере компьютерной информации и ее детерминанты // Общество, право, государственность: ретроспектива и перспектива. 2025. № 1 (21). С. 59.

²⁴⁶ Отюцкий Г. П. Концепции современного естествознания. М. : Юрайт. 2025. С. 70.

²⁴⁷ Петровская В. Н., Щепин В. И. Концепции современного естествознания: словарь терминов. Указ. соч. С. 20.

обеспечения информационной безопасности, защиты информации, функционирования различных технических устройств и т. п. Наступление шестого цикла Кондратьева²⁴⁸, как нового индустриального уклада, связывают с развитием биотехнологий, генной инженерии и, безусловно, информационно-телекоммуникационных технологий, включая современный стек (от англ. «stack» – набор инструментов или информационных технологий, используемых для реализации проекта) индустрий Web 4.0 и в большей мере Web 5.0, которые представлены технологиями искусственного интеллекта, распределенного реестра (блокчейн), сверхвысокой передачи данных, Интернета вещей, а также виртуальной и дополненной реальности.

Основным преимуществом новой эпохи когнитивных технологий выступают глобализация, скорость связи и перемещения, постоянное повышение уровня комфорта жизни населения²⁴⁹ с задействованием вышеперечисленных технологий. Вместе с тем уже на постоянной основе возникают проблемы, связанные с обеспечением безопасности эксплуатации информационно-телекоммуникационных технологий. В этой связи наряду с генезисом преступлений, совершаемых в сфере компьютерной информации, необходимо рассмотрение основных ее детерминант как комплекса явлений, совместное действие которых порождает противоправные деяния.

Аналогично тому, как интенсивное развитие промышленности породило экологические проблемы планетарного масштаба, а достижения в области ядерной физики создали угрозу глобальной ядерной войны, на сегодняшний день можно констатировать, что информатизация является причиной таких негативных последствий, как возросший уровень преступных деяний, совершаемых с использованием информационно-телекоммуникационных технологий. Появление «информационного оружия», как следствие развития информационных технологий, по степени опасности может превзойти ядерное оружие, поскольку даже запуск средств массового поражения в ряде случаев осуществляется командой в автоматизированной системе боевого управления.

Анализ криминогенной обстановки в Российской Федерации свидетельствует о том, что преступность в сфере компьютерной информации стала

²⁴⁸ Sadovnichiy V. A., Akaev A. A., Davydova O. I. Modeling and forecasting the evolutionary economic development of the BRICS and G7 countries in the first half of the twenty-first century // Journal of globalization studies. 2024. V. 15. № 2. С. 5.

²⁴⁹ История науки, техники и транспорта: учебник для вузов / под ред. В. В. Фортунатова. М. : Юрайт. 2024. С. 14.

одним из ключевых деструктивных факторов общественного развития.

Количественный рост преступлений, сопровождающийся их качественными изменениями, создает реальную угрозу социально-экономическому развитию, стабильности государственности и национальной безопасности²⁵⁰. Криминализация использования информационно-телекоммуникационных технологий усугубляется активным вовлечением в нее организованных преступных групп, которые постоянно ищут новые способы совершения преступлений, используя передовые достижения науки и техники.

По этой причине итогом пятилетней работы государств-членов Организации Объединенных Наций стало одобрение разработанной по инициативе Российской Федерации Конвенции против киберпреступности, являющейся универсальным договором, предусматривающим укрепление международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий. Принятый документ подчеркивает особую важность борьбы с указанным видом преступлений, поскольку они зачастую связаны с отмыванием денег, террористическими и экстремистскими актами, неправомерным использованием криптовалют, коррупцией, торговлей людьми, незаконным изготовлением и оборотом оружия, наркотических и психотропных веществ и пр., а ст. 55 вышеуказанной конвенции предусматривает проведение каждым отдельно взятым государством анализа тенденций, характеризующих совершаемые на их территории киберпреступления.

Рассматривая феномен преступлений, совершаемых в сфере компьютерной информации, с исторической точки зрения можно выделить несколько ключевых факторов (условных этапов), которые способствовали ее широкому распространению и развитию. Одной из очевидных причин стало появление в 1940–1960-е гг. первых электронно-вычислительных машин, которые в большей степени эксплуатировались на предприятиях. Это стало отправной точкой развития таких примитивных деструктивных форм, как нарушение правил хранения и обработки информационных ресурсов и несанкционированный доступ к защищаемым данным²⁵¹.

Последующее массовое распространение компьютеров в 1970–1980-е гг. определило появление первых злоумышленников, взламывающих компьютерные

²⁵⁰ Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. Указ. соч. С. 58.

²⁵¹ Воробьева А. А., Пантюхин И. С. История развития программно-аппаратных средств защиты информации. СПб. : Университет ИТМО, 2017. С. 11.

системы и осуществляющих доступ к личным данным пользователей и, преимущественно, движимых любопытством, желанием исследовать новые для них возможности использования информационно-телекоммуникационных технологий. Указанный этап характеризуется постепенным распространением компьютерных сетей, что обусловило распространение вирусного программного обеспечения и зарождение первых сетевых атак²⁵².

Глобализация сети «Интернет» в 1990–2000 г.г. создала единое информационное пространство, доступное практически каждому пользователю, что обусловило появление таких актуальных даже на сегодняшний день видов преступлений, как фишинг, распространение вредоносного программного обеспечения в телекоммуникационных сетях, атаки на веб-ресурсы²⁵³, кража данных с электронных банковских счетов и пр. Также в указанный период зародился теневой рынок сети даркнет.

Следующий этап связан с использованием мобильных средств связи, веб-сайтов и социальных сетей в 2000–2020 г.г. Так, смартфоны с возможностью скоростной передачи данных стали неотъемлемой частью жизни общества, что привело к массовому их использованию, и, как следствие, распространению преступлений рассматриваемого вида в геометрической прогрессии²⁵⁴.

Современный этап характеризуется развитием сложных и целевых кибератак, направленных на проникновение в конкретные системы и кражу конфиденциальной информации отдельно взятой личности. Также широко распространяется возможность использования искусственного интеллекта для автоматизации атак, синтетической генерации контента в целях установления с жертвой доверительных отношений и последующего совершения противоправных деяний или дезинформации общества. Кроме указанных явлений широко распространяются различные цифровые активы, позволяющие анонимно осуществлять финансирование противоправной деятельности, атаки на IoT-устройства²⁵⁵ и т. п., широкое распространение получают распределенные реестры и квантовые вычислительные среды.

²⁵² Tzavara V., Vassiliadis S. Tracing the evolution of cyber resilience: a historical and conceptual review // *International journal of information security*. 2024. V. 23. P. 12.

²⁵³ Florido-Benitez L. The types of hackers and cyberattacks in the aviation industry // *Journal of transportation security*. 2024. V. 17. P. 17.

²⁵⁴ Radoniewicz F. *Cyberspace, cybercrime, cyberterrorism*. Cham : Springer, 2024. P. 35.

²⁵⁵ Lundberg E., Mozeliuss P. The potential effects of deepfakes on news media and entertainment // *AI & Society*. 2024. V. 1. P. 2.

Отдельного внимания заслуживает появление метавселенных, которые создают новые возможности совершения преступлений в сфере компьютерной информации, таких как мошенничество с цифровыми аватарами пользователей, виртуальное насилие, кража виртуальных активов и пр., а также взлом широко внедряемых в различные сферы биометрических систем распознавания и нейроинтерфейсов.

История развития криминалистики, как и любой другой науки, представляет собой систему фактов, позволяющих не только проследить закономерности становления научного знания, но и определить пути дальнейшего его совершенствования²⁵⁶. Прогностика как специальная отрасль знаний изучает общие принципы построения методов прогнозирования развития объектов любой природы и закономерности процесса разработки прогнозов. Целью прогностики является создание рабочих методов научного предвидения в целях обоснованного предположения о необходимости или вероятности наступления событий, процессов, которые либо еще не произошли, либо существуют, но еще не наблюдаются²⁵⁷.

Предиктивный анализ, обеспечиваемый на сегодняшний день уже типовыми технологическими решениями, построенными на базе искусственного интеллекта, облачных технологий, распределенных баз данных и пр., становится частью общественного сознания²⁵⁸. Так, появление новых форм преступлений в сфере компьютерной информации будет обусловлено сложным взаимодействием технологических, социальных, экономических и политических факторов. Рассмотрим основные ее детерминанты. Среди технологических факторов стоит отметить возможности генеративного искусственного интеллекта (от англ. «generative AI» – системы на базе искусственного интеллекта), позволяющие создавать синтетически сгенерированный контент в виде текста, изображений, аудио- и видеофайлов на основе текстовых запросов (промптов), способного принести значительные преимущества, одновременно увеличивая риски угроз безопасности. Являясь технологией с открытым исходным кодом, он способствует быстрому распространению за счет снижения барьеров на пути к созданию генеративных моделей, одновременно становясь платформой для создания новых

²⁵⁶ Криминалистика: история и перспективы развития : монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. М. : Юрайт, 2024. С. 47.

²⁵⁷ Аверьянова Т. В. Криминалистика. Указ. соч. С. 131.

²⁵⁸ Сологубова Г. С. Составляющие цифровой трансформации : монография. М. : Юрайт, 2024. С. 38.

средств совершения преступлений.

По прогнозам ЗАО «Лаборатория Касперского»²⁵⁹ основными угрозами и трендами в области киберпреступности станут новые методы использования генеративного искусственного интеллекта для обмана населения путем генерации мультимедийных материалов на основе реальных кадров – дипфейков.

К предполагаемым рискам в отношении генеративного искусственного интеллекта можно отнести манипулирование сознанием населения с помощью синтетического контента, распространение дезинформационных сообщений и подрыв доверия к информации в целом (путем использования гиперреалистичных ботов и синтетически сгенерированных моделей, влияющих на общественный настрой), внедрение в киберфизические системы (интеграция в критически важные системы и инфраструктуру чревата утечкой конфиденциальных данных, появлением предвзятых алгоритмов, нарушением процессов управленческих решений ввиду неэффективных мер обеспечения информационной безопасности), подготовку и проведение масштабных кибератак с помощью специально разработанных методов фишинга или тиражирования вредоносного программного обеспечения (искажение обучающих данных («отравление данных»), хайджекинг выходных данных модели («внедрение промптов»), извлечение конфиденциальных обучающих данных («инверсия модели»), искажение информации («возмущение») и незаконное использование вычислительных мощностей)²⁶⁰ и пр.

Значимыми представляются угрозы не только в индексируемой сети «Интернет» (от англ. «open web» – белый или открытый «Интернет»), но и в неиндексируемой глубокой сети (от англ. «deep web» – «глубокий «Интернет») и сети даркнет (от англ. «dark web» – темный «Интернет»).

Указанные области информационно-телекоммуникационной сети содержат криминалистически значимую информации, которая может быть ценной для расследования, по этой причине важно понимание всех возможностей использования тех или иных инструментов и методов исследования цифровых

²⁵⁹ Тренды киберугроз будущего // Акционерное общество «Лаборатория Касперского» : офиц. сайт. URL: <https://www.kaspersky.ru/blog/cyberthreats-and-trends-predictions-in-2025/38852> (дата обращения: 11.01.2025).

²⁶⁰ Информационно-аналитический отчет «Риски безопасности генеративного искусственного интеллекта» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации – ФГБУ «Научно-исследовательский институт «Интеграл» : офиц. сайт. URL: <https://digital.gov.ru/ru/ministry/departments/46> (дата обращения: 08.02.2025).

доказательств²⁶¹.

Кроме того, возрастает роль использования моделей на основе искусственного интеллекта для разработки сложного и адаптивного вредоносного программного обеспечения, автоматизации процессов кибератак, управления трудно обнаруживаемыми ботнетами. При этом большинство имеющихся на сегодняшний день технологий и методов шифрования данных позволят обойти развивающиеся технологии квантовых вычислений, а увеличение количества IoT-устройств и API-интерфейсов в области прикладного программирования создаст множество дополнительных уязвимостей и точек воздействия для преступников. Среди технологических факторов все чаще выделяют появление еще сложно воспринимаемых в реальности, но распространяющихся в метaprостранстве, генерируемом с задействованием элементов дополненной реальности, преступных схем, связанных с виртуальными активами и цифровыми аватарами. Метавселенные порождают относительно новые виды преступных деяний (кража виртуальной собственности, идентификатора личности, виртуальный вандализм, кибербуллинг, виртуальные домогательства и насилие с использованием аватаров).

Постиндустриальная информационная среда обеспечивает широкие возможности для создания многочисленных и мощных баз данных, легкость распространения информации, простоту ее копирования, агрегирования и модификации, что способствует появлению новых информационных угроз для отдельно взятого человека²⁶². Соответственно, среди социальных факторов можно выделить увеличение зависимости общества от информационно-телекоммуникационных технологий, что делает его более уязвимым к атакам преступников, относительно низкий уровень грамотности населения в области информационных технологий, сложность восприятия принципов построения вновь возникающих технических средств и киберфизических систем, а также распространение деструктивных сведений в информационном пространстве и т. п.

Экономические факторы обусловлены увеличением объемов электронной торговли, развитием сервисов онлайн-банкинга и виртуальных финансовых инструментов, что создает новые платформы совершения преступлений в сфере компьютерной информации не только в «белом» интернете, но и в сети даркнет.

²⁶¹ Усов А. И. Стандарты судебной экспертизы как инструмент цифровизации криминалистики // Современные технологии и подходы в юридической науке и образовании : сборник материалов международного научно-практического форума. Калининград : Балтийский федеральный университет им. Иммануила Канта, 2021. С. 214.

²⁶² Малащенко А. В., Нисневич Ю. А., Рябов А. В. Становление постиндустриальной цивилизации: от цифровизации до варварства : монография. М. : Юрайт, 2024. С. 90.

Отдельного внимания заслуживают такие политические факторы как использование кибератак в качестве инструмента для достижения стратегических целей. Так, например, осуществлять разведку и сбор информации все чаще приходится с задействованием широкого спектра информационно-телекоммуникационных технологий и технических средств, соответственно, усиление геополитической напряженности может приводить к росту кибершпионажа между государствами. Нельзя оставить без внимания ряд организационных факторов, которые определяют недостаток квалифицированных специалистов в области противодействия преступлениям в сфере компьютерной информации, а также сложность их расследования, поиска, собирания и анализа цифровых доказательств, а также определения ответственности в информационном пространстве. Все вышеперечисленные факторы создают сложную и довольно динамичную среду, в которой будут развиваться новые формы преступлений в сфере компьютерной информации в будущем.

Одной из особенностей постнеклассической науки является интеграция гуманитарных, естественных и технических наук²⁶³, по этой причине, предполагается, что для эффективной борьбы с преступлениями в сфере компьютерной информации необходимы комплексные меры, включающие задействование информационно-телекоммуникационных технологий, усиление мер обеспечения информационной безопасности, повышение осведомленности населения и квалификации специалистов в области раскрытия и расследования рассматриваемого вида преступных деяний, а также совершенствование правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации, налаживание международного сотрудничества.

С точки зрения Р. С. Белкина, существуют три этапа формирования и развития криминалистики²⁶⁴: консолидация первых криминалистических рекомендаций и формулирование научных методов расследования; выделение криминалистики как самостоятельной области научного познания; развитие частных криминалистических теорий.

Активная интеграция информационных технологий в криминалистику подразумевает цифровизацию применяемых технико-криминалистических средств в целях раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, технических средств и

²⁶³ Садохин А. П. Концепции современного естествознания. М. : Юнити-Дана, 2006, С. 14.

²⁶⁴ Белкин Р. С. История отечественной криминалистики. М. : Норма, 1999, С. 476.

различных информационных систем в цифровой среде²⁶⁵, определяя так называемый четвертый этап развития криминалистики («Криминалистика 4.0»²⁶⁶), однако, формирующееся в наши дни направление развития Индустрии 5.0²⁶⁷ в свете формирования цифровых двойников объектов, явлений или процессов, прогнозирования и принятия решений на основе искусственного интеллекта, технологий компьютерного зрения, машинного обучения и интеграции больших языковых моделей вполне позволяет определить принципиально новый подход направления противодействия современным преступлениям и именовать его подходом «Криминалистика 5.0» (данный подход будет рассмотрен подробнее в главе 4).

Соответственно, базовым механизмом противодействия деструктивным формам в исследуемой области является разработка технических средств, широко освещаемых зарубежными источниками в доктринальной концепции «Юридические технологии» (описывающей систему знаний о юридико-технических средствах, приемах и способах применения, совершенствования и систематизации различных правовых инструментов), и именуемых «LegalTech-инструментами» (от англ. «legal technology» – технологичные решения в области информационно-технического обеспечения юридической деятельности)²⁶⁸. Наряду с указанными средствами целесообразно развитие таких направлений системы «Юридических технологий» как «CrimeTech» (от англ. «crime technology» – современные решения на основе информационно-телекоммуникационных технологий, используемые в преступных целях) и «DeepTech» (от англ. «deep technology» – инновационные информационно-телекоммуникационные технологии, принятые на вооружение преступниками, но требующие значительных временных и экономических затрат для оказания противодействия им).

Криминалистическое прогнозирование основано на познании закономерностей развития преступности и методов противодействия ей и опирается на экстраполяцию знаний, используя такие методы научного познания

²⁶⁵ Каминский А. М. Криминалистическая категория «след преступления» в анализе правонарушений в сфере компьютерной информации // Уголовно-правовые, уголовно-процессуальные и криминалистические вопросы борьбы с преступностью : сборник трудов V Всероссийской научно-практической конференции. Краснодар : КГАУ, 2021. С. 169.

²⁶⁶ Нестеров А. В. Виртуальные следы в криминалистике. М.: КноРус», 2024. С. 52.

²⁶⁷ Индустрия 5.0 : На пути к устойчивой, ориентированной на человека парадигме // Европейский союз : офиц. сайт. URL: <https://op.europa.eu/en/publication-detail/publication/468a892a-5097-11eb-b59f-01aa75ed71a1> (дата обращения: 27.05.2025).

²⁶⁸ Dariusz S., Mariusz Z. Legal tech: information technology tools in the administration of justice. Baden-Baden : Nomos Verlagsgesellschaft GmbH & Co KG, 2021. P. 18.

как индукция, дедукция, аналогия и моделирование.

Результатом прогнозирования должна быть система аргументированных представлений о возможных изменениях в преступности, а также средствах и методах ее предупреждения. Отправной точкой для криминалистического прогнозирования является генезис преступлений, совершаемых в сфере компьютерной информации, а основанием для прогноза служат теоретические знания о закономерностях развития преступности в совокупности со знаниями смежных научных дисциплин. Источниками данных для прогнозирования служат общие и частные криминалистические теории, статистические данные в виде количественных показателей преступности и ее раскрываемости, информация о новых способах совершения преступлений, недостатках существующих методов расследования и перспективах новых криминалистических средств.

Таким образом, история становления преступлений в сфере компьютерной информации является отражением развития информационно-телекоммуникационных технологий, причем каждый новый этап их развития позволял создавать новые возможности для совершения преступных деяний, что, в свою очередь, побуждало к разработке новых методов противодействия им. Анализ исторических факторов позволяет не только понять природу преступлений в сфере компьютерной информации, но и ее тенденции с наиболее уязвимыми областями в целях разработки эффективных стратегий противодействия ей в будущем.

Основными причинами возникновения и широкого распространения преступлений в сфере компьютерной информации являются повсеместный рост использования информационно-телекоммуникационных технологий и различных онлайн-сервисов, переход к цифровой экономике, развитие технических средств и технологий обезличивания в киберсреде и т. п. при сравнительно низком уровне цифровой грамотности населения и, как следствие, недостаточной защищенности личных данных пользователей. Существенной проблемой является использование интернет-пространства для политических и экономических манипуляций наравне с относительной легкостью анонимного совершения рассматриваемых преступлений и, в большей части, безнаказанности за совершенные деяния.

Факторами, способствующими появлению новых форм преступлений в сфере компьютерной информации, выступают: стабильное увеличение количества пользователей, использующих информационно-телекоммуникационные технологии; широкое внедрение технологий искусственного интеллекта и квантовых вычислений в повседневную деятельность человека; развитие

метавселенных, а также цифровых активов²⁶⁹. Дальнейшая эволюция способов совершения преступлений в сфере компьютерной информации будет обусловлена относительно легкой разработкой и внедрением различных ботнетов, в том числе на основе моделей искусственного интеллекта для совершения кибератак, применением квантовых алгоритмов для взлома защищенных систем, расширенных методов социальной инженерии и иммерсивного воздействия для манипуляции персональными данными граждан.

Поэтому одним из перспективных направлений в системе юридических технологий является разработка и совершенствование криминалистического обеспечения расследования преступлений, в частности, технико-криминалистических средств и информационных систем, которые могли бы учитывать не только текущие угрозы, но и новые, перспективные в плане появления, формы. Одной из основных задач, решаемых подобными инструментами, является обнаружение, фиксация, изъятие и исследование цифровых доказательств, а также автоматизация процесса расследования и обеспечение целостности собранной информации, что позволяет определить ключевым для ее реализации новый стек индустрий Web 4.0 и Web 5.0, представленными технологиями искусственного интеллекта, распределенного реестра, сверхвысокой передачи данных 5G, Интернета вещей, а также виртуальной и дополненной реальности.

²⁶⁹ Харисова З. И., Лонцакова А. Р. Обеспечение прав и свобод гражданина в области использования цифровых финансовых активов // Евразийский юридический журнал. 2020. № 3 (142). С. 167.

ГЛАВА 2. КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ОСНОВЫ ИССЛЕДОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

2.1. Криминалистические средства расследования преступлений в сфере компьютерной информации

В истории науки результатом взаимопроникновения различных областей знания нередко становилось рождение нового направления научных исследований. Наглядный тому пример – наука криминалистика, возникшая как результат интеграции уголовного права, уголовного процесса с достижениями естественных и технических наук²⁷⁰. Криминалистика с момента своего возникновения была направлена на разработку средств и методов для их практического применения, что изначально давало основания считать ее прикладной дисциплиной. Характеристика «прикладная наука», с одной стороны, подчеркивала ее принадлежность к естественно-техническим дисциплинам, достижения которых ею адаптировались для решения собственных задач²⁷¹, с другой стороны, определяла науку, способную своими достижениями удовлетворить практические потребности в иных областях знаний.

На сегодняшний день криминалистическая наука оперирует рядом устоявшихся фундаментальных категорий, которые формируют ее основу в виде теоретического аппарата и методологических подходов. К числу основных криминалистических категорий относят такие понятия как криминалистическое (технико-криминалистическое) средство, криминалистические прием и рекомендация, тактическая комбинация (операция), следственная ситуация, тактическое решение, способ совершения и сокрытия преступления, криминалистическая характеристика преступного деяния и иные концепты.

Рассматривая преступления в сфере компьютерной информации необходимо отметить, что одним из важнейших элементов механизма его совершения является способ, значимость выявления которого обусловлена необходимостью установления следовой картины. Данный элемент весьма специфичен, поскольку по рассматриваемому виду преступных деяний, как правило, преобладают

²⁷⁰ Криминалистика. Теоретический курс. Указ. соч. С. 28.

²⁷¹ Гончаренко В. И. Использование данных естественных и технических наук в уголовном судопроизводстве. М. : Высшая школа, 1980. С. 19.

цифровые (электронные) следы. Свойство отражения, присущее всем видам и формам материи, заключается в том, что каждый объект материального мира в процессе взаимодействия с окружающей средой подвергается воздействию внешних факторов. Известно, что отражение присутствует всегда, когда происходит взаимодействие двух и более материальных объектов – объектов следообразования. Поэтому основой для распознавания способа совершения преступления в сфере компьютерной информации служит следовая картина в виде материальных (поскольку отражаются на материальных объектах) цифровых следов²⁷², механизм следообразования которых является электронным или электромагнитным. Указанные цифровые следы возможно определить исключительно с использованием технико-криминалистических средств, под которыми понимают технические инструменты, специально разработанные, приспособленные или заимствованные с целью обнаружения, фиксации, изъятия или исследования доказательств, либо для предотвращения преступлений.

Применение того или иного технико-криминалистического средства определяет технико-криминалистический и тактико-криминалистический (тактический) приемы. Криминалистическая методика, в свою очередь, объединяет положения криминалистической техники и криминалистической тактики применительно к конкретным условиям или задачам расследования конкретного вида преступлений и содержит систему научных положений и разрабатываемых на их основе рекомендаций по организации и осуществлению расследования и предотвращения преступлений²⁷³. Техничко-криминалистические средства в совокупности с приемами криминалистических техники и тактики аккумулируются в криминалистической методике в соответствии с особенностями расследования конкретного вида преступного деяния²⁷⁴. Соответственно, для решения той или иной криминалистической задачи выбирается наиболее эффективное технико-криминалистическое средство²⁷⁵, позволяющее достигнуть наилучших результатов расследования в оптимальные сроки, что соотносимо с основными специальными задачами науки криминалистики. К числу ее

²⁷² Россинская Е. Р. Особенности оценки и использования в доказывании результатов судебных экспертиз в условиях цифровизации // Законы России: опыт, анализ, практика. 2021. № 3. С. 2; Майлис Н. П. Инновационные технологии, способствующие развитию цифровой трасологии // Вестник Московского университета МВД России. 2024. № 5. С. 97.

²⁷³ Баев О. Я. Избранные работы : в 2 т. Воронеж : Издательство Воронежского государственного университета, 2011. Т. 2. С. 6.

²⁷⁴ Аверьянова Т. В. Криминалистика. Указ. соч. С. 665.

²⁷⁵ Josang A. Cyber organizational structures and regulation. Cybersecurity. Cham : Springer, 2025. P. 360.

дополнительных специальных задач также относят: привлечение данных естественных и технических наук в целях оптимизации научно-технического обеспечения раскрытия и расследования преступлений; совершенствование имеющихся технико-криминалистических средств и применяемых тактических приемов, методических рекомендаций; анализ практики с целью выявления потребностей в новых средствах, а также установления степени надежности и перспективности тех, которые были ранее рекомендованы к внедрению²⁷⁶.

Не менее важной частью предмета криминалистики являются непосредственно методы и средства раскрытия и расследования преступлений, исследования доказательств по делам, а также вопросы профилактики преступных деяний. Для криминалистического исследования технических средств, информационных систем и компьютерной информации необходим комплекс знаний, сформированный на базе теории информационно-компьютерного обеспечения криминалистической деятельности²⁷⁷. Предметом входящего в указанную теорию учения о криминалистическом исследовании компьютерных средств и систем является система закономерностей собирания криминалистически значимой информации, анализ которой предполагает разработку технико-криминалистических методов и средств, а также методик и приемов обнаружения, фиксации и изъятия цифровых доказательств.

Криминалистическая техника, как раздел науки, представлена, прежде всего, системой знаний о закономерностях объективной действительности, составляющих научную основу разработки технико-криминалистических средств, приемов и методов, предназначенных для использования в раскрытии и расследовании преступлений²⁷⁸. Развитие информационных технологий постоянно опережает развитие правовых рамок, создавая разрыв между возможностями преступников и инструментами, доступными правоохранительным органам. Этот диссонанс подчеркивает необходимость адаптации правовых механизмов к динамической природе киберугроз²⁷⁹, а сложность идентификации преступников и собирания доказательственной базы требует совершенствования

²⁷⁶ Курс криминалистики. Указ. соч. Т. 1. С. 37.

²⁷⁷ Россинская Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии // Вестник Университета имени О. Е. Кутафина. 2022. № 2 (90). С. 35.

²⁷⁸ Зеленский В. Д., Меретуков Г. М. Криминалистика. Санкт-Петербург : Юридический центр-Пресс, 2015. С. 115.

²⁷⁹ Amoo O., Atadoga A., Abrahams T. The legal landscape of cybercrime: a review of contemporary issues in the criminal justice system // World journal of advanced research and reviews. 2024. № 21 (02). P. 208.

криминалистических методов и средств расследования, что, в свою очередь, сонаправлено наиболее актуальным на сегодняшний день научно-исследовательским приоритетам в области криминалистики²⁸⁰, а именно: разработке и своевременной модернизации технико-криминалистических средств, тактических приемов и методологических алгоритмов обнаружения, фиксации, изъятия и исследования криминалистически значимой информации; оптимизации технико-криминалистических средств, соответствующих новым методам расследования и предотвращения преступной деятельности; развитию общих и частных криминалистических теорий как теоретико-методологической базы формирования системы технико-криминалистических средств и методов судебного исследования.

Четвертый этап развития криминалистики («Криминалистика 4.0»), связанный с цифровизацией применяемых технико-криминалистических средств в целях раскрытия и расследования преступлений, соответствует вышеуказанным научно-исследовательским приоритетам. Формирование информации о противоправном деянии и его субъектах выступает системообразующим элементом, опосредующим взаимосвязь между криминальной активностью и процессуально-познавательной деятельностью.

Криминалистика рассматривает деятельность по раскрытию и расследованию преступлений как процесс трансформации криминальной информации в доказательственную посредством поиска доказательств, их исследования и дальнейшей оценки. Способы совершения преступлений в сфере компьютерной информации в зависимости от доступа к техническим средствам и информационным системам можно подразделить на способы, связанные с непосредственным доступом и удаленным (посредством использования информационно-телекоммуникационной сети), в других случаях вовлечение потерпевшего, в той или иной степени, является необходимым условием доведения преступных намерений до конца²⁸¹. Соответственно, способ совершения преступлений определяет одну из главнейших ролей на стадии возникновения информации о преступном деянии, поскольку он, будучи отражаемым объектом, в то же время своими составляющими (действия, используемые средства для совершения действий) отражается в среде события преступления.

²⁸⁰ Аверьянова Т. В. Криминалистика. Указ. соч. С. 66.

²⁸¹ Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3 (148). С. 91.

Таким образом, можно сделать вывод, что рассмотренные выше категории составляют ключевые элементы упрощенной модели, отражающей последовательность этапов расследования преступления в сфере компьютерной информации, которую можно идентифицировать как каскадную модель жизненного цикла программного обеспечения²⁸², заимствованную из методологии создания информационных систем, включающей их планирование, разработку, тестирование и развертку (от англ. «software development life cycle²⁸³» – жизненный цикл разработки программного обеспечения)²⁸⁴.

Сущность метода моделирования состоит в том, что объект, прямое (непосредственное) исследование которого невозможно или нецелесообразно по различным причинам, изучается посредством специально созданной модели²⁸⁵, которая является заменителем объекта в процессе познания²⁸⁶. Под моделью понимается воспроизведение реальной системы (объекта или процесса) в материальном или абстрактном виде²⁸⁷. В ходе расследования замена исходного объекта моделью позволяет провести его косвенное изучение через анализ упрощенного аналога. Так, в рассматриваемой модели способ совершения преступления, как исходный вектор, влияет на тип оставляемых цифровых следов²⁸⁸. Цифровые следы, в свою очередь, обнаруживаются использованием технико-криминалистических средств, которые определяют методику расследования преступлений в сфере компьютерной информации, алгоритм действий для поиска и собирания доказательств и их дальнейшей юридической интерпретации.

²⁸² Зараменских Е. П. Управление жизненным циклом информационных систем : монография. Новосибирск : Центр развития научного сотрудничества, 2014. С. 14.

²⁸³ Benington H. D. Production of large computer programs // *Annals of the history of computing*. 1983. V. 5. № 4. P. 356.

²⁸⁴ Харисова З. И. Оптимизация процесса поиска, анализа и интерпретации цифровых доказательств с использованием алгоритмов искусственного интеллекта // *Общество, право, государственность: ретроспектива и перспектива*. 2025. № 3 (23). С. 60.

²⁸⁵ Li J. Multi-governance model of new cybercrime under the risk of new technologies risks and responses // *Lecture notes in education psychology and public media*. 2024. V. 73. № 1. P. 26.

²⁸⁶ Лузгин И. М. Моделирование при расследовании преступлений. М. : Юридическая литература, 1981. С. 7; Волчецкая Т. С. Теоретические проблемы использования метода моделирования в криминалистической науке // *Социальные и гуманитарные науки на Дальнем Востоке*. 2012. № 4 (36). С. 17.

²⁸⁷ Лозовский Д. Н. Использование метода криминалистического моделирования в процессе расследования преступлений // *Проблемы экономики и юридической практики*. 2010. № 1. С. 115; Chechulin A., Gorda M. Cybercrime investigation model // *2024 16th International conference on communication systems and networks*. 2024. № 22. P. 37.

²⁸⁸ Jain R., Sonowal B. Analyzing the procedure for investigation in cybercrime and admissibility of electronic evidence. *Cybercrime unveiled*. Cham : Springer, 2025. P. 288.

Модель представленного вида является динамичной, элементы ее находятся в тесной взаимосвязи. Изменение исходного вектора в виде способа совершения преступления должно закономерно влиять на все последующие этапы, обеспечивая их непрерывное совершенствование.

Правовые основания применения технико-криминалистических средств представляют собой систему закрепленных норм и принципов, определяющих условия допустимости их задействования и порядок процессуального оформления фактов их использования. Применение рассматриваемых средств осуществляется исключительно при наличии правовых оснований для их использования. В то же время УПК РФ не содержит четкого определения данных средств, хотя их применение прямо упоминается несколько раз. Так, возможность применения технико-криминалистических средств при проведении следственных действий закреплена ч. 6 ст. 164 УПК РФ с обязательным уведомлением об их использовании участников процесса, а также п. 33 ч. 1 ст. 13 Федерального закона от 07 февраля 2011 г. № 3-ФЗ «О полиции»²⁸⁹, в соответствии с которым полиция вправе применять специальные технические средства в случае, если они не наносят вред жизни и здоровью граждан и окружающей среде. Дополнительное регулирование содержится в ведомственных актах, таких как приказ МВД России от 28 апреля 2023 г. № 260 «Об организации научной и научно-технической деятельности в системе Министерства внутренних дел Российской Федерации»²⁹⁰, в котором к научно-техническим разработкам относят аппаратно-программные комплексы, автоматизированные информационные системы, программные средства, программно-технические средства и базы данных.

Однако законодательство не в полной мере определяет перечень субъектов, уполномоченных применять технико-криминалистические средства, исходя из анализа УПК РФ и Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»²⁹¹ можно выявить, что ими являются суд, следователи, дознаватели, оперативные сотрудники, а также эксперты и

²⁸⁹ О полиции : Федеральный закон от 07 февраля 2011 г. № 342-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_110165 (дата обращения: 22.10.2025).

²⁹⁰ Об организации научной и научно-технической деятельности в системе МВД России : приказ МВД России от 28 апреля 2023 г. № 260 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=exp&n=824308#lw8jkuu8yvnolnff1> (дата обращения: 22.02.2025).

²⁹¹ Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_7519 (дата обращения: 01.04.2025).

специалисты, привлекаемые к процессу на основании ст. 58, 168 и 270 УПК РФ.

По принципу допустимости критериями возможности применения технико-криминалистических средств являются научная обоснованность, законность, безопасность и этичность. Научная обоснованность подразумевает соответствие технико-криминалистических средств современным научным требованиям. Законность обеспечивается нормативным закреплением их применения, безопасность – запретом использования средств, создающих угрозу жизни и здоровью, а этичность – недопустимостью насилия и унижения человеческого достоинства.

Процессуальное закрепление использования технико-криминалистических средств является обязательным. В соответствии со ст. 166 УПК РФ каждый факт их применения фиксируется в протоколе, который в обязательном порядке должен содержать сведения о средствах, объектах исследования и полученных результатах. Согласно ст. 190 УПК РФ, результаты, полученные с использованием технико-криминалистических средств, подлежат приобщению к материалам дела. Созданные или приспособленные для решения криминалистических задач средства в узком смысле определяют криминалистическую технику, которая занимается вопросами разработки понятийного аппарата и классификаций объектов исследования и их признаков. Так, например, на основе проведенной классификации папиллярных узоров возможно применение средств криминалистической идентификации, а на классификации внешних признаков человека базируется метод словесного портрета.

Классификация, являясь основой таксономии (учения о принципах и практике систематизации сложноорганизованных сущностей²⁹²), играет особую роль для развития любой дисциплины. Применительно к криминалистике систематизация знаний о технико-криминалистических средствах определяет эффективность системы противодействия преступлениям. В частности, классификация технических способов собирания и исследования доказательств способствует правильному их выбору в зависимости от сложившейся следственной ситуации, сложности задач и организационных возможностей²⁹³.

По криминалистическим основаниям технико-криминалистические средства можно классифицировать по²⁹⁴:

- целевому назначению средств, приемов и методов (для обнаружения,

²⁹² Большая советская энциклопедия : в 30 т. М. : Советская энциклопедия, 1976. Т. 25. С. 220.

²⁹³ Эксархопуло А. А. Криминалистика. Указ. соч. С. 149.

²⁹⁴ Криминалистика. Теоретический курс. Указ. соч. С. 335.

фиксации, изъятия и исследования доказательств, а также для предотвращения или предупреждения преступлений);

- субъектам применения средств и методов (для следователей, оперативных работников, экспертов, специалистов и т. д.);

- степени специализации средств, приемов и методов (узкоспециализированные средства, то есть выполняющие только одну функцию и универсальные средства, имеющие две и более функций);

- по происхождению средств, приемов и методов (специальные криминалистические средства (созданные криминалистикой), средства, созданные в других отраслях науки и техники и приспособленные криминалистикой для решения задач, и общетехнические средства, заимствованные криминалистикой без каких-либо изменений для использования в криминалистических целях);

- по отрасли знания, данные которой положены в основу технико-криминалистических средств (приемов и методов) различают физические, химические, биологические, кибернетические (программные) и пр. средства.

По правовым основаниям технико-криминалистические средства можно подразделить на три группы: по сфере применения, по доказательственному значению и по правовой регламентации.

Так, по сфере применения указанные средства могут быть разделены на используемые в оперативно-розыскной, следственной и экспертной деятельности, а также в деятельности специалиста.

По доказательственному значению результатов применения технико-криминалистические средства можно разделить на средства, результаты применения которых могут иметь значение доказательств (средства фиксации) и средства, результаты применения которых имеют в основном вспомогательное значение и могут быть использованы в оперативных целях, для выдвижения версий, планирования расследования и т. д.²⁹⁵.

По правовой регламентации технико-криминалистические средства можно подразделить на: средства, применение которых в силу закона обязательно (например, обязательная фиксация с помощью технических средств хода и результатов следственного действия, проводимого без понятых (ч. 1.1. ст. 170 УПК РФ)); технические средства, применение которых допустимо законом (например, применение киносъемки, звуко- или видеозаписи при допросе (ч. 4 ст. 189 УПК) и др.; технические средства, применение которых допустимо в силу отсутствия запрета на их использование (в силу общих положений о допустимости применения

²⁹⁵ Криминалистика. Теоретический курс. Указ. соч. С. 337.

средств, изложенных в ст. ст. 9, 164. УПК РФ и др)²⁹⁶. Соответственно, по функциональной направленности можно выделить технико-криминалистические средства, используемые в целях²⁹⁷: выявления и раскрытия преступлений; расследования преступных деяний и проведения следственных действий; предотвращения преступлений; ведения криминалистических учетов; организации противодействия преступлениям и научной организации труда следователя; обеспечения безопасности участников уголовного процесса. Перечисленный перечень криминалистически значимых оснований общего характера далеко не исчерпывающий, что обусловлено постоянным развитием криминалистической техники за счет создания новых инструментов, динамикой законодательства, регламентирующего их применение и динамикой преступности, в борьбе с которой они используются. Техничко-криминалистические средства можно классифицировать группировкой, отражающей возможности их использования²⁹⁸.

При рассмотрении преступлений в сфере компьютерной информации возможна систематизация знаний методом «от обратного» – допустимо выявить применимость того или иного средства на основе имеющихся представлений о свойствах цифровых доказательств. В связи с этим целесообразно выявление и систематизация современных технико-криминалистических средств, использование которых позволит определить наиболее эффективную тактику подготовки и проведения отдельных следственных действий исходя из складывающихся по преступлению в сфере компьютерной информации обстоятельств. Техничко-криминалистические средства включают в себя широкий круг аппаратных, программно-аппаратных и программных средств, которые могут быть классифицированы по различным основаниям. В соответствии с этим могут быть построены различные взаимосвязанные классификации, исходящие из разных криминалистически значимых классификационных критериев²⁹⁹. Имеющиеся на сегодняшний день технико-криминалистические средства, применение которых целесообразно при расследовании преступлений в сфере компьютерной информации, можно классифицировать по характеру воздействия на информацию, уровню автоматизации расследования, источнику получаемой информации, цели применения и функциональному назначению. Так, по характеру воздействия на

²⁹⁶ Криминалистика. Теоретический курс. Указ. соч. С. 337.

²⁹⁷ Федоров Г. В., Григорович В. Л. Инновационные направления развития криминалистики : монография. М. : Юрлитинформ, 2012. С. 49.

²⁹⁸ Выявление причин преступности и предупреждение преступлений. Общие положения / под. ред. П. Ф. Гришанина. М. : НИИРПО МВШ МООН СССР, 1967. С. 114.

²⁹⁹ Поляков В. В Криминалистическая классификация средств высокотехнологичных преступлений // Вестник Санкт-Петербургского государственного университета. Право. 2024. № 2. С. 3.

информацию указанные средства можно подразделить на:

- пассивные, не оказывающие воздействия на исследуемую криминалистически значимую компьютерную информацию и направленные на поиск и исследование существующих данных (анализ сетевого трафика или дампов памяти, мониторинг веб-ресурсов и пр.);
- активные, предполагающие непосредственное воздействие на исследуемую информацию с целью проверки выдвинутых версий (динамический анализ вредоносного кода, внедрение сетевых «ловушек» и пр.);
- комбинированные, включающие возможности как активных, так и пассивных средств (например, использование сетевых анализаторов для пассивного сбора трафика с последующим активным анализом полученных данных³⁰⁰ и т. п.).

По уровню автоматизации расследования рассматриваемых преступлений технико-криминалистические средства можно классифицировать на:

- неавтоматизированные (требующие для выполнения действий участия следователя или специалиста (например, ручной анализ лог-файлов, исследование исходного кода вредоносного программного обеспечения³⁰¹ и т. п.));
- автоматизированные (на базе программного обеспечения, функционирующего по настраиваемому пользователем алгоритму (например, избирательное восстановление удаленных файлов и их последующий анализ));
- автоматические (на базе программных средств, функционирующих по заранее определенному жесткому алгоритму (это могут быть SIEM-системы (от англ. «security information and event management – система управления информационной безопасностью и событиями безопасности»)³⁰² или антивирусные программы, используемые для обнаружения вредоносных объектов и пр.).

По источнику получаемой информации можно выделить технико-криминалистические средства, направленные на анализ:

- криминалистически значимой информации в компьютерах, мобильных средствах связи, серверных станциях и других устройствах³⁰³ (анализ файловой структуры, реестра операционной системы устройства и пр.);

³⁰⁰ Hartono W. Challenges of criminal investigation cybercrime // Awang long law review. 2024. V. 7. № 1. P. 12.

³⁰¹ Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования. Указ. соч. С. 700.

³⁰² Jajodia S., Samarati P., Yung M. SIEM system. Encyclopedia of cryptography, security and privacy. Cham : Springer, 2025. P. 1022.

³⁰³ Gomathy C. K. Cybercrime in the era of mobile and wireless devices // International journal of scientific research in engineering and management. 2024. V. 8. № 9. P. 3.

- сетевого трафика или предполагающие получение данных из информационно-телекоммуникационной сети, протоколов обмена файлами и пр. (например, захват и анализ сетевого трафика, анализ DNS-запросов и пр.);

- данных из облачных хранилищ, которые направлены на получение сведений из удаленно расположенных серверов (например, анализ активности пользователей в облачном хранилище поставщика услуг средствами специализированного программного обеспечения и т. п.);

- сведений из общедоступных баз данных и ресурсов сети «Интернет» (OSINT-разведка, от англ. – «open source intelligence» – инструменты для получения и анализа информации из открытых источников³⁰⁴).

По цели применения можно рассматривать технико-криминалистические средства для:

- идентификации преступника (выявление IP-идентификатора или MAC-адреса пользователя, метаданных файлов и пр.);

- установления факта совершения преступления (например, подтверждение факта несанкционированного доступа к компьютерной информации или распространения вредоносного программного обеспечения путем анализа лог-файлов или сетевого трафика);

- определения нанесенного ущерба (например, анализ финансовых транзакций или простоя технологического оборудования).

По функциональному назначению можно выделить технико-криминалистические средства, применяемые в целях:

- создания образов носителей информации и дампов памяти для их последующего анализа;

- анализа файловых систем (исследование структуры и содержимого системы организации, хранения и именования данных на носителях информации);

- захвата и исследования сетевого трафика для выявления аномалий и вредоносной активности³⁰⁵;

- анализа лог-файлов (поиск, сбор и анализ информации о работе технических средств или программного обеспечения)³⁰⁶;

- восстановления данных;

³⁰⁴ Roberts A. Importance of OSINT. Cyber threat intelligence. Apress : Berkeley, 2021. P. 131.

³⁰⁵ Tiutiunyk I., Toptunenko D., Flaumer A. Classifying cybercrime networks: organized and transnational schemes in the digital // Socio-economic relations in the digital society. 2024. V. 3. P. 122.

³⁰⁶ Gomathy C. K., Rajesh P. V., Manohar D. S. Legal frameworks for regulating cybercrime and cyber terrorism // International journal of scientific research in engineering and management. 2024. V. 8. № 9. P. 3.

– визуализации данных (отображение в наглядной форме взаимосвязей с целью выявления закономерностей) и пр.

Таким образом, рассматриваемые технико-криминалистические средства представляют собой, преимущественно, совокупность программных инструментов поиска и анализа цифровых доказательств. Практическая значимость приведенной классификации определяется возможностью систематизации знаний об имеющихся на сегодняшний день средствах, применяемых при расследовании преступлений в сфере компьютерной информации, что облегчает их поиск и выбор для решения конкретных задач, формулирования принципов применения, определения критериев их подбора под конкретный вид преступного деяния, стимулирования разработки инструментов, направленных на расследование вновь возникающих преступлений, а также стандартизации использования указанных средств в процессе сбора цифровых доказательств и обеспечения их допустимости в суде. Таким образом, преступления в сфере компьютерной информации, в отличие от традиционных форм преступных деяний, совершаются с использованием технических средств и различных информационно-телекоммуникационных технологий, что формирует принципиально новую трудно поддающуюся для криминалистического исследования цифровую среду. Способ совершения преступления в сфере компьютерной информации влияет на тип оставляемых следов, обнаруживаемых с использованием технико-криминалистических средств, которые в дальнейшем определяют методику расследования, алгоритмы действий по поиску, собиранию доказательств и их дальнейшей юридической интерпретации. По этой причине расследование рассматриваемого вида преступлений требует применения методов и средств, сформированных на базе информационных технологий (аналогичных по своей природе инструментам, используемым злоумышленниками).

Расследование преступлений в сфере компьютерной информации базируется на обнаружении, фиксации, изъятии и исследовании цифровых доказательств, осуществляемых с использованием технико-криминалистических средств в виде программного обеспечения, что позволяет сохранить целостность следовой картины, точность и воспроизводимость результатов анализа криминалистически значимой информации. По этой причине целесообразно дальнейшее рассмотрение особенностей расследования преступлений в сфере компьютерной информации с использованием программного обеспечения, что позволит в дальнейшем сформировать концептуальные основы криминалистического исследования цифровой информации, способствующие решению имеющихся в настоящее время проблем в деятельности по поиску цифровых доказательств.

2.2. Роль программных технико-криминалистических средств при расследовании преступлений в сфере компьютерной информации

Важнейшими задачами науки криминалистики из числа специальных являются привлечение данных естественных и технических наук в целях оптимизации научно-технического обеспечения, а также совершенствование криминалистических средств, методов, тактических приемов и методических рекомендаций раскрытия, расследования и предупреждения преступлений.

По этой причине одной из основных задач криминалистики в рамках расследования преступлений в сфере компьютерной информации является ее адаптация к современным условиям в плане использования информационных технологий, разработки новейших криминалистических средств в целях своевременного обнаружения, фиксации и исследования следов (в том числе цифровых), образующихся в результате совершения преступных деяний в киберпространстве.

Как ранее было указано, в качестве основного следообразующего объекта по преступлениям в сфере компьютерной информации выступает системное программное обеспечение (которое может обеспечивать управление такими общими компонентами для всех технических средств как центральное процессорное и оперативно запоминающее устройства, каналы ввода-вывода, а также сетевое и коммуникационное оборудование), а также прикладное программное обеспечение (обеспечивающее выполнение конкретных задач на устройстве). При этом следовоспринимающим объектом принимается носитель информации.

Под цифровым следом понимают любую криминалистически значимую компьютерную информацию (сведения, сообщения, данные о событиях или действиях), представленную в виде электрических сигналов, вне зависимости от средств их хранения, обработки и передачи, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи. Под смежным понятием «электронно-цифровой след» понимают совокупность сведений, выраженную посредством сигналов в форме, пригодной для обработки с использованием технических средств, в результате создания (модификации) определенного кода на электронном носителе информации³⁰⁷. Непосредственно

³⁰⁷ Колычева А. Н. Расследование преступлений с использованием компьютерной информации из сети Интернет : учебное пособие / под ред. А. Г. Волеводза. М. : Проспект, 2020. С. 9.

цифровыми следами могут выступать, например, электронный файл, сетевой адрес, веб-сайт, программное обеспечение, база данных, информационная система, электронное сообщение, электронные денежные средства, цифровая валюта, электронная цифровая подпись и пр.³⁰⁸. Определенный интерес представляет позиция, обозначенная в методических рекомендациях по защите персональных данных, сформированных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), в которых понятие «цифровой след» выделяется как результат цифровой активности субъекта за счет своей деятельности и с помощью своих устройств, а термин «цифровая тень» определяется как результат цифровой активности третьих лиц³⁰⁹, при этом совокупность цифровых следов и цифровых теней именуется «цифровым штампом». В соответствии со ст. 74 УПК РФ доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном УПК РФ, устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела. Исходя из вышеизложенного и содержания ст. 74 УК РФ под цифровым доказательством можно понимать любую компьютерную информацию, на основе которой суд, прокурор, следователь, дознаватель устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела. Здесь и далее в работе под доказательством, представленным в цифровой форме, будут подразумеваться информация или данные, хранящиеся или передаваемые в виде двоичного кода, что определено в ГОСТ Р ИСО/МЭК 27037–2014³¹⁰, вопреки часто употребляемому отчасти синонимичному термину «электронное доказательство». К категории цифровых доказательств в соответствии с положениями УПК РФ могут быть также отнесены «иные документы» в виде скриншотов переписки на бумажных носителях, ответов на

³⁰⁸ Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). С. 269.

³⁰⁹ Методические рекомендации по организационной защите физическим лицом своих персональных данных // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Роскомнадзор : офиц. сайт. URL: https://rkn.gov.ru/docs/mr_itog.docx (дата обращения: 02.02.2025).

³¹⁰ ГОСТ Р ИСО/МЭК 27037–2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме; дата введения: 09 сентября 2014 г. М. : Стандартинформ, 2015. С. 7.

запрос поставщиков услуг в отношении конкретного пользователя и т. п. При этом в соответствии со ст. 84 УПК РФ документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде (например, материалы фото-, аудио- и видеозаписей и иные носители информации). Соответственно, когда указанные документы обладают признаками, указанными в ч. 1 ст. 81 УПК РФ, они могут признаваться вещественными доказательствами в силу ч. 4 ст. 84 УПК РФ. Вещественными доказательствами также могут быть признаны: фонограммы записи переговоров (в соответствии с ч. 8 ст. 186 УПК РФ, на основании постановления следователя); приложение к заключению эксперта либо к заключению специалиста; ходатайство, заявление или жалоба, поданные в форме электронного документа (в соответствии со ст. 474.1 УПК РФ); приложение к протоколу следственного и судебного действий (в том числе результаты применения криминалистических средств фиксации хода и результатов следственного действия; изъятые и полученные в ходе проведения проверки сообщения о преступлении предметы и документы в порядке, установленном ст. 146 УПК РФ; результаты оперативно-розыскных мероприятий (в ряде случаев); результаты использования аудиовизуального, электронного и иного средства контроля (в соответствии со ст. 105.1, ч. 14 ст. 107 УПК РФ).

В соответствии со ст. 164.1 УПК РФ копирование информации, содержащейся на электронном носителе информации, в ходе производства следственных действий вправе осуществлять следователь, при этом необходимо использование криминалистических средств с обязательной фиксацией порядка их использования, а также полученных результатов в протоколе следственного действия. При этом изъятие электронного носителя информации осуществляется с участием специалиста. По ходатайству владельца изымаемого носителя специалистом, участвующим в следственном действии, в присутствии понятых с изымаемого носителя осуществляется копирование данных на иной электронный носитель информации («клон»), который предоставляется законным владельцем, после чего «клонированный» носитель, содержащий скопированную информацию, передается владельцу, а в протоколе указывается соответствующая запись. Собираанию цифровых доказательств присущи как общие, так и специальные черты. Например, составление протокола следственного действия, связанного с рассматриваемым видом доказательства, должно производиться уполномоченным субъектом, указанным в УПК РФ, однако при этом необходимо участие специалиста, при этом экспертизу должен осуществлять специалист в соответствующей области, однако, осмотр веб-сайта, создание и сохранение

скриншотов должны производиться следователем или дознавателем с участием соответствующего специалиста и понятых³¹¹.

В качестве орудий и средств совершения преступлений в сфере компьютерной информации выступают различные технические средства в совокупности со специализированным программным обеспечением, использование которых может быть выявлено по специфическим для каждого применяемого инструмента цифровым следам. Индивидуальность и электронная форма указанных следов определяют возможность их исследования исключительно с применением программно-аппаратных средств, что обусловлено неприменимостью традиционных методов собирания доказательств к среде цифровых данных.

Изучению закономерностей возникновения и сокрытия цифровых следов и разработкой на знании этих закономерностей технических средств, приемов и методов по обнаружению, фиксации, изъятию и исследованию данных следов в целях раскрытия, расследования и предупреждения преступлений посвящено криминалистическое учение о цифровой (компьютерной) информации, систему которого составляют криминалистическое исследование цифровых следов, документированной цифровой информации и вредоносных компьютерных программ³¹². Так, например, программные средства для анализа цифровой информации, сетевого трафика, компьютеров и информационных систем, восстановления удаленных файлов, извлечения зашифрованных данных на сегодняшний день являются основой криминалистической деятельности в киберпространстве³¹³.

Без специализированных цифровых инструментов невозможно корректно идентифицировать источник атаки, отследить действия преступника и обеспечить доказательственную базу, соответствующую правовым требованиям. Соответственно, к основным инструментам, способствующим расследованию преступлений в сфере компьютерной информации, относят технико-криминалистические средства, направленные на выявление, извлечение, анализ и сохранение цифровых доказательств.

³¹¹ Процессуальная деятельность защитника по собиранию и представлению доказательств в российском уголовном судопроизводстве : монография / под ред. Н. Р. Мухудиновой. Саранск : Издательство Мордовского университета, 2008. С. 27.

³¹² Цифровая криминалистика. Указ. соч. С. 18.

³¹³ Nelufule N. Intersection of electronic security and digital forensics: data protecting techniques and uncovering data clues // Towards new e-infrastructure and e-services for developing countries. Cham : Springer, 2025. V. 1. P. 351.

Система криминалистического исследования электронных носителей информации включает в себя методологические основы анализа криминалистической техники, в частности учение о цифровых следах, о методах, об электронных документах и т. п., а также исследования отдельных видов технических средств³¹⁴. Развитие данной области знаний происходит в направлении расширения объектов исследований, а также различных средств. Техничко-криминалистические средства могут являться программными и аппаратными средствами анализа цифровых доказательств³¹⁵, устройствами аппаратного восстановления данных, комплексами перехвата сетевого трафика³¹⁶ и т. п. Криминалистическое обеспечение раскрытия и расследования преступлений рассматриваемого вида стратегически целесообразно планировать с возможностью автоматизации рутинных задач, что возможно с задействованием технологий искусственного интеллекта³¹⁷, анализа больших данных³¹⁸, хранения доказательств в распределенных системах³¹⁹, моделирования преступных деяний и пр. Таким образом, внедрение информационных технологий в технико-криминалистическое обеспечение расследования преступлений в сфере компьютерной информации дает возможность формирования значительного массива криминалистически значимой информации, новых криминалистических учетов, их обработки и использования в профессиональной деятельности следователей, дознавателей, оперативных сотрудников и экспертов.

С точки зрения уголовно-процессуального законодательства обнаружение, фиксация и изъятие цифровых следов производятся в ходе таких следственных действий как следственный осмотр, обыск и выемка, при которых непосредственно компьютерную информацию невозможно изъять, но можно осуществить ее копирование. Чтобы эффективно провести собирание, фиксацию, оценку или копирование цифровых доказательств необходимо не только наличие специальных

³¹⁴ Криминалистическая техника : учебник / под ред. К. Е. Демина. М. : Юридический институт Российского университета транспорта, 2017. С. 341.

³¹⁵ Shamoo Y. Cybercrime investigation and fraud detection with AI // IGI Global. 2025. P. 85.

³¹⁶ Baroniya Y., Bharadwaj V. Cyber and digital forensic. Textbook of forensic science. Singapore : Springer, 2023. P. 774.

³¹⁷ Россинская Е. Р. Система теории цифровизации судебно-экспертной деятельности // Теория и практика судебной экспертизы. 2024. Т. 19. № 3. С. 23.

³¹⁸ Pinney J., Bentotahewa V., Tomlinson, M. Exploring applications and implications of big data predictive analytics in policing cyberspace // Navigating the intersection of artificial intelligence, security, and ethical governance. Cham : Springer, 2025. P. 2.

³¹⁹ Adams T. A. Trends, Challenges and opportunities of engaging digital forensics for cybercrime investigations // Advances in multidisciplinary and scientific research journal publication. 2024. V. 15. № 1. P. 10.

знаний, но и применение специальных технических средств. В целях снижения временных и трудовых затрат при расследовании преступлений в сфере компьютерной информации, неоправданного назначения компьютерно-технических экспертиз, важно понимать, где и какие цифровые доказательства целесообразно искать, как их фиксировать и, соответственно, с помощью каких технических средств осуществлять их копирование и последующую оценку.

С целью подтверждения вышеуказанного можно рассмотреть отдельные возможности расследования преступлений в сфере компьютерной информации с применением программных (рассматриваемых в качестве технико-криминалистических) средств в виде отечественных и зарубежных решений.

Так, с учетом обозначенных в параграфе 1.2.1 слеодообразующих и следовоспринимающих объектов в отношении неправомерного доступа к компьютерной информации (ст. 272 УК РФ) программные средства позволяют автоматизировать собирание доказательств, проводить анализ носителей данных («Мобильный криминалист (десктоп, эксперт, эксперт плюс)³²⁰», «Elcomsoft Premium Forensic Bundle»³²¹, «Sleuth Kit», «Autopsy», «Caine», «HDDScan» и пр.), исследовать метаданные («jExifToolGUI», «Metadata», «ExifTool» и др.), идентифицировать факт несанкционированного доступа («SQL Forensics», «DB Shield» и пр.), восстановить удаленную информацию (например, «EnCase», «FTK Forensic Toolkit», «PC-3000»³²²), зафиксировать сетевой трафик («TcpDump», «Wireshark», «Zeek»), а также сформировать журнал событий и активности злоумышленника («IBM QRadar», «Splunk» и др.).

Использование указанного программного обеспечения позволяет автоматизировать и ускорить поиск и исследование цифровых доказательств, сводя к минимуму человеческий фактор. Тем не менее, интерпретация полученных данных зачастую требует экспертных знаний, что в целом очень сильно зависит от полноты исходных данных по делу.

³²⁰ Программное обеспечение «Мобильный Криминалист Эксперт Плюс» // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации : офиц. сайт. URL: https://reestr.digital.gov.ru/reestr/423110/?sphrase_id=5937674 (дата обращения: 07.04.2025).

³²¹ Программное обеспечение «Elcomsoft Premium Forensic Bundle» // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации : офиц. сайт. URL: https://reestr.digital.gov.ru/reestr/436808/?sphrase_id=5929589 (дата обращения: 07.04.2025).

³²² Программное обеспечение «PC-3000 Portable» // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации : офиц. сайт. URL: https://reestr.digital.gov.ru/reestr/310277/?sphrase_id=5929598 (дата обращения: 07.04.2025).

В рамках расследования незаконного использования, передачи, сбора и хранения компьютерной информации, содержащей персональные данные граждан (272.1 УК РФ), с учетом обозначенных в параграфе 1.2.2 следообразующих и следовоспринимающих объектов, программные средства могут обеспечивать фиксацию утечек конфиденциальных сведений («Maltego», «SpiderFoot», «Symantec Data Loss Prevention», «Have I Been Pwned» и др.), в том числе запрещенных к распространению данных (поисковая система «Seus»)³²³, выявление маршрутов передачи данных («Wireshark» и др.), мониторинг трафика, в том числе выявление продаж баз данных с персональными данными в сети даркнет («Darknet Tracer», «CipherTrace» и пр.), предотвращения утечек информации (DLP-системы (от англ. «data leakage prevention – предотвращение утечки данных) «Symantec», «InfoWatch» и пр.). Преимуществами использования указанного программного обеспечения являются возможность анализа значительных объемов данных, мониторинга подозрительной активности в реальном времени, высокая эффективность выявления мест хранения скомпрометированных данных, автоматизация поиска утечек конфиденциальных сведений на теневых рынках. При этом недостатками являются высокая вычислительная нагрузка, вероятность ошибок при автоматизированном анализе, а также риск нарушения конфиденциальности при обработке персональных данных.

В отношении создания, использования и распространения вредоносного программного обеспечения (ст. 273 УК РФ) и обозначенных в параграфе 1.2.3 следообразующих и следовоспринимающих объектов, программные технико-криминалистические средства позволяют исследовать вредоносный код, например, идентифицируя способы его распространения и алгоритмы исполнения («IDA Pro», «OllyDbg», «Ghidra», «VirusTotal» и пр.), динамический анализ и эмуляцию поведения вирусов («Cuckoo Sandbox», «Any.Run» и пр.), фильтрацию подозрительного трафика («Snort», «Suricata» и пр.), фиксацию вредоносной активности («Kaspersky», «Symantec», «McAfee» и пр.). Преимуществами использования вышеуказанных программных средств являются высокая точность в определении функционала вредоносных программ, обновляемые базы данных сигнатур, автоматизированное обнаружение новых угроз и возможность отслеживания цепочек их распространения. При этом необходимо постоянное

³²³ Программное обеспечение «Поисковая система SEUS» // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации : офиц. сайт. URL: https://reestr.digital.gov.ru/reestr/305124/?sphrase_id=5929711 (дата обращения: 07.04.2025).

обновление аналитических средств и значительные вычислительные ресурсы при исследовании файлов и информационных систем.

В целях обнаружения нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) используются программные средства, фиксирующие действия пользователей и системных администраторов («QRadar», «ArcSight» и пр.), централизованный мониторинг нарушений требований информационной безопасности и фактов несанкционированного доступа или неправильной эксплуатации программного обеспечения («Solar Dozor», «Snort», «Suricata» и пр.), выявление уязвимостей в сетевых устройствах («Nessus», «OpenVAS»), анализ журналов событий и изменения программного обеспечения («AlienVault», «ArcSight», «Graylog», «LogRhythm» и пр.). Несмотря на все преимущества использования указанных программ и возможность предотвращения инцидентов информационной безопасности, общим их недостатком являются трудоемкость сбора и интерпретации данных.

В целях выяснения обстоятельств, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также исследования обозначенных в параграфе 1.2.4 следообразующих и следовоспринимающих объектов, программные средства также позволяют осуществлять мониторинг и анализ сетевого трафика, отслеживание производительности сети (программное обеспечение «Wireshark», «Network Miner», «SolarWinds Network Performance Monitor»), обнаруживать вредоносную активность (программы «IDA Pro», «OllyDbg», «Ghidra», «VirusTotal» и пр.), восстанавливать удаленные или поврежденные данные с электронных носителей информации с последующим их анализом («Elcomsoft Premium Forensic Bundle», «Sleuth Kit», «Autopsy», «Caine», «HDDScan», «PC-3000» и пр.), исследовать метаданные (программное обеспечение «jExifToolGUI», «Metadata», «ExifTool» и др.), проводить аудит управления учетными записями (средства автоматизации управления доступом «IDM» (от англ. «identity management» – управление идентификацией), «IAM» (от англ. (identity and access management» – управление идентификацией и доступом) и «IGA» (от англ. «identity governance & administration» – управление идентификацией и ее администрированием)), а также формировать журнал событий и активности злоумышленника (программы «IBM QRadar», «Splunk» и др.). Кроме указанных непосредственно субъектами критической информационной инфраструктуры РФ может применяться иное

вспомогательное программное обеспечение, позволяющее идентифицировать нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также расследовать инциденты информационной безопасности.

В отношении неправомерного воздействия на объекты критической информационной инфраструктуры РФ (ст. 274.1 УК РФ), с учетом обозначенных в параграфе 1.2.5 следообразующих и следовоспринимающих объектов, программные средства, например, могут обеспечить обнаружение атак на промышленные системы («Wireshark», «Tofino Xenon», «Radiflow», «Nozomi Networks» и пр), мониторинг сетевого трафика и выявление аномалий в режиме реального времени («Splunk», «ELK Stack», «NetFlow» и пр), анализ трафика и журналов событий («IBM X-Force», «FireEye») и пр.

В целях выявления нарушений правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ) программные средства могут позволить, например, выявлять нарушения при управлении интернет-трафиком («Суверенный Рунет», «NetWitness», «Deep Packet Inspection», «BGPmon», «RIPEstat» и пр), проводить аудит управления учетными записями (средства автоматизации управления доступом «IDM», «IAM» и «IGA»), проводить расследования инцидентов и отслеживать запрещенные ресурсы, контролировать доступ к ресурсам («Ревизор», «FireEye SORM», «Farsight Security», «Cisco Umbrella», «Palo Alto») и пр. В отношении неправомерного использования GSM-шлюзов, SIM-боксов и виртуальных телефонных станций (ст. 274.3 УК РФ) также возможно использование специализированного программного обеспечения (например, «Openmind's sim box detection solution», «ActivML» и др.). В целях выявления деятельности по незаконному обороту SIM-карт (ст. 274.4 УК РФ), аккаунтов и учетных данных (ст. 274.5 УК РФ) возможна лишь интеграция превентивных решений, например, на основе искусственного интеллекта, с целью выявления фиктивных биометрических данных при продаже SIM-карт, либо фиксации подозрительной активности конкретного аккаунта и т. п.

Кроме указанных инструментов операторами связи, собственниками или владельцами сетей связи, точек обмена трафиком, линий связи, организаторами распространения информации в сети «Интернет», а также провайдерами хостинга может применяться иное вспомогательное программное обеспечение,

позволяющее идентифицировать нарушения правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования, а также расследовать инциденты информационной безопасности. Кроме того, осуществить мониторинг сети связи общего пользования могут позволить, например, система контроля состояния идентификационных модулей информационных систем «ПАК КСИМ», обеспечивающая мониторинг соблюдения операторами связи требований по идентификации абонентов, национальная система доменных имен, обеспечивающая доступность отечественных интернет-ресурсов в случае искажения или недоступности информации в глобальной системе доменных имен и безопасного их преобразования в IP-адреса, автономная система IP-сетей и маршрутизаторов, управляемых операторами, система «Антифрод»³²⁴, позволяющая выявлять подменные номера и др.

Применение специализированных программных технико-криминалистических средств является основой современной методики расследования преступлений в сфере компьютерной информации, которая обеспечивает оперативное выявление и анализ инцидентов в режиме реального времени, восстановление и реконструкцию цифровых следов с высокой точностью, интеграцию данных с различных источников и уровней инфраструктуры.

Приведенный перечень программных средств не является исчерпывающим, однако позволяет показать широту их потенциала в расследовании преступлений в сфере компьютерной информации, а также говорит о возможности использования указанных средств в криминалистических целях. Так, например, на сегодняшний день в работе органов внутренних дел широко применяются сервисы обеспечения повседневной и оперативно-служебной деятельности системы ИСОД МВД России, а также различные информационные системы поискового и экспертного назначения. Однако стоит отметить сложившийся недостаток оснащения средствами³²⁵, позволяющими восполнить конкурентное преимущество в борьбе с

³²⁴ Ежемесячный отчет Центра мониторинга и управления сетью связи общего пользования // Федеральное государственное унитарное предприятие «Главный радиочастотный центр» : офиц. сайт. URL: https://portal.noc.gov.ru/documents/235/Публичный_отчет_декабрь_2024_итог_.pdf (дата обращения: 22.03.2025).

³²⁵ Горбунова Е. Ю. Проблемы качества судебно-экспертных исследований (судебная компьютерно-техническая экспертиза) // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции. Москва : Российский государственный университет правосудия, 2021. С. 206.

преступлениями, что снижает эффективность деятельности правоохранительных органов по раскрытию, расследованию и предотвращению преступных деяний. Оптимизации сроков осуществления следственных действий и иных процессуальных действий, направленных на установление обстоятельств, входящих в предмет доказывания, будет способствовать закрепление в законодательстве более четких оснований и регламентов, регулирующих собирание цифровых доказательств с применением информационных технологий и программных технико-криминалистических средств.

Таким образом, можно сделать вывод, что в условиях цифровизации общества программные технико-криминалистические средства приобретают стратегическое значение в борьбе с преступлениями, обеспечивая, во-первых, непосредственное обнаружение, фиксацию, изъятие и исследование цифровых доказательств (за счет использования экспертных и поисковых систем), во-вторых, их верификацию и проверку подлинности и сохранности (например, за счет использования алгоритмов хеширования для создания контрольных сумм цифровых объектов и последующей проверки их неизменности), в-третьих – восстановление удаленных и зашифрованных данных (например, за счет применения методов цифровой стеганографии или интеграции блокчейн-технологий), а также удобство и оперативность обработки больших массивов данных (за счет использования технологий машинного обучения и хранения данных в распределенных реестрах), выдачи прогнозов и рекомендаций (на базе предиктивного и корреляционного анализа).

В настоящее время в свободном доступе имеется разнообразное программное обеспечение в области поиска, анализа и интерпретации цифровых доказательств, однако его применение сотрудниками правоохранительных органов ограничено в силу отсутствия четкого нормативного регулирования. Так, на примере OSINT-инструментов для поиска информации из открытых источников можно констатировать, что в силу действующего законодательства применение подобного метода сбора данных возможно лишь при наличии судебного решения, однако даже в этом случае возникают риски нарушения конституционных прав граждан, включая неприкосновенность частной жизни, личную и семейную тайну, а также тайну переписки. Соответственно, для эффективного выявления и пресечения преступной деятельности в сфере компьютерной информации необходима правовая регламентация применения программных технико-криминалистических средств, обеспечивающая баланс между возможностями правоохранительных органов и соблюдением конституционных прав граждан.

Поскольку предполагаемым вектором развития киберпреступности является использование различных генеративных алгоритмов машинного обучения, соответственно, для противодействия таким угрозам необходимы программные средства, способные самостоятельно, на основе гибких алгоритмов искусственного интеллекта, без участия человека, например, идентифицировать аномалии в сетевом трафике, анализировать вредоносный код и, соответственно, адаптироваться к новым видам атак. Определенную трудность будет также представлять появление квантовых компьютеров, способных взламывать современные криптографические алгоритмы. Для противодействия этой угрозе программные комплексы должны будут включать гибридные квантовые алгоритмы взлома шифрования, сочетающие традиционные методы криптоанализа с вероятностными вычислениями квантовых систем. Таким образом, только программные технико-криминалистические средства смогут эффективно бороться с атаками, управляемыми искусственным интеллектом в будущем, что подчеркивает насущность их рассмотрения в настоящее время.

Значимость применения программных технико-криминалистических средств при расследовании преступлений в сфере компьютерной информации определяется следующими факторами:

- современное криминалистическое программное обеспечение позволяет оперативно собрать, зафиксировать, классифицировать и проанализировать цифровые доказательства, снижая вероятность пропуска криминалистически значимой информации среди объемных массивов электронных данных;
- исключительно программные технико-криминалистические средства позволяют анализировать информационные системы и цифровые данные, сетевой трафик, облачные хранилища, дампы оперативной памяти и текущие информационные процессы в цифровых устройствах, в том числе в режиме реального времени, восстанавливать удаленные файлы, выявлять скрытые данные, дешифровывать закодированную информацию, моделировать сценарии преступлений и пр.;
- обеспечить легитимность собранных электронных данных, целостность файловых структур позволяют только сертифицированные программные технико-криминалистические средства;
- только специализированное криминалистическое программное обеспечение позволяет выявлять корреляции между преступными деяниями и типичными методами сокрытия информации;
- использование программных технико-криминалистических средств

ускоряет расследование и позволяет эффективно распределять трудовые ресурсы;

- проводимый с использованием криминалистического программного обеспечения анализ цифровой информации позволяет обеспечить воспроизводимость исследований, гарантируя возможность верификации полученных данных другими специалистами.

Недостатками и сложностями использования программных технико-криминалистических средств при расследовании преступлений в сфере компьютерной информации являются:

- отсутствие механизма допуска следователя к непосредственному анализу собранных цифровых доказательств;

- недостаточная квалификация следователей и экспертов в области исследования цифровых устройств и цифровой информации, которая может привести к изменению или утрате доказательной информации;

- отставание функциональных возможностей программного обеспечения и технических средств, используемых правоохранительными органами в расследовании преступлений, в сравнении с возможностями программных средств и устройств, используемыми преступниками;

- использование несертифицированных средств, не значащихся в реестре отечественного программного обеспечения, может привести к недопустимости рассмотрения собранных доказательств в суде.

В целях устранения указанных недостатков предполагается целесообразным:

- расширение перечня полномочий следователя, например, при производстве осмотра места происшествия по преступлениям, совершаемым в сфере компьютерной информации, или предметов, в частности, носителей информации, их исследования с помощью программных технико-криминалистических средств и пр.;

- оказание информационной поддержки действующим сотрудникам правоохранительных органов в целях эффективного использования криминалистического программного обеспечения в рамках проводимых следственных действий (например, по линии Департамента информационной безопасности Банка России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России и пр.);

- разработка современных программных технико-криминалистических средств и централизованных цифровых криминалистических платформ с

интуитивно понятным интерфейсом, адаптированным для использования неспециалистами по заранее определенным алгоритмам и методикам проведения исследования;

- формирование единой базы данных цифровых следов (нового криминалистического учета), что позволит следователям обмениваться информацией о новых методах атак и инструментах защиты информации;

- своевременное обновление и развитие программных технико-криминалистических средств и внедрение в следственную практику с учетом эволюции преступлений в сфере компьютерной информации.

С учетом вышеизложенного можно сделать вывод, что особенности киберсреды исключают традиционные технико-криминалистические средства, поскольку цифровые следы не имеют физических характеристик в классическом понимании, являются легко изменяемыми и уничтожаемыми, кроме того, большие массивы цифровой информации зачастую размещены в различных средах и (или) хранилищах, что исключает их ручной анализ.

В отличие от традиционных вещественных доказательств цифровые доказательства требуют специфических подходов к собиранию, хранению и анализу, так как они легко поддаются модификации. Автоматизацию исследования цифровой информации, точность и воспроизводимость результатов ее анализа, обеспечение своевременного собирания и использования криминалистически значимой информации в электронной форме позволяют обеспечить только программные технико-криминалистические средства. Таким образом, программные технико-криминалистические средства играют ключевую роль в расследовании преступлений в сфере компьютерной информации, что обусловлено предоставляемыми ими возможностями обнаружения, фиксации, изъятия, исследования и хранения криминалистически значимой компьютерной информации. В связи с этим в дальнейшем необходимо рассмотреть основные проблемы и пути совершенствования указанной деятельности с использованием программных технико-криминалистических средств.

2.3. Проблемы и пути совершенствования деятельности по собиранию, исследованию, оценке и использованию цифровых доказательств при расследовании преступлений в сфере компьютерной информации

Развитие индустрии информационных технологий, экспоненциальный рост цифровизации большинства социально-экономических процессов, повсеместное использование технических устройств, информационно-телекоммуникационной сети «Интернет», а также мобильных средств связи, развитие дистанционного банковского обслуживания, увеличение безналичного денежного оборота и иные факторы, определяющие информатизацию общества, привели к тому, что за прошедшие несколько лет существенно изменились способы, средства и условия совершения преступлений. Указанная тенденция способствовала беспрецедентному росту преступлений в сфере компьютерной информации, противодействие которым до настоящего времени осложняется несовершенством процесса собирания (обнаружения, фиксации, изъятия, сохранения)³²⁶, исследования, оценки и использования³²⁷ криминалистически значимой компьютерной информации, а также отсутствием необходимых технико-криминалистических средств.

Одну из наиболее важных на сегодняшний день задач в области криминалистики можно определить как синергичную ее адаптацию к современным условиям в плане применения информационных технологий и разработки новейших технических средств в целях своевременного выявления следов, образующихся в результате совершения преступных деяний (в том числе электронных). По этой причине важно рассмотрение типичных проблем и путей совершенствования деятельности по собиранию, исследованию, оценке и использованию цифровых доказательств при расследовании преступлений в сфере компьютерной информации, что может выступить необходимой основой в борьбе с киберпреступностью, обеспечения своевременного обнаружения криминалистически значимой компьютерной информации и последовательного изложения концепции настоящего исследования³²⁸.

³²⁶ Белкин Р. С. Собираение, исследование и оценка доказательств. Сущность и методы. М. : Наука, 1966. С. 29.

³²⁷ Белкин А. Р. Теория доказывания в уголовном судопроизводстве. М. : Норма, 2007. С. 11.

³²⁸ Харисова З. И. Проблемы и пути совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2025. № 2 (108). С. 117.

Многофункциональность и постоянное совершенствование технических средств, программного обеспечения и информационных технологий в целом расширяет как пользовательские, так и криминалистические возможности, в этой связи в криминалистической теории наблюдается тенденция изучения так называемых цифровых следов преступной деятельности³²⁹. При расследовании преступлений в сфере компьютерной информации зачастую требуются специальные знания, которые охватывают сравнительно больший объем в соотношении с базовыми и общеизвестными или общедоступными профессиональными знаниями. Современная криминалистика основывается на комплексном использовании специальных знаний, позволяющих эффективно расследовать преступления, устанавливая обстоятельства дела и формируя при этом доказательственную базу. Однако их применение зависит от процессуального режима, в котором они реализуются.

Специальные знания могут быть задействованы в двух ключевых формах – процессуальной (в рамках уголовно-процессуальной деятельности, следователем и судом) и непроцессуальной (при проведении оперативно-розыскных мероприятий, а также при предварительных исследованиях, осуществляемых в информационно-тактических целях). Данное разграничение имеет принципиальное значение, поскольку определяет юридическую силу полученных результатов и возможности их последующего использования в доказывании. Несмотря на то, что полученные в непроцессуальной форме данные не имеют статуса доказательств, они выполняют важную криминалистическую функцию, способствуя выдвижению версий, розыску преступников и оптимизации процесса расследования. Понятие «исследование» в криминалистике довольно часто употребляется в значении криминалистического исследования объектов с целью выявления признаков преступной деятельности или причастности к ней конкретного лица, планирования расследования и пр.

Предварительное исследование может быть проведено, например, в ходе осмотра места происшествия, однако, при этом не должны меняться свойства, имеющие доказательственное значение. Стоит также отметить, что предварительное исследование недопустимо в отношении большинства объектов, которые в последующем изымаются в ходе осмотра или в отношении которых впоследствии может быть назначена судебная экспертиза.

³²⁹ Цифровые следы преступлений : монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. М. : Проспект, 2023. С. 3.

Применительно к преступлениям в сфере компьютерной информации, например, недопустимо предварительное исследование электронных носителей ввиду возможной утраты содержащейся на них информации³³⁰. На стадии возбуждения уголовного дела специальные знания используются при осуществлении проверок сообщений о преступлениях, исследованиях предметов и документов, производстве осмотра места происшествия, а также в ходе производства судебной экспертизы. В ходе расследования, в соответствии со ст. 168 УПК РФ, к участию в производстве следственных действий могут привлекаться специалисты.

Практика анализа преступлений, способов и средств их совершения позволяет сделать заключение о наиболее вероятном расположении следов, оставляемых при том или ином способе совершения преступления³³¹. Криминалистическое изучение особенностей преступлений и главным образом способов их совершения дает исходные положения для разработки технико-криминалистических средств, при помощи которых следы преступления окажутся зафиксированными наиболее полно и будут пригодными для дальнейшего исследования. Доказывание в понимании познавательной деятельности – это оперирование доказательствами³³², поэтому процесс доказывания складывается из четырех элементов – собирания (обнаружения, фиксации и изъятия), исследования, оценки и использования доказательств³³³, грамотность проведения и правильность процессуального оформления которых способствуют оперативному изобличению участников преступного события и обеспечению надежной доказательственной базы³³⁴.

Обнаружение (поиск) цифровых доказательств является важным элементом расследования рассматриваемых преступлений, что подтверждается рядом международных правовых документов и многочисленными исследованиями. Так, ст. 23 Конвенции против киберпреступности определяет необходимость принятия на государственном уровне законодательных и иных мер в целях установления

³³⁰ Курс криминалистики. Указ. соч. Т. 1. С. 647.

³³¹ Выявление причин преступности и предупреждение преступлений. Общие положения / под. ред. П. Ф. Гришанина. Указ. соч. С. 117.

³³² Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. М. : Юридическая литература, 1987. С. 76.

³³³ Егоров Н. Н. Собирание вещественных доказательств: понятие, содержание, направления совершенствования : монография. Хабаровск : Дальневосточный государственный университет путей сообщения, 2005. С. 4.

³³⁴ Скобелин С. Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 44.

полномочий и процедур в отношении уголовных правонарушений, совершенных с помощью информационно-телекоммуникационных технологий, акцентируя особое внимание на собирании доказательств в электронной форме. В соответствии со ст. 14 Будапештской конвенцией Совета Европы ETS 185 государства должны обеспечить наличие мер процессуального характера, позволяющих собирать, анализировать и использовать цифровые доказательства. Кроме того, во всестороннем исследовании проблем киберпреступности Управления Организации Объединенных Наций (по наркотикам и преступности) цифровые доказательства также определяются неотъемлемой частью процесса доказывания. Методы сбора цифровых доказательств отмечаются в специализированных руководствах Международной организации уголовной полиции (Интерпол)³³⁵. Таким образом, без выявления цифровых доказательств невозможно процессуально зафиксировать и доказать совершение преступления в сфере компьютерной информации.

Несмотря на наличие правового регулирования, действующая правоприменительная практика в настоящее время довольно часто сталкивается с проблемами обнаружения, фиксации, изъятия и исследования цифровых доказательств, их процессуального оформления, достоверности (неизменяемости) и допустимости их в суде, а также рядом технических трудностей, связанных с последующим хранением данных.

Эффективность собирания криминалистически значимых объектов часто зависит от уровня использования следователем технических средств, специализированного программного обеспечения и информационных технологий, а также специальных знаний. Нередки случаи, когда произвести поиск, фиксацию и изъятие доказательств без использования специальных знаний либо в отсутствие специалиста не представляется возможным, что обусловлено, например, применением современных решений при совершении преступлений³³⁶. Так, в отсутствие специальных знаний в области собирания и анализа цифровых доказательств или программных технико-криминалистических средств, действия следователя могут привести к утрате или упущению цифровых следов преступного

³³⁵ Guidelines for digital forensics first responders. Best practices for search and seizure of electronic and digital evidence // Международная организация уголовной полиции (Интерпол) : офиц. сайт. URL: <https://www.interpol.int/content/download/16243/file/Guideline> (дата обращения: 07.04.2025).

³³⁶ Thakur K. S., Ahuja R. Safeguarding justice employing blockchain-enabled secure chain of custody framework for digital evidence // Innovations in electrical and electronic engineering. 2024. № 115. P. 3.

деяния³³⁷.

Таким образом, эффективность расследования преступлений в сфере компьютерной информации в большинстве случаев зависит от качества обнаружения, фиксации, изъятия и исследования цифровых доказательств путем использования технико-криминалистических средств. Так, например, идентифицировать преступника (или используемое им техническое средство), определить его причастность к инциденту поможет выявление: IP-адресов и MAC-идентификаторов задействованных устройств; данных лог-файлов, маршрутизаторов и журналов системного программного обеспечения³³⁸; метаданных файлов и записей реестров сетевой активности; фактов использования виртуальных частных сетей и систем прокси-серверов и пр.

Восстановить и реконструировать хронологию событий и, как следствие, эффективно спланировать дальнейшие следственные действия позволяет анализ временных меток в информационных системах³³⁹, объективность расследования могут обеспечить данные о местоположении мобильного средства связи и анализ коммуникаций участников уголовного процесса, что, в свою очередь, может подтвердить или опровергнуть показания подозреваемых, свидетелей и пр.

К основным проблемам, связанным с обнаружением (поиском), фиксацией и исследованием цифровых доказательств, можно отнести фрагментарность и изменчивость цифровой информации (когда создается риск утраты или искажения криминалистически значимой информации, что особенно актуально при работе с оперативной памятью технических средств и облачными сервисами³⁴⁰), возможность шифрования и анонимизации данных (значительно затрудняет идентификацию и поиск цифровых доказательств и требует специальных средств противодействия для их обхода), разнообразие среды исследования и невозможность стандартизации процесса выявления доказательств (компьютеры с различными видами операционных систем и носителей информации, мобильные средства связи, облачные хранилища данных, сетевая инфраструктура и прочие

³³⁷ Агibalов В. Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. М. : Юрлитинформ, 2012. С. 35.; Саркисян А. А. Цифровизация судебно-экспертной деятельности. М. : Юрайт, 2025. С. 83.

³³⁸ Федотов Н. Н. Форензика – компьютерная криминалистика. М. : Юридический мир, 2007. 432 с. С. 142.

³³⁹ Cantelli-Forti A., Longo G., Lupia F. A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence. International journal of information security. 2025. № 24 (81). P. 7.

³⁴⁰ Yi X., Zhou Y., Lin Y. Digital rights management scheme based on redactable blockchain and perceptual hash // Peer-to-peer networking and applications. 2023. № 16. P. 2640.

устройства, к которым предъявляются конкретные требования к методам поиска данных).

Решение указанных проблем при расследовании преступлений в сфере компьютерной информации преимущественно заключается в автоматизации указанных процессов путем использования программных технико-криминалистических средств, поскольку автоматическую классификацию и детектирование киберугроз, в том числе среди больших массивов сведений, в совокупности с геометрически растущим объемом цифровых данных, возможно охватить исключительно используя программное обеспечение, в частности, построенного на базе технологий искусственного интеллекта и машинного обучения³⁴¹.

Обнаружение цифровых следов преступлений является поисковой деятельностью следователя, которая направлена на собирание доказательственной и ориентирующей криминалистически значимой информации, что возможно с использованием технических средств (компьютера, ноутбука, электронного планшета и пр.)³⁴² и программных технико-криминалистических средств в виде специализированного программного обеспечения. Под фиксацией цифровых доказательств предполагается сохранение фактических данных, находящихся в электронной форме, которое осуществляется в следующем порядке³⁴³:

- производится трансформация доказательственных электронных данных, содержащихся на носителях информации, в форму, доступную для восприятия ее человеком;

- устанавливаются сведения об электронном носителе информации, на котором найдена криминалистически значимая компьютерная информация, его владелец, возможность передачи данных, хранящихся на носителе, операционная система устройства с установленным накопителем, файлы и каталоги данных, в которых найдены доказательства, а также сведения об их создании или изменении;

- обеспечивается фильтрация значимых данных о событии преступления из массива всех имеющихся сведений на носителе информации, выявление способов их получения, а также сохранение доказательственной информации для

³⁴¹ Kreso I. Using blockchain technology for preserving digital evidence in digital forensics // Knowledge international journal. 2025. № 68 (3). P. 331.

³⁴² Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 108.

³⁴³ Бычков В. В. Электронное следообразование преступной деятельности в сети Интернет // Расследование преступлений: проблемы и пути их решения. 2020. № 1 (27). С. 108.

неоднократного ее использования в процессе доказывания, например, в процессе судебно-экспертного исследования, предъявления как доказательства в ходе допроса и т. п.³⁴⁴ путем фотографирования (формирования скриншота) экрана с выведенной криминалистически значимой компьютерной информацией;

– криминалистически значимая компьютерная информация изымается вместе с электронным носителем информации, либо создается клон носителя информации, в случае, когда его изъятие невозможно или нецелесообразно.

К проблемам фиксации цифровых доказательств и, как следствие, обеспечения целостности данных и их доказательной силы в суде, можно отнести отсутствие единых методологических стандартов по их закреплению, недостаток сертифицированных программных технико-криминалистических средств, а также значительные временные и трудовые издержки неавтоматизированной фиксации криминалистически значимой информации. Непосредственное исследование данных зачастую осложняется их разнородностью, величиной массивов информации, подлежащих обработке, что требует использования специализированного программного обеспечения и высокопроизводительных вычислительных мощностей, что в совокупности обуславливает увеличение времени, затрачиваемого на анализ. По этой причине целесообразна разработка и активное использование адаптивных программных средств, позволяющих в условиях постоянной трансформации и эволюции киберпреступности систематизировать преступления в сфере компьютерной информации (присвоить им уникальные коды), в автоматизированном виде обеспечить как обнаружение, так и фиксацию доказательств в цифровой среде различного генеза³⁴⁵.

Достоверность (неизменяемость) и допустимость изъятых цифровых доказательств может обеспечить расчет контрольных сумм файлов. Как известно, основным способом установления дублирования, равно как определения идентичности двух электронных файлов, является дедупликация (тестовая проверка данных, заключающаяся в расчете их контрольных сумм (хеш-функций))³⁴⁶. По результатам выполнения теста в виде хеширования и установления полного соответствия хеш-функций можно сделать вывод об идентичности сравниваемых файлов. Соответственно, рассчитанная контрольная

³⁴⁴ Цифровые следы преступлений. Указ. соч. С. 18.

³⁴⁵ Харисова З. И. Программные технико-криминалистические средства как основа современной методики расследования преступлений в сфере компьютерной информации // Вестник Института права Башкирского государственного университета. 2025. № 3. С. 237.

³⁴⁶ Medjedovic Dz., Tahirovic E. Algorithms and data structures for massive datasets. New York : Manning Shelter Island, 2024. P. 44.

сумма электронного файла исключает проблему установления достоверности (неизменяемости) цифровых доказательств в процессе ее копирования или исследования. По этой причине необходимо рассмотрение возможности учета контрольных сумм цифровых доказательств в целях последующей допустимости их в суде, либо альтернативной возможности в виде внедрения блокчейн-платформ на базе распределенных реестров для обеспечения неизменности выявляемых данных³⁴⁷. Достоверность доказательств, в первую очередь, оценивается с точки зрения уголовно-процессуального законодательства, но стоит отметить, что источник получения доказательств должен быть своевременно проверен, должно быть подтверждение существования источника и факт получения доказательства. Относимость доказательств раскрывается применительно ко всем видам доказательств, так как данные, которые были получены в ходе проведения следственных действий, должны действительно иметь место и связь с подозреваемым или обвиняемым, либо с фактом совершенного преступления.

Помимо исследования все доказательства нуждаются в оценке. Это также род мыслительной деятельности субъектов расследования, при которой доказательства должны «придерживаться» критериев достоверности³⁴⁸, относимости и допустимости. Это нужно для того, чтобы при рассмотрении уголовного дела судом не возникло замечаний, отводов и ходатайств со стороны защиты. Стоит отметить, что все цифровые доказательства должны исследоваться и оцениваться в совокупности, так как отдельно взятое доказательство может противоречить другому отдельно рассматриваемому доказательству.

К насущным проблемам процессуального оформления цифровых доказательств можно отнести неопределенность процессуального статуса цифровых данных. Так, в соответствии с п. 4 ст. 81 УПК РФ электронные носители информации могут признаваться вещественными доказательствами, однако, критерии их допустимости не раскрываются. Кроме того, отсутствует четкая регламентация процедуры изъятия таких данных, например, с облачных сервисов или распределенных хранилищ. Кроме того, имеются пробелы в соблюдении правил изъятия и фиксации цифровых доказательств при удаленном доступе к данным, когда в соответствии со статьей 177 УПК РФ для этого требуется участие

³⁴⁷ Ryu J., Sharma P., Jo J. A blockchain-based decentralized efficient investigation framework for IoT digital forensics // The journal of supercomputing. 2019. № 75. P. 4380.

³⁴⁸ Харисова З. И., Лонщикова А. Р., Антонов В. В. Обеспечение достоверности и информационной безопасности проведения психофизиологических исследований в рамках уголовного судопроизводства в РФ и за рубежом // Евразийский юридический журнал. 2019. № 9 (136). С. 240.

понятых. Это может привести к оспариванию доказательств в суде.

Существенной проблемой является поиск и дальнейшее приобщение к делу криминалистически значимой информации, полученной из открытых источников сети «Интернет» и сервисов OSINT-разведки³⁴⁹, деятельность которых признается незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну, что стало особенно важно в свете дополнения УК РФ статьей 272.1, устанавливающей уголовную ответственность за незаконные сбор и хранение персональных данных, а также создание на их основе информационных ресурсов, предназначенных для распространения личной информации. Указанная коллизия может породить прецеденты, когда полученные цифровые доказательства признаются недопустимыми. С целью устранения данной проблемы возможно развитие систем сертификации специалистов, задействованных в раскрытии и расследовании преступлений в сфере компьютерной информации.

Таким образом, решение проблемы процессуального оформления цифровых доказательств при расследовании преступлений в сфере компьютерной информации требует комплексного подхода, включающего не только юридические нормы, но и технические меры, а также усовершенствованные криминалистические методики.

В целях соблюдения целостности и аутентичности цифровых доказательств целесообразно придерживаться широко распространенного в настоящее время принципа хронологической документации (от англ. «chain of custody» – цепочка поставок)³⁵⁰, который сможет обеспечить фиксацию всех этапов работы с доказательством. Проблема обеспечения сохранности цифровых данных при расследовании преступлений в сфере компьютерной информации, безусловно, требует технологических инноваций. Так, предотвратить утрату данных можно путем организации центров обработки данных на основе распределенных баз и облачных массивов, независимых дисковых данных (RAID-массивов) (от англ. «redundant array of independent disks» – избыточный массив независимых дисков) с возможностью расчета контрольных сумм и контроля версий хранилищ, либо внедрения блокчейн-технологий с временными метками, что обеспечит

³⁴⁹ Омельченко В. А., Фаниев П. А. Использование программного обеспечения категории Open Source, для создания анонимной рабочей среды и проведения разведки OSINT. М. : Перо, 2024. С. 52.

³⁵⁰ Nath S., Summers K., Jaejong B. Digital evidence chain of custody: navigating new realities of digital forensics // Intelligent systems, and applications. 2024. № 6. P. 12.

неизменность данных и прозрачность процесса их хранения. При этом защиту цифровых доказательств от посягательств можно обеспечить использованием квантово-устойчивых алгоритмов шифрования³⁵¹, что является одним из перспективных направлений реализации подобных систем в будущем. Таким образом, актуальность совершенствования механизма собирания цифровых доказательств в Российской Федерации обусловлена ростом преступлений в сфере компьютерной информации, обновлением способов, средств и условий совершения преступных деяний, а также рядом технологических вызовов. Реализация выдвигаемых предложений позволит повысить эффективность раскрытия и расследования указанного вида преступлений, обеспечить юридическую и техническую состоятельность цифровых доказательств, а также усилить взаимодействие между государственными органами и частным сектором в борьбе с киберугрозами.

Переходя к функциональным особенностям анализа доказательств в электронной форме необходимо отметить, что развитие информационных технологий способствовало не только информатизации общества, но и появлению новых способов и средств совершения преступлений, которые отличаются удобством применения и возможностью сокрытия цифровых следов. Как было указано ранее – собирание, исследование и оценку цифровых доказательств в настоящее время возможно осуществлять исключительно с применением программных технико-криминалистических средств. Соответственно, одним из вариантов обеспечения быстрой и эффективной обработки собранной криминалистически значимой компьютерной информации является внедрение в алгоритмы функционирования программ технологий искусственного интеллекта, основанных на математических моделях, реализованных по принципу организации сетей нервных клеток человека.

Однако расследование преступлений в сфере компьютерной информации осложняется не только проблемой выявления способов и средств совершения преступных деяний, но и сложностью исследования больших объемов электронных данных³⁵². При этом, как правило, лишь малая часть из массивов анализируемых сведений может представлять собой криминалистически значимую информацию. Определенный интерес в этом свете представляет модель регулирования

³⁵¹ Xiong J., Shen L., Liu Y. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption // Scientific Reports. 2025. № 15 (3). P. 12.

³⁵² Reyes A. Cybercrime investigations: bridging the gaps between security professionals, law enforcement, and prosecutors. Rockland : Syngress publishing, 2007. P. 24.

искусственного интеллекта, представленная в «Конвенции об искусственном интеллекте, правах человека, демократии и верховенстве права»³⁵³, согласно которой алгоритмы должны быть, во-первых, объяснимыми (для повышения уровня доверия к интеллектуальным технологиям за счет их понимания внешним наблюдателем), прозрачными (для осуществления общественного контроля за работой искусственного интеллекта) и справедливыми (для исключения дискриминации на расовой, культурной и гендерной почве), во-вторых, человекоцентричными. Поэтому автоматизировать процессы собирания и исследования цифровых доказательств с минимальными трудозатратами позволит специализированное программное обеспечение, разработанное на базе искусственного интеллекта и машинного обучения, при этом точность и прозрачность анализа данных смогут обеспечить самоинтерпретируемые модели (ХАИ-системы) (от англ. «explainable artificial intelligence (XAI) – объяснимый искусственный интеллект»), способные объяснять принимаемые решения адаптированным для человека языком, что особенно важно для исключения проблем предвзятости алгоритмов.

Наиболее перспективными направлениями применения методов обработки данных на основе искусственного интеллекта в области расследования преступлений в сфере компьютерной информации являются: проведение исследований и выдача заключений по вопросам, разрешение которых требует специальных знаний (например, в области информационно-телекоммуникационных технологий, эксплуатации информационных систем или использования программных технико-криминалистических средств), приобретаемых путем специальной подготовки и профессионального опыта, необходимых для решения вопросов, возникающих в процессе уголовного, гражданского судопроизводства, производства по делам об административных правонарушениях³⁵⁴; внедрение систем на основе искусственного интеллекта для проведения автоматизированного обнаружения, фиксации, изъятия и анализа цифровых доказательств; использование технологий распознавания по изображениям и видеоданным; анализ объемных мультимедийных файлов и пр. При этом необходимо соблюдать этическое использование интеллектуальных

³⁵³ Рамочная конвенция об искусственном интеллекте, правах человека, демократии и верховенстве права // Совет Европы : офиц. сайт. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225> (дата обращения: 11.01.2025).

³⁵⁴ Мещеряков В. А. Особенности специальных знаний, используемых в цифровой криминалистике // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4 (2). С. 91.

технологий, а также обеспечивать строгую регламентацию обучения и переобучения разрабатываемых на его основе систем, что возможно только при соблюдении единых стандартов управления процессами для анализа данных³⁵⁵. В этих целях на международном уровне активно ведутся дискуссии об ответственном использовании интеллектуальных разработок, разрабатываются национальные стратегии и планы по этичному использованию нейросетевых технологий, так, например, подготовлены документы по фундаментальным основам применения искусственного интеллекта «Принципы искусственного интеллекта»³⁵⁶, «Руководящие принципы по доверию искусственному интеллекту»³⁵⁷ и пр.

Таким образом, на сегодняшний день важно принять факт неотвратимости задействования технологий искусственного интеллекта в процесс расследования преступлений. Однако на стадии зарождения и реализации основного функционала рассмотренных систем необходимо заблаговременно определить базовые требования к нейросетевым разработкам и возможности их использования в области противодействия преступлениям с учетом применимости принципов справедливости, подотчетности, прозрачности и объяснимости всех осуществляемых искусственным интеллектом действий и принимаемых решений. Однако не существует единого инструмента или метода, который может собрать все необходимые доказательства, поскольку многие инструменты необходимо комбинировать, чтобы добиться их максимальной эффективности. Имеются методики использования инструментов, которые по преступлениям в сфере компьютерной информации могут являться эффективнее других (так, например, широко используется комплекс специальных знаний, сформированный на основе частной теории информационно-компьютерного обеспечения криминалистической деятельности³⁵⁸, или, например, OSINT-разведка, которые помогают осуществлять собирание цифровых доказательств и определять хронологию событий преступлений на основе методов анализа файловых хранилищ и активности в сети), а также криминалистическая регистрация, обеспечивающая сбор и накопление сведений для раскрытия, расследования и

³⁵⁵ Modeling problems legal regulation of the field of artificial intelligence / Z. I. Kharisova, V. V. Antonov, N. R. Kalimullin, A. I. Abdunagimov // IOP Conference Series: materials science and engineering. 2021. V. 1069. №. 1. P. 012002.

³⁵⁶ Recommendation of the council on artificial intelligence // Организация экономического сотрудничества и развития : офиц. сайт. URL: <https://legalinstruments.oecd.org> (дата обращения: 12.03.2025).

³⁵⁷ Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence // Портал законодательства Европейского союза : офиц. сайт. URL: <https://eur-lex.europa.eu/legal-content> (дата обращения: 12.03.2025)

³⁵⁸ Россинская Е. Р. Криминалистика. Указ. соч. С. 30.

предупреждения преступлений, создание условий для идентификации объектов, поиска ориентирующей информации, необходимой при принятии процессуальных и тактических решений, а также предоставления сведений, необходимых для правильной уголовно-правовой квалификации преступных деяний³⁵⁹.

Цифровые доказательства находятся в сложных формах, обусловленных структурой электронного носителя информации, соответственно, работа с ними осуществляется в рамках процессуальных действий, к производству которых, как правило, привлекаются специалисты. Так, в соответствии с ч. 2 ст. 164.1 УПК РФ, при производстве обыска или выемки, в ходе которых планируется изъятие компьютеров или иных носителей компьютерной информации, необходимо участие специалиста, обладающего специальными знаниями в области компьютерной техники, средств связи и передачи цифровой информации³⁶⁰.

Носителем компьютерных данных на международном уровне признается электронный носитель информации, представляющий из себя любой предмет или материал, с которого можно воспроизводить информацию с помощью или без помощи какого-либо устройства³⁶¹. Действующая в настоящее время процедура изъятия электронных носителей информации сопряжена с рядом трудностей и не всегда обеспечивает достаточную эффективность, а допустимость электронных доказательств в значительной степени определяется участием при обыске и выемке компьютерной информации специалиста. Однако данный факт все чаще вызывает сложности у практических работников и обширные дискуссии в научных кругах³⁶². Сторонники обязательного привлечения специалиста указывают на его роль в предотвращении утраты или искажения изымаемой информации³⁶³.

³⁵⁹ Ищенко П. П. Информационное обеспечение следственной деятельности : научно-практическое пособие. М. : Юрлитинформ, 2011. С. 33.

³⁶⁰ Курс криминалистики. Указ. соч. Т. 3. С. 170.

³⁶¹ National Cybercrime Strategy : Guidebook // Международная организация уголовной полиции (Интерпол) : офиц. сайт. URL: https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf (дата обращения: 11.01.2025).

³⁶² Flander B. Erbeznik A. Toolkit for handling and admissibility of electronic evidence empowering legal practitioners to critically. Review electronic evidence from the procedural rights perspective // Научно-исследовательский центр «ZRS Koper» : офиц. сайт. URL: https://www.zrs-kp.si/wp-content/uploads/2024/07/innocent_monografija_online_edition.pdf (дата обращения: 07.04.2025).

³⁶³ Гаврилин Ю. В., Балашова А. А. Процессуальный порядок собирания доказательств на энергонезависимых локальных электронных носителях информации // Сибирский юридический вестник. 2020. № 2 (89). С. 81; Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 23; Федулова А. Е. Участие специалиста в производстве следственных действий с электронными носителями информации // Юридическая наука и правоохранительная практика. 2023. № 1 (63). С. 82.

Ряд исследователей считают требование, закрепленное ч. 2 ст. 164.1 УПК РФ, избыточным³⁶⁴, аргументируя это ограничением процессуальной самостоятельности следователя, усложнением организационных мероприятий при подготовке и проведении следственных действий, увеличением затрачиваемого на уголовное судопроизводство времени.

Придерживаясь второй позиции необходимо отметить, что имеется ряд ситуаций, когда участие специалиста, безусловно обязательно, например, в случае изъятия энергозависимых носителей или вмешательства в конструкцию сложных технических средств. При этом, очевидно, что при изъятии съемных носителей информации участие специалиста не требуется, поскольку достаточно лишь их герметичного упаковывания.

Сложность исследования электронного носителя информации также зависит от его вида. Наиболее просты в работе объекты, не имеющие функций, ограничивающих к ним доступ, в отличие от мобильных средств связи³⁶⁵ и компьютеров. Стоит отметить также сложности, возникающие при осмотре IoT-устройств, а также удаленно расположенных носителей данных (веб-ресурсов), облачных хранилищ, распределенных реестров, аппаратных криптокошельков³⁶⁶, информационно-телекоммуникационных сетей с туннелированием³⁶⁷ и т. п. объектов и сред, которые могут потребовать участия в раскрытии и расследовании не только специалистов Управления по организации борьбы с противоправным использованием информационно-телекоммуникационных технологий, но также дополнительного привлечения сотрудников специализированных компаний в сфере информационно-телекоммуникационных технологий. Кроме того, требование участия специалиста при производстве копирования информации в ходе производства следственных действий представляется оправданным,

³⁶⁴ Шигуров А. В. Новеллы и проблемы правового регулирования порядка проведения следственных действий, связанных с изъятием электронных носителей информации // Гуманитарные и политико-правовые исследования. 2021. № 2 (13). С. 66; Козловский П. В., Седельников П. В. Участие специалиста в изъятии электронных носителей // Научный вестник Омской академии МВД России. 2014. № 1 (52). С. 18; Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : 12.00.09 : автореф. дис. ... канд. юрид. наук. Москва, 2020. С. 13.

³⁶⁵ Jian X., Siegel M., Towards a joint semantic analysis in mobile forensics environments // Digital investigation. 2025. V. 301846. P. 2.

³⁶⁶ Тисен О. Н. Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют // Уголовное право. 2024. № 3. С. 72.

³⁶⁷ Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. Т. 17. № 3 (136). С. 105.

поскольку это объяснимо необходимостью отождествления изъятой и скопированной информации.

По этой причине предполагается рациональным закрепление за следователем права, но не обязанности привлечения специалиста при изъятии электронного носителя информации, исходя из собственных компетенций³⁶⁸ (в зависимости от реальной необходимости в использовании специальных знаний при проведении следственных действий). Если в ходе следственных действий не проводится исследование информации, содержащейся на электронном носителе информации, как, например, в случае его осмотра или копирования данных, то решение вопроса об участии специалиста вполне может осуществляться следователем (дознавателем) самостоятельно в порядке ст. 168 УПК РФ³⁶⁹. Обращение с простыми электронными носителями информации, например, USB-накопителями, является на сегодняшний день бытовым навыком³⁷⁰, по этой причине, целесообразным представляется следующее дополнение ч. 2 ст. 164.1 УПК РФ – «Энергозависимые электронные носители информации подлежат изъятию с участием специалиста. В иных случаях специалист привлекается по усмотрению следователя при отсутствии у последнего компетенций, исключающих риск повреждения, модификации или уничтожения данных. Изъятие или копирование информации сопровождается видеозаписью, за исключением ситуаций изъятия энергонезависимых носителей без исследования их содержимого».

Дополнительно следует рассмотреть вопрос о разработке методических рекомендаций по изъятию цифровых доказательств, адаптируемых к изменяющимся условиям технического прогресса и совершенствовании системы подготовки специалистов. Указанные проблемы также требуют учета современных технологических вызовов, включая распространение облачных хранилищ и IoT-устройств, не подпадающих под традиционное понимание носителя информации.

³⁶⁸ Мещеряков В. А., Цурлуй О. Ю., Кудрявцев Ю. С. К вопросу об оценке компетенции судебного эксперта // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научной конференции. Москва : Российский государственный университет правосудия, 2021. С. 420.

³⁶⁹ Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С.48.

³⁷⁰ Рудаков Б. В. К вопросу о проблемах использования цифровых (электронных) данных в доказывании по уголовным делам // Правопорядок: история, теория, практика. 2021. № 1 (28). С. 67

Рассматривая направления оптимизации процесса собирания, исследования, оценки и использования цифровых доказательств стоит отметить тенденцию цифровизации деятельности МВД России, отражающуюся в мероприятиях по реализации программ развития³⁷¹, направленных на повышение эффективности применения современных технических средств в интересах совершенствования процесса управления и взаимодействия подразделений МВД России с населением. Так, вводимое понятие «цифровой полицейский» подразумевает под собой сотрудника органов внутренних дел Российской Федерации, оснащенного современными программными технико-криминалистическими средствами, осуществляющего свою деятельность в едином цифровом пространстве МВД России³⁷².

Ускоренный темп технологического прогресса, переход к цифровой экономике, внедрение технологий автоматизации в различные процессы жизнедеятельности человека привели к повсеместной обработке данных в электронной форме. Однако положительные тенденции развития технологий одновременно породили негативные, связанные с их противоправным применением. Ежегодный рост числа преступлений, совершаемых с применением информационно-телекоммуникационных технологий³⁷³, показывает, что применение традиционных методов собирания и исследования доказательств при расследовании одних из наиболее распространенных в настоящее время преступных деяний недостаточно. Поэтому активное внедрение современных технологий в деятельность правоохранительных органов будет способствовать расширению использования аналитических методов, что значительно повлияет на организацию расследования преступлений. Соответственно, автоматизация процессов сбора, хранения, систематизации и анализа криминалистически значимой информации повысит эффективность следственной, оперативно-розыскной, экспертной и судебной деятельности, способствуя научной организации труда и оптимизации процессов расследования³⁷⁴.

³⁷¹ Об утверждении концепции научного обеспечения деятельности органов внутренних дел Российской Федерации на период до 2030 года : приказ МВД России от 13 ноября 2020 г. № 767 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_7519 (дата обращения: 17.03.2025).

³⁷² Сухов А. В., Конюшев В. В. Цифровая полиция как эргатическая система, функционирующая в цифровой экосистеме // Правовая информатика. 2021. № 2. С. 29.

³⁷³ Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 года и ожидаемые тенденции ее развития. Указ. соч. С. 55.

³⁷⁴ Зеленский В. Д., Меретуков Г. М. Криминалистика. Указ. соч. С. 704.

Проведенное исследование позволяет сделать вывод, что основными направлениями совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации являются:

- подробная регламентация и алгоритмизация процесса собирания, хранения и использования цифровых доказательств³⁷⁵, что в условиях постоянной трансформации и эволюции преступлений рассматриваемого вида возможно, например, при тщательной классификации способов, средств и условий совершаемых преступных деяний, а также присвоения им уникальных кодов в целях разработки общей концепции их расследования и выработки соответствующих заданным условиям алгоритмов расследования;
- введение национальных стандартов по фиксации и анализу цифровых доказательств³⁷⁶, а также развитие систем сертификации специалистов, задействованных в раскрытии и расследовании преступлений в сфере компьютерной информации;
- расширение перечня программных технико-криминалистических средств для автоматизированного поиска, фиксации и исследования цифровых доказательств на базе технологий искусственного интеллекта и анализа больших данных;
- развитие облачных платформ для безопасного и неизменного хранения цифровых доказательств с применением блокчейн-технологий, распределенных реестров;
- создание единого кластера данных с возможностью оперативного доступа к цифровым доказательствам, поиска и обработки криминалистически значимой информации с использованием ключевых слов и фильтров в едином сегменте сети.

Подводя итог вышеуказанному, можно отметить, что криминалистика как наука, изучающая закономерности механизма преступления и возникновения информации о нем, в условиях всеобщей цифровизации и интеллектуализации приобретает новые исследовательские и практико-ориентированные возможности.

Технологии искусственного интеллекта представляют собой дополнительный инструмент, интегрируемый в систему криминалистических

³⁷⁵ Об утверждении плана мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства Российской Федерации от 14 августа 2025 г. № 2207-р // Правительство Российской Федерации : офиц. сайт. URL: <http://government.ru/docs/55975> (дата обращения: 14.08.2025).

³⁷⁶ Усов А. И. Стандарты судебной экспертизы как инструмент цифровизации криминалистики. Указ. соч. С. 220.

средств. Искусственный интеллект при этом может рассматриваться многоаспектно – как прикладная компьютерная система, как область фундаментального научного знания, как предмет научного познания, метод решения научных и иных задач и как признак технологической системы³⁷⁷.

В соответствии с Указом Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» искусственный интеллект представляет собой совокупность технологических решений, позволяющих имитировать когнитивные функции человека, включая способность к принятию решений вне рамок заранее заданного алгоритма. Одним из наиболее значимых направлений использования искусственного интеллекта в криминалистике является установление закономерных связей между элементами криминалистической характеристики преступления, что позволяет выявлять причинно-следственные и вероятностные связи между обстоятельствами преступных деяний, формулировать частные криминалистические версии, в том числе версии о распространенности (серийности) преступлений, идентифицировать лиц, потенциально причастных к преступной деятельности и пр. Кроме указанной возможности перспективным представляется анализ и интерпретация цифровых доказательств. Однако следует отметить наличие структурных и технических ограничений, связанных с фрагментацией существующих информационных ресурсов. На текущий момент базы данных различных ведомств являются несогласованными, разобценными, что затрудняет доступ следователей и оперативных сотрудников к информации. Это обуславливает необходимость разработки единой криминалистической информационной платформы с унифицированными протоколами доступа.

В качестве подтверждения важности применения искусственного интеллекта в криминалистике необходимо отметить исследование, проведенное Научно-исследовательским институтом криминалистики Главного управления криминалистики Следственного комитета Российской Федерации. Интеллектуальный анализ более 1000 уголовных дел о серийных преступлениях сексуального характера, совершенных 186 преступниками, позволил построить цифровые криминалистические модели серийных преступников, включающие 27 личностных признаков, географические координаты мест совершения преступлений и жительства преступника и потерпевшего, время и используемые средства совершения преступления, а также возраст потерпевших³⁷⁸.

³⁷⁷ Бахтеев Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 2 (28). С. 32.

³⁷⁸ Бессонов А. А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1. С. 98.

Применение методов математической статистики и анализа данных на основе интеллектуальных алгоритмов обеспечило точность прогнозирования на уровне 92–98 %, что свидетельствует о высокой криминалистической значимости примененных подходов. На том же наборе данных был разработан алгоритм географического профилирования, направленный на прогнозирование расстояния от места преступления до возможного места жительства преступника, его возраста, вероятности наличия у него психических расстройств, судимости, транспортного средства, а также факта его знакомства с жертвой и семейного статуса. Точность прогноза варьировалась в диапазоне 76–96 % в зависимости от конкретного признака, что являлось подтверждением эффективности построенной интеллектуальной архитектуры для решения криминалистических задач.

При рассмотрении направлений повышения эффективности расследования рассматриваемых в работе преступлений с задействованием технологий искусственного интеллекта, в частности, для обработки цифровых доказательств, с учетом проведенного структурно-содержательного анализа представляется вполне целесообразным выделение криминалистических характеристик преступлений в сфере компьютерной информации (различных по составу). Именно методы искусственного интеллекта могут позволить провести тщательный корреляционный анализ цифровых данных³⁷⁹, обеспечивая устранение ложных корреляций и составление корреляционных таблиц, отображающих коэффициенты взаимосвязи между различными переменными анализа (элементами криминалистической характеристики преступления). Соответственно, основой большинства выводов, формируемых искусственным интеллектом, могут являться закономерные связи, выявляемые между элементами криминалистической характеристики преступления. Однако в рамках этих закономерностей могут встречаться исключения и отклонения от типичных случаев.

Преимуществом искусственного интеллекта является способность обрабатывать и учитывать такого рода отклонения, обучаясь в том числе на них, что позволяет выходить за рамки стереотипных представлений о взаимосвязях между элементами криминалистической характеристики и формировать новые структуры криминалистического знания, опираясь на вероятность, а не только на повторяемость³⁸⁰. Применение искусственного интеллекта также способствует развитию частных криминалистических теорий, так, его интеграция в указанные теории способствует расширению методологической базы криминалистики, трансформации ее понятийного аппарата и практических методик. Отсюда следует,

³⁷⁹ Harisha A., Mishra A., Singh C. Advancements in cybercrime investigation and digital forensics. New York : Apple Academic Pres, 2023. P. 27;

³⁸⁰ Gautam Y. Integrating artificial intelligence into cybercrime investigation: Challenges and future directions // International journal for multidisciplinary research. 2024. V. 6. № 5. P. 2.

что интеграция искусственного интеллекта в криминалистическую практику становится не просто желательной, но и объективно необходимой.

В условиях роста объемов данных, связанных с преступлениями в сфере компьютерной информации, важным аспектом становится использование искусственного интеллекта и методов машинного обучения для анализа больших данных, выявления шаблонов преступной активности и оперативного принятия решений в условиях неопределенности. На сегодняшний день при расследовании рассматриваемых преступлений традиционных средств и методов управления данными для реализации полноценного анализа формируемых больших массивов цифровых доказательств явно недостаточно. Для решения указанной проблемы также возможно использование технологий искусственного интеллекта. Поскольку методы и способы совершения преступлений в сфере компьютерной информации постоянно меняются, анализ, основанный на жестких алгоритмах, становится неприменим. В противовес, технологии искусственного интеллекта и машинного обучения позволяют анализировать такие данные в режиме реального времени, с возможностью выдачи решения по поставленной задаче с гибкой адаптацией к систематически изменяющимся характеристикам массивов информации.

Однако наравне с преимуществами существуют риски использования искусственного интеллекта в противодействии преступности, связанные с предвзятым принятием решений, по этой причине в обязательном порядке необходимо использование технологий объяснимого искусственного интеллекта, т. е. самоинтерпретируемых ХАИ-систем, обеспечивающих создание информационных систем, способных объяснять свои действия и принимать решения понятным для человека образом.

Таким образом, использование технологий искусственного интеллекта в раскрытии и расследовании преступлений в сфере компьютерной информации представляет собой перспективное направление, способствующее развитию криминалистической науки и совершенствованию правоохранительной деятельности. Оно отражает переход к новой парадигме криминалистического мышления, основанной на вероятностных данных и цифровом моделировании. В свете рассмотрения прикладных аспектов расследования преступлений в сфере компьютерной информации в дальнейшем необходимо выявить особенности возбуждения уголовных дел и производства следственных действий по указанным преступным деяниям, определив взаимосвязи между складывающимися следственными ситуациями и алгоритмами расследования.

ГЛАВА 3. ОСНОВЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

3.1. Особенности возбуждения уголовных дел о преступлениях в сфере компьютерной информации

Уголовное преследование, осуществляемое на стадии предварительного расследования, представляет собой сложный вид деятельности, требующей от следователя или дознавателя высокого уровня профессиональных знаний и навыков, активности и настойчивости при раскрытии и расследовании преступного деяния, а также своевременного и юридически обоснованного привлечения к уголовной ответственности лиц, причастных к его совершению. Наиболее эффективно реализовать полномочия по уголовному преследованию возможно при условии строгого соблюдения норм и требований уголовно-процессуального законодательства, квалифицированного применения криминалистических средств при производстве следственных действий, а также рациональной организации расследования, в основе которой лежит техника планирования.

К стадии возбуждения уголовного дела относят систему действий и правоотношений в виде принятия, рассмотрения и проверки заявлений и сообщений о совершенных или готовящихся преступлениях, принятие мер по их предотвращению, пресечению или предупреждению, а также принятие решений о возбуждении уголовного дела или об отказе в нем³⁸¹.

Поводами для возбуждения уголовного дела о преступлениях, совершаемых в сфере компьютерной информации, являются: обращения (заявления) физических и юридических лиц, обладающих правом собственности или законным правом пользования компьютерной информацией, подвергшейся противоправному воздействию; обнаружение признаков преступления органом дознания в результате проверки сообщения о совершенном или готовящемся преступлении, поступившем из оперативных источников, в ходе проведения оперативно-розыскных мероприятий, по материалам проверок или при задержании лица с поличным на месте совершения преступления; материалы, опубликованные в

³⁸¹ Белкин Р. С. Курс криминалистики. Указ. соч. С. 69.

средствах массовой информации; факты обнаружения признаков преступления следователем или прокурором при расследовании преступлений иного вида; явка с повинной³⁸².

Исходя из анализа материалов уголовных дел и судебно-следственной практики в подавляющем большинстве поводом для возбуждения уголовного дела по ст. ст. 272 и 273 УК РФ являлись заявления о преступлении. По иным составам наблюдались обращения представителей операторов связи о выявлении противоправных деяний, совершаемых сотрудниками компании или организаций, представляющих дилерскую сеть.

Для принятия обоснованного решения о возбуждении уголовного дела уполномоченному субъекту необходимо иметь в распоряжении совокупность определенных сведений и документов, в частности, письменное заявление потерпевшего или протокол, составленный в соответствии с положениями УПК РФ, о принятии устного заявления о совершенном деянии, содержащем признаки преступления, рапорт об обнаружении признаков преступного деяния и сопутствующие материалы (например, полученные в результате проведения оперативно-розыскных мероприятий, либо документальных проверок, ревизий), письменное объяснение заявителя, включающее все криминалистически значимые сведения (время и место совершения (обнаружения) преступления, предмет преступного посягательства, его индивидуальные характеристики, данные о технических средствах, используемых предполагаемым субъектом преступления, включая задействованные IP-адреса, IMEI-коды, MAC-идентификаторы, учетные данные, абонентские номера и иные технические данные, идентифицирующие преступника).

Помимо указанных к материалам проверки могут приобщаться протоколы осмотров места происхождения, технических средств, электронных носителей информации или информационных систем, средств защиты информации, программного обеспечения, в том числе вредоносного, информационно-телекоммуникационных сетей, информационных ресурсов и пр., документы (или их копии), подтверждающие правомерность доступа или владения компьютерной информацией, техническими средствами, электронными носителями информации или информационными системами и прочими объектами преступного посягательства в виде договоров на оказание услуг связи, предоставления доступа к сети «Интернет», хостингового или банковского обслуживания, сведения о

³⁸² Криминалистика : учебник / под ред. Л. В. Бертовского. М. : РГ-Пресс, 2018. С. 939.

сертификатах электронной цифровой подписи, удостоверения о владении доменом, свидетельства о государственной регистрации программ для ЭВМ и т. п., а также заключения экспертов по исследованиям объектов, документы, удостоверяющие факт распространения вредоносного программного обеспечения или охраняемой законом информации, либо электронные носители информации с защищаемыми данными, акты проверок служб, обеспечивающих информационную безопасность, локальные нормативные документы организаций, регламентирующие работу с техническими средствами, электронными носителями информации, информационными системами, средствами защиты информации, программным обеспечением, информационно-телекоммуникационными сетями, информационными ресурсами и т.п.

Обстоятельствами, подлежащими установлению и доказыванию по делам о преступлениях в сфере компьютерной информации, являются: факт совершения преступного деяния с установлением возможности непреодолимых факторов; причина наступления уничтожения, блокирования, модификации либо копирования компьютерной информации; правовой статус компьютерной информации (публичного либо ограниченного доступа); место и время совершения преступного деяния; способ реализации преступного умысла (непосредственный или удаленный доступ); правовой режим доступа к компьютерной информации и техническим средствам, обрабатывающим ее; конкретные технические средства, электронные носители информации, информационные системы, средства защиты информации, программное обеспечение, информационно-телекоммуникационные сети и информационные ресурсы, задействованные при совершении преступного деяния, включая их тип, характеристики, функциональные и эксплуатационные возможности, техническое состояние, идентифицирующие признаки; наличие уязвимостей в технических средствах, информационных системах, средствах защиты информации, программном обеспечении или информационно-телекоммуникационных сетях или утечек конфиденциальных сведений из информационных систем, баз данных и пр.; размер причиненного ущерба и порядок его определения; служебные действия, с которыми сопряжено преступление, круг лиц, ответственных за их выполнение и их должностные инструкции (регламенты), локальные нормативные акты, регламентирующие работу с техническими средствами, электронными носителями информации, информационными системами, средствами защиты информации, программным обеспечением, информационно-телекоммуникационной сетью, информационными

ресурсами и другие данные о личности подозреваемого, включая уровень его профессиональных навыков в области информационных технологий; сведения о возможных соучастниках, роли каждого участника; мотивы преступного деяния; данные о потерпевшем лице и предмете преступного посягательства; сведения о возможных свидетелях преступного деяния, лицах содействовавших сокрытию преступления; причины и условия, способствовавшие совершению преступного деяния, включая возможные причины нарушений требований нормативных актов, инструкций и регламентов.

Должностное лицо, уполномоченное на принятие и регистрацию такой информации, составляет рапорт об обнаружении признаков преступления в соответствии со ст. 143 УПК РФ. Довольно часто источниками указанных сведений являются материалы, полученные в рамках проведения оперативно-розыскных мероприятий.

От своевременности и полноты проверки сообщения (заявления) о преступлении, заключающейся в сборе первичной информации, зависит возможность фиксации следов преступления и обеспечение сохранности доказательственной базы. В силу ч. 1 ст. 144 УПК РФ решение о возбуждении уголовного дела, передаче по подследственности либо об отказе в его возбуждении должно быть принято не позднее 3 суток с момента поступления соответствующего сообщения. Однако на практике, как показал анализ уголовных дел, часто имеет место продление сроков проверки в порядке ч. 3 ст. 144 УПК РФ под предлогом ожидания ответа на направленный запрос (особенно по направленным на бумажных носителях), например, поставщикам услуг связи, финансово-кредитным и иным учреждениям, что в ряде случаев является фактором, влияющим на увеличение срока расследования.

Использование сервисов электронного документооборота при направлении запросов в организации, с которыми заключен соответствующий договор, отчасти решает данную проблему.

Так, установлены правила предоставления владельцем агрегатора сведений с использованием единой системы межведомственного электронного взаимодействия по запросам уполномоченных государственных органов, которые осуществляют присоединение информационных систем различных организаций к инфраструктуре, обеспечивающей информационно-технологическое

взаимодействие систем, используемых для предоставления государственных и муниципальных услуг в электронной форме³⁸³.

Недостаточная скорость обмена данными не позволяет повысить эффективность предотвращения, выявления и пресечения преступлений и угроз государственной безопасности Российской Федерации, что в свою очередь создает риски причинения ущерба жизни, здоровью и имуществу граждан. В результате налаженного взаимодействия предоставление сведений (например, о пользователе агрегатора (абонентский номер в сети оператора подвижной радиотелефонной связи, адрес электронной почты), точные дата и время осуществления доступа пользователя к агрегатору, IP-адрес пользователя, сведения о товарах, работах и услугах, размещенных или выполненных посредством агрегатора пользователем и пр.) будет осуществляться в кратчайшие сроки.

Для преступлений в сфере компьютерной информации характерно осуществление противоправного воздействия посредством использования различных технических средств, электронных носителей информации и информационно-телекоммуникационных сетей. В рамках доследственной проверки сведений о рассматриваемых преступлениях особую значимость приобретают такие следственные действия как осмотр места происшествия, предметов и документов, назначение и производство судебных экспертиз, а также иные процессуальные действия, направленные на обеспечение фиксации, изъятия и последующего исследования доказательств, преимущественно относящихся к цифровым данным. По рассматриваемым преступлениям довольно важное значение имеют также получение объяснений, истребование документов и предметов, направление запросов, предъявление требований, поручений, в том числе поручений о проведении оперативно-розыскных мероприятий.

³⁸³ Положение о единой системе межведомственного электронного взаимодействия : постановление Правительства Российской Федерации от 08 сентября 2010 г. № 697 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_104665/59a1ee33e6096f0bf3fd23d27eeb41a502ed129e (дата обращения: 30.10.2025); О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме : постановление Правительства Российской Федерации от 22 декабря 2012 г. № 1382 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_139820/fbd07791b302296474e4be2c2_ee28baf46599852 (дата обращения: 31.07.2025); Об утверждении Правил предоставления владельцем агрегатора информации о товарах (услугах) сведений с использованием единой системы межведомственного электронного взаимодействия по запросу уполномоченного государственного органа, осуществляющего оперативно-розыскную деятельность : постановление Правительства Российской Федерации от 30 августа 2025 г. № 1328 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: <https://www.consultant.ru/law/hotdocs/90673.html> (дата обращения: 27.05.2025).

Стоит также отметить, что в ходе проведения осмотра места происшествия, предметов и документов зачастую осуществляется не только выявление, но и изъятие технических средств и электронных носителей информации, потенциально содержащих следы преступной деятельности. Отдельного внимания заслуживает определение важности процедуры получения объяснений на стадии проверки сообщения о преступлении. В соответствии со ст. 144 УПК РФ при проверке сообщения о преступном деянии допустимо получать у граждан объяснения, при этом условно возможно применять положения, регламентирующие порядок проведения следственных действий, в том числе допросов граждан³⁸⁴. Такого рода документы (относимые к категории «иные») являются источником информации об обстоятельствах, подлежащих доказыванию, и потенциально могут выступать в качестве ориентирующей информации для проводящего проверку сообщения должностного лица. Важность объяснений заключается в том, что они способствуют пониманию, имеются ли основания для возбуждения уголовного дела, а также обозначают возможные направления проведения следственных действий и подготовки предписаний для исполнения поручений о проведении оперативно-розыскных мероприятий. Стоит отметить, что именно получение объяснений, как это будет описано далее, может выступить отправной точкой алгоритмизации процесса расследования преступлений в сфере компьютерной информации и процесса поддержки принятия решений по уголовному делу должностным лицом.

Проведенный анализ уголовных дел свидетельствует об отсутствии систематичности при планировании следственных действий по преступлениям в сфере компьютерной информации, что обусловлено их многообразием, сложностью в определении подхода к их расследованию, а также выявления механизма совершения преступлений, исследования технических средств, поиска, собирания цифровых доказательств. Стоит также отметить, что зачастую совместная работа служб и подразделений правоохранительных органов выстроена недостаточно эффективно, проверочные мероприятия и следственные действия, направленные на установление обстоятельств совершенных преступлений, обнаружение, фиксацию цифровых следов и исследование последствий, предусмотренных объективной стороной состава указанного вида преступлений, в полном объеме не проводятся.

³⁸⁴ О порядке получения объяснений : разъяснения прокуратуры // Генеральная прокуратура Российской Федерации (Саратовская область) : офиц. сайт. URL: https://epp.genproc.gov.ru/ru/proc_64/activity/legal-education/explain/e692937/ (дата обращения: 07.05.2025).

Одно из направлений развития криминалистики соотносится с алгоритмизацией оперативно-розыскной, следственной и экспертной деятельности³⁸⁵. Систематичность при планировании следственных действий по преступлениям определенного вида может быть достигнута использованием заранее сформированного исходя из сложившейся практики расследования алгоритма действий. В связи с этим необходимо рассмотреть действующую последовательность шагов и их типичных вариаций на этапе возбуждения уголовного дела. Так, на примере расследования преступления в сфере компьютерной информации на стадии доследственной проверки можно сформулировать алгоритм в виде порядка действий. Алгоритмизация может заключаться в формализации действий (процесс перевода описания задач на язык формального представления) в соответствии с действующими нормативными актами, регламентирующими порядок действий сотрудников в той или иной ситуации. Так, при получении сообщения (заявления) о преступлении сотрудник дежурной части в ходе устного опроса заявителя (лица, сообщившего об указанном факте) уточняет обстоятельства, имеющие значение при проведении проверки сообщения о преступлении, а именно дату, время, способ и средства совершения преступления (с указанием задействованных при совершении преступления учетных записей, абонентских номеров, с которых поступали телефонные звонки, аккаунты мессенджеров и социальных сетей, в которых осуществлялась переписка, номера расчетных счетов, банковских карт, электронных кошельков) и прочие установочные данные лица, от которого поступило сообщение (заявление). После регистрации обращения в книге учета сообщений о преступлениях подчиненным дежурным нарядом в течение дежурных суток организуется проведение первоначальных проверочных мероприятий. Сотрудник органа дознания или следственного подразделения проводит опрос лица, сообщившего о преступлении в сфере компьютерной информации, устанавливая:

- обстоятельства обнаружения потерпевшим факта совершения преступного деяния, время обнаружения, местонахождение, тип и иные данные технических средств, используемых при совершении преступления, точки выхода в сеть «Интернет» (при наличии) и пр.;
- последствия совершенных преступниками действий, например, в результате уничтожения, блокирования, модификации, либо копирования информации, нарушения правил эксплуатации технических средств и пр.

³⁸⁵ Колдин В. Я. Типовые модели и алгоритмы криминалистического исследования. М. : Московский университет, 1989. С. 4.

- факт установленного на техническом средстве антивирусного программного обеспечения, его параметры, характеристики;
- факт и обстоятельства передачи третьим лицам учетных данных к техническим средствам, носителям информации или информационным системам;
- факт наличия на технических средствах или электронных носителях информации учетных данных для доступа к компьютерной информации;
- иные особенности, связанные с действиями потерпевшего, например, факт перехода по фишинговым ссылкам в сети «Интернет», скачивание вредоносного программного обеспечения, наступление последствий после совершенных действий, в частности, при взломе аккаунтов социальных сетей факт получения писем или сообщений от имени потерпевшего его подписчиками (кто получал письма, какого характера сообщение, сведения, указанные в нем, в том числе банковские реквизиты, номера банковских карт, абонентских номеров и пр.);
- обстоятельства регистрации аккаунта социальной сети (дата, местонахождение, тип технических средств, использованные адреса электронной почты) с учетом того, что при регистрации авторизационные данные могут храниться в материалах входящей корреспонденции электронной почты потерпевшего.

После выяснения указанных обстоятельств сотруднику органа дознания или следственного подразделения целесообразно проверить полученные сведения об использованных в преступной схеме банковских реквизитах, IP-адресах и абонентских номерах по учетам подсистемы информационно-аналитического обеспечения мероприятий по раскрытию преступлений, совершаемых с использованием информационных технологий интегрированного банка данных «Дистанционное мошенничество».

Сбор информации при проверке сообщений о преступлениях (т. е. до возбуждения уголовного дела) может производиться, например, при осмотре места происшествия, документов и предметов (ст. 176 УПК РФ) или в рамках судебной экспертизы (ст. 197 УПК РФ). Не останавливаясь на деталях производства указанных следственных действий (поскольку их раскрытие предполагается по тексту в дальнейшем) стоит отметить, что анализ особенностей проведения осмотра по делам о преступлениях в сфере компьютерной информации, осуществляемого именно на этапе возбуждения уголовного дела, позволяет акцентировать внимание на необходимости решения следующих организационно-процессуальных задач:

- обеспечение изоляции технических средств от несанкционированного

доступа (физического и удаленного) в целях предотвращения изменений в обстановке совершения преступного деяния и уничтожения цифровых доказательств;

- поиск на месте происшествия различных электронных носителей информации и устройств считывания данных;
- анализ и изъятие документации и записей, например, находящихся рядом с осматриваемыми техническими средствами;
- надлежащее изъятие и упаковка объектов с участием специалиста, обладающего специальными знаниями в области информационных технологий;
- грамотная фиксация цифровых доказательств, в том числе следов общего криминалистического происхождения, в частности, с использованием программных технико-криминалистических средств.

Содействие в обнаружении, фиксации и изъятии цифровых следов, консультирование следователя по вопросам применения технических средств, установлении функциональных особенностей исследуемых объектов оказывает привлеченный к производству осмотра специалист, присутствие которого обусловлено в первую очередь необходимостью своевременного и грамотного сбора криминалистически значимой информации. Кроме того, в целях повышения эффективности осмотра может быть привлечен, например, владелец электронного носителя информации, системный или сетевой администратор организации, программист, знакомый с архитектурой, топологией и техническими параметрами исследуемых устройств.

Проведение проверки сообщения о преступлении, совершенного в сфере компьютерной информации, требует получения, исследования и анализа цифровых следов и иной криминалистически значимой информации. В целях установления обстоятельств, подлежащих доказыванию, необходимо инициировать истребование документов посредством направления соответствующих запросов в учреждения и организации, обладающие сведениями, имеющими доказательственное значение, в том числе – к операторам связи и провайдерам доступа в сеть «Интернет». Кроме того, источниками информации, имеющей значение для уголовного дела, могут являться компьютерное и серверное оборудование, мобильные устройства, базы данных, облачные хранилища данных и сетевой трафик. Основным методом сбора цифровых доказательств является использование специализированных программных технико-криминалистических средств, например, для анализа дампов памяти и сетевого трафика, исследования облачных ресурсов.

Опрос лиц, предположительно осведомленных о событии преступления, должен включать в себя:

- установление объективности сведений, полученных от лица, по соответствию произошедшему, в том числе выяснение осведомленности лица в области использования компьютерной информации и информационных технологий в целом, с указанием данных о его личности (образование, род деятельности и пр.);
- получение информации о технических средствах (в том числе о телекоммуникационных устройствах), посредством которых лицом осуществлялся выход в сеть «Интернет» или иная цифровая активность, имеющая отношение к совершению противоправных деяний, с целью их последующего изъятия и проведения криминалистического исследования;
- установление канала подключения к сети «Интернет» (посредством проводных и беспроводных сетей или мобильной сети связи);
- выяснение информации об используемом интернет-браузере с целью возможного выявления в нем данных об истории посещенных ресурсов, принимаемых в качестве цифровых доказательств;
- выявление фактов использования альтернативных операционных систем, специализированных браузеров (например, «Tor»), средств анонимизации и обхода блокировок (сервисов «VPN», прокси-серверов и пр.).

Кроме того, процессуальный порядок получения и фиксации цифровой доказательственной информации определяется ее техническими характеристиками и правовой природой. Однако производство следственных действий, в том числе обнаружение, изъятие, копирование и исследование информации в электронном виде, имеющей значение для дела, требует интеграции юридических и технических знаний. Сложность расследования преступлений, связанных с использованием информационно-телекоммуникационных технологий и различных технических средств, зачастую объясняется стохастической и бесперспективной практикой принятия решений на основе лишь личного опыта, либо интуиции следователя, без задействования современных научных методов познания, а также выявления и анализа криминалистически значимой информации, с учетом возможностей электронных вычислительных машин³⁸⁶.

По этой причине в дальнейшем необходимо рассмотреть и систематизировать организационно-тактические особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации.

³⁸⁶ Типовые модели и алгоритмы криминалистического исследования. Указ. соч. С. 65.

3.2. Организационно-тактические особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации

Предварительное расследование является одной из форм правоохранительной деятельности, в рамках которой наделенные соответствующими полномочиями государственные органы реализуют одну из важнейших социальных функций – расследование преступных деяний, что представляет собой процессуально урегулированную форму деятельности, осуществляемую в соответствии с уголовно-процессуальным законодательством.

На первоначальном этапе расследования преступления в сфере компьютерной информации одной из важнейших задач является фиксация обстановки места происшествия, а также следовой информации и состояния функционирования технических средств, программного обеспечения, информационных систем, средств защиты информации и пр. Важным также является выявление очевидцев и лиц, обладающих сведениями, которые представляют интерес для следствия. Однако наиболее значимым на данном этапе является процессуальное закрепление информации о предмете и механизме преступного посягательства, способах и средствах совершения преступления, а также поиск цифровых доказательств. В случае расследования трансграничных преступлений зачастую необходима организация международного оперативного взаимодействия с правоохранительными органами иных государств и международными полицейскими структурами. На последующем и заключительном этапах расследования детально исследуются способы совершения преступления, устанавливаются особенности механизма преступного деяния, выявляется личность преступника (либо сведения, способствующие его розыску). Субъект расследования сосредоточивает процессуальные усилия на собирании доказательственной информации, устанавливающей вину подозреваемого, мотивы его действий, а также причинно-следственные связи между его поведением и наступившими последствиями. Кроме того, анализируются результаты экспертиз, запросов и поручений, на основе которых при необходимости проводятся повторные следственные действия и экспертизы, что предшествует формированию доказательственной базы, а также установлению обстоятельств, подлежащих доказыванию. Особенность предварительного расследования заключается в том, что она сопряжена с реализацией принудительных мер, затрагивающих конституционные права личности, по этой причине применение таких мер должно

строго соответствовать основным принципам уголовного судопроизводства. УПК РФ достаточно подробно регламентирует только общие правила следственных действий, предоставляя при этом следователю определенную степень свободы, например, в выборе тактических приемов, возможности привлечения специалиста, а также использования технико-криминалистических средств, необходимых для получения доказательственной информации, что является довольно важным аспектом по преступлениям в сфере компьютерной информации. Указанный факт создает предпосылки для применения криминалистических знаний, методов и новейших информационных технологий в целях повышения эффективности расследования преступлений. От обстоятельств, сложившихся в рамках той или иной следственной ситуации (которые по рассматриваемому виду преступлений преимущественно подразумевают активные действия злоумышленника по умышленному искажению или сокрытию следов преступной деятельности), зависит организация первоначального этапа расследования преступления, выдвижение версий и постановка задач.

Типичные следственные ситуации формируются на основе анализа и систематизации следственной практики³⁸⁷ и играют значимую роль в целях определения направлений следственной деятельности на конкретном этапе расследования. Так, указанные следственные ситуации (как фактическое положение на конкретный момент расследования и степень информационной осведомленности субъекта расследования в указанный момент) могут выступать основанием для моделирования возможных сценариев хода расследования, с учетом специфики исходной информации и криминалистической характеристики преступного деяния. Кроме того, они позволяют осуществлять алгоритмизацию расследования, установление приоритетности, объема и последовательности следственных действий, а также оперативно-розыскных мероприятий, необходимых для достижения задач уголовного судопроизводства. Следственные ситуации, складывающиеся по рассматриваемым преступным деяниям, можно подразделить на несколько условных характерных, описывающих варианты, когда:

- информация о мотивах, способах совершения преступления, субъекте преступного деяния отсутствует;
- установлены мотив и способ совершения преступления, но личность преступника неизвестна (наиболее распространенный случай).

³⁸⁷ Косарев С. Ю. История и теория криминалистических методик расследования преступлений. Указ. соч. С. 309.

– известны мотив, способ совершения преступления, личность преступника и другие обстоятельства³⁸⁸.

Для наиболее распространенных случаев осуществляется, например, следующий алгоритм действий:

- анализ поступивших материалов доследственной проверки на предмет их полноты и соответствия требованиям УПК РФ;
- возбуждение уголовного дела;
- формирование плана расследования;
- допрос заявителя и потенциальных свидетелей (при наличии);
- допрос специалиста или эксперта, проводивших исследования;
- получение информации о соединениях между абонентами и (или) абонентскими устройствами (при необходимости);
- проведение комплекса оперативно-розыскных мероприятий по установлению причин совершения преступления, выявления лиц, виновных в его совершении, обнаружению следов преступного деяния, вещественных и цифровых доказательств;
- производство выемки и осмотра технических средств, электронных носителей информации, средств защиты информации, программного обеспечения, предметов, материалов и документов;
- допрос ответственных лиц за технологические операции и обеспечение информационной безопасности и защиты информации (в организации);
- консультации у специалиста;
- при установлении подозреваемого – принятие мер по его задержанию, личный обыск, обыск по месту работы или жительства подозреваемого, допрос подозреваемого;
- назначение судебной компьютерно-технической экспертизы и пр.³⁸⁹.

С точки зрения уголовно-процессуального законодательства, поиск, фиксация и изъятие цифровых следов совершения преступления в сфере компьютерной информации осуществляется в рамках трех основных следственных действий – следственного осмотра, обыска и выемки, при этом следует понимать, что компьютерную информацию нельзя изъять, ее можно только скопировать,

³⁸⁸ Олиндер Н. В. Следственные действия на первоначальном этапе расследования преступлений, совершенных с использованием электронных платежных средств и систем // Юридический вестник Самарского государственного университета. 2015. Т. 1. № 4. С. 88.

³⁸⁹ Криминалистика : учебник / под ред. Л. В. Бертовского. М. : РГ-Пресс, 2018. С. 939.

заблокировать, модифицировать либо уничтожить³⁹⁰. В соответствии со ст. 183 УПК РФ выемка производится лишь при необходимости изъятия определенных предметов и документов, имеющих значение для уголовного дела, и в случае, если точно известно, где и у кого они находятся, по этой причине выемка по рассматриваемым деяниям производится редко. В случае возбуждения уголовного дела следователь обязан организовать и реализовать комплекс действий, направленных на установление обстоятельств совершенного противоправного деяния, разработать план совместных следственных действий и оперативно-розыскных мероприятий, в котором необходимо определить конкретные сроки их выполнения, а также изложить и обосновать проверяемые версии, выдвинутые на основании собранных фактических данных.

Следователю необходимо признать и допросить в установленном процессуальном порядке в качестве потерпевшего лицо, в отношении которого были совершены преступные действия, а также произвести его допрос с целью получения первичных сведений, имеющих доказательственное значение.

В числе первоначальных следственных действий необходимо осуществить осмотр технических средств, используемых потерпевшим, с обязательной фиксацией хода и результатов следственного осмотра. При этом по возможности следует зафиксировать и изъять цифровую информацию из устройства потерпевшего, включая сведения о сеансах доступа к различным сервисам, информационным ресурсам и пр. (IP-адреса, время доступа, используемые технические средства, параметры операционной системы, веб-браузера и пр.), историю изменения учетных данных и поступившие уведомления. При наличии достаточных оснований производится выемка предметов и документов, имеющих значение для уголовного дела, если данные материалы ранее не были приобщены к материалам доследственной проверки.

Целесообразно также проведение допроса в качестве свидетелей лиц, указанных потерпевшим, а также иных граждан, в отношении которых имеются сведения об их возможной осведомленности относительно обстоятельств преступления, либо о причастности к его совершению. Кроме того, при наличии данных о неправомерном списании денежных средств со счета потерпевшего, например, посредством удаленного использования его банковского приложения,

³⁹⁰ Особенности производства предварительного следствия по уголовным делам о преступлениях, связанных с неправомерным доступом к компьютерной информации, в том числе совершенных путем кибератак (сетевых атак) / под ред. Е. А. Пидусова : научно-практическое пособие. Воронеж : Воронежский институт МВД России, 2024. С. 23.

необходимо допросить представителей кредитной организации с целью установления факта несанкционированного доступа к охраняемой законом компьютерной информации, находящейся в ведении банка, и последствий, наступивших в результате совершенного деяния (уничтожение, блокирование, модификация, копирование информации и пр.).

В целях установления механизма совершения преступления направляются запросы в банковские учреждения о предоставлении сведений о попытках несанкционированного доступа к банковским сервисам, принадлежащим потерпевшему, на дату совершения преступления, а также информации об администрировании учетной записи. Дополнительно оформляются поручения о производстве отдельных следственных действий и оперативно-розыскных мероприятий, отчетов и сведений, полученных при сборе первоначального материала. Анализ поступивших данных из различных организаций служит основанием для составления дополнительного плана расследования. Данный план должен быть ориентирован на установление лиц, причастных к совершению преступного деяния, с учетом первоначальных и вновь выдвинутых следственных версий, основанных на способе, времени и месте совершения преступления.

Следует также истребовать у операторов связи и интернет-провайдеров сведения о владельцах IP-адресов, с которых осуществлялось неправомерное действие, а также данные об изменении регистрационных параметров учетных записей потерпевшего. В случае установления, что указанный IP-адрес принадлежит иностранному провайдеру, подготавливается и направляется международное поручение о правовой помощи в компетентные органы соответствующего иностранного государства.

При установлении персональных данных лиц, на которых зарегистрированы абонентские номера, банковские карты, почтовые адреса или аккаунты, а также при идентификации субъекта, пользовавшегося определенным IP-адресом, оформляется поручение в орган дознания на проведение проверки в отношении установленного лица, включая сбор дополнительных сведений, необходимых для организации обыска по месту жительства, проведения оперативно-розыскных мероприятий, направленных на получение доказательств его причастности к расследуемому и иным преступлениям. Необходимо также наладить взаимодействие с оперативными подразделениями³⁹¹, организовать и провести

³⁹¹ Подольный Н. А. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). С. 116.

обыск по месту проживания установленного субъекта, осуществить его допрос по факту возможного участия в преступлении. При наличии оснований принимается решение о задержании указанного лица и его доставлении к месту расследования.

В случае изъятия предметов и документов, обладающих признаками вещественных доказательств, необходимо произвести их осмотр и назначить соответствующие экспертизы. По мере необходимости следователь организует и проводит иные следственные действия, обусловленные логикой предварительного расследования, включая направление дополнительных запросов в банковские учреждения, представительства социальных сетей, а также в иные регулирующие и надзорные органы. Одновременно подготавливаются представления об устранении причин и условий, способствующих совершению преступления, а также о блокировании ресурсов, использованных в преступной деятельности.

Несмотря на то, что на первоначальном этапе расследования преступлений в сфере компьютерной информации арсенал возможных следственных действий достаточно велик, чаще всего он сводится к осмотру³⁹².

Осмотр места происшествия, местности, жилища, иного помещения, предметов или документов производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела. Осмотр технических средств обычно приводит к необходимости его изъятия для последующего экспертного исследования и (или) приобщения к делу в качестве вещественного доказательства. Кроме того, осмотр предметов может быть отдельным следственным действием или являться составной частью иных (обыска, выемки, проверки показаний на месте и пр.).

Осмотр осуществляется с участием не менее двух понятых, за исключением случаев, предусмотренных ч. 1.1 ст. 170 УПК РФ, когда следователь вправе отказаться от их участия, зафиксировав ход и результаты следственного действия с использованием средств фотофиксации и видеосъемки. В случае невозможности проведения осмотра на месте, технические средства изымаются с соблюдением требований УПК РФ и иных рекомендаций. При этом следователь должен убедиться, что устройства выключены. Данное следственное действие может касаться как оборудования, принадлежащего заявителю, так и технического средства, находящегося во владении подозреваемого. Его целью является выявление данных, относящихся к предмету проверки. Привлечение специалиста при этом необходимо для обнаружения наиболее значимых файлов – текстов, изображений и

³⁹² Мещеряков В. А., Трухачев В. В. Формирование доказательств на основе электронной цифровой информации // Вестник Воронежского института МВД России. 2012. № 2. С. 108.

иных цифровых данных.

Проведение экспертизы не требуется, если задачей является только обнаружение информации без ее исследования, что, к примеру, может быть вполне достигну встроенными в операционную систему инструментами. Результаты оформляются протоколами осмотра места происшествия или осмотра предметов и документов.

Целью осмотра места происшествия по рассматриваемым преступлениям, как правило, является установление конкретного технического средства и компьютерной информации, которая может выступать в качестве предмета либо орудия совершения преступления и нести в себе следы преступной деятельности³⁹³. Объектами осмотров чаще всего являются следующие технические средства: компьютеры (стационарные, настольные, одноплатные и портативные (неттопы, планшеты и пр.), рабочие станции, моноблоки, тонкие клиенты³⁹⁴); мобильные средства связи; электронные носители информации; серверное оборудование; видеорегистраторы и камеры видеонаблюдения; IoT-устройства или датчики; портативные устройства навигации; цифровые фотоаппараты и часы; платежные системы; терминалы оплаты; банкоматы и пр.

Осмотр помещений, принадлежащих организации, осуществляется в присутствии представителя административного персонала, в случае невозможности участия представителя организации при осмотре делается соответствующая запись в протоколе.

В соответствии с общим алгоритмом действий при осмотре технических средств целесообразно:

- провести его внешний осмотр;
- проверить наличие сетевых проводных и беспроводных подключений;
- осмотреть компьютерную информацию, отражающую сведения о текущих исполняемых процессах, планировщиках задач и сервисах операционной системы, сетевом трафике и виртуальных конечных точках сетевой карты (портах);
- осуществить поиск и осмотр электронных файлов, программного обеспечения (в том числе работающего под централизованной (групповой) политикой в организации), журналов событий в системе, средств защиты

³⁹³ Сысенко А. Р. Особенности осмотра места происшествия при расследовании компьютерных преступлений // Закон и право. 2020. № 12. С. 217.

³⁹⁴ ГОСТ Р 71201–2024. Персональные электронно-вычислительные машины. Типы, основные параметры, общие технические требования; дата введения: 01 июня 2024 г. М. : Российский институт стандартизации, 2024. С. 2.

информации и пр.;

- создать дампы содержимого оперативной памяти (для случая ранее включенного технического средства) и носителя информации, а также облачных хранилищ (при наличии доступа к ним) с задействованием специалиста;
- в случае изъятия отсоединить кабели и внешние устройства от технического средства;
- составить протокол следственного действия и упаковать изъятые предметы.

Стоит отметить, что осмотр системы, состоящей из нескольких технических средств, осложняется необходимостью исследования не только рабочих станций, но и серверного оборудования (почтовые серверы, «VPN» и (прокси)-серверы, серверы контроллеров доменов) и обеспечивающих их эксплуатацию сетевых устройств (маршрутизаторов, коммутаторов и пр.).

В случае невозможности изъятия средств вычислительной техники или возникшей проблемы клонирования содержимого носителей информации ввиду их большого размера, либо невозможности физического разделения составных элементов, возможно частичное копирование файлов, имеющих значение для расследования уголовного дела. Если по обстоятельствам дела необходимо производство судебной экспертизы системы, состоящей из нескольких технических средств, изъятию подлежат объекты, включающие в себя аппаратное и программное обеспечение, а также компьютерную информацию.

При осмотре необходимо выделять действия поэтапно. Так, в ходе подготовительного этапа при осмотре места происшествия, например, у руководителя организации, а также лица, отвечающего за обслуживание и использование технических средств, либо иного сотрудника предприятия следует получить объяснение, выяснить обстоятельства, связанные с исследуемым помещением, определить местоположение технических средств, информационных систем или программного обеспечения, а также учетные данные, обеспечивающие беспрепятственный к ним доступ. При этом в состав следственно-оперативной группы в зависимости от конкретной следственной ситуации помимо следователя могут входить: специалист-криминалист, знающий особенности работы со следами по преступлениям данной категории; сотрудник регионального центра защиты информации (при обработке на месте происшествия конфиденциальной компьютерной информации, специальных средств защиты информации от несанкционированного доступа и (или) технических средств негласного получения (уничтожения, блокирования) компьютерной информации; специалист по сетевым

технологиям (в случае наличия периферийного оборудования удаленного доступа или локальной компьютерной сети); специалист по системам электросвязи (при использовании для дистанционной передачи данных каналов электросвязи); оперативные сотрудники (например, отдела Бюро специальных технических мероприятий МВД России); инспектор отдела вневедомственной охраны Росгвардии (в случае когда электронная вычислительная машина (или место происшествия в целом) является охраняемым объектом). При необходимости в состав следственно-оперативной группы могут быть включены незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электронщики, программисты, аналитики, тестировщики, бухгалтеры, специалисты по спутниковым системам связи, операторы компьютерных систем и сетей электросвязи и др.).

Установление связи между преступлением и осматриваемым местом происшествия возможно с использованием специальных знаний и с применением технико-криминалистических средств³⁹⁵. При предположении, что при осмотре может быть обнаружена переписка лиц в электронной почте и мессенджерах необходимо заблаговременно подготовить: накопитель достаточного объема памяти, например, внешний жесткий диск с возможностью оперативной записи на него образа (дампа) оперативной памяти и соответствующее программное технико-криминалистическое средство, например «РС-3000», предназначенное для выгрузки и восстановления данных с электронных носителей информации, «Dumplt», «MKScout» или др.) или аналоги; привод для записи информации на оптические носители информации и несколько носителей для возможного копирования информации с обнаруженного в ходе следственного действия технического средства или облачного хранилища, доступ к которому может быть осуществлен при проведении следственного действия³⁹⁶. По прибытии следственно-оперативной группы на место происшествия в первую очередь рекомендуется зафиксировать визуально сложившуюся на месте происшествия обстановку путем фотографирования, а также составления протокола. Вместе с тем специалисту в данной отрасли знаний предлагается выполнить мероприятия, направленные на недопущение воздействия на имеющуюся информацию.

³⁹⁵ Россинская Е. Р. Избранное. Указ. соч. С. 578.

³⁹⁶ Сбор и анализ цифровых следов преступления : практическое пособие / под ред. С. В. Петраков. СПб. : Санкт-Петербургская академия Следственного комитета Российской Федерации, 2023. С. 6.

Вся обнаруженная в ходе осмотра криминалистически значимая компьютерная информация аккумулируется и распечатывается на бумаге и (или) копируется на носители информации, которые прилагаются к протоколу следственного действия. На основании всех собранных сведений формируется хронологическая последовательность событий, связанных с преступлением в сфере компьютерной информации, например, составляется схема воздействия вредоносной атаки или вероятные схемы обхода правил эксплуатации технических средств, информационно-телекоммуникационных сетей, программного обеспечения и пр.

На подготовительном этапе осмотра компьютера необходимо провести информирование участников о принятии мер обеспечения сохранности информации. В ходе рабочего этапа осмотра указываются сведения о техническом средстве, конфигурация его системы и параметры оборудования, после чего осматривается и фиксируется содержимое экрана и протекающие на момент осмотра процессы, касаемые функционирования программного обеспечения (что особенно важно по делам, связанным с созданием, распространением и использованием вредоносного программного обеспечения³⁹⁷). При этом проводится не просто описание увиденного на экране, но и осуществляется открытие и осмотр диспетчера задач (инструмента для управления запущенными процессами и мониторинга системных ресурсов), каталогов, файлов, программ, в частности, браузеров, и иной информации на компьютерном устройстве. Если следствие интересуется конкретный документ, возможно с известным или предполагаемым именем, производится его поиск по ключевым словам. Затем внимательно описываются все реквизиты и содержание документов, указывается их расположение. Отдельное внимание необходимо уделить носителям информации (в том числе облачным хранилищам) и сетевой карте устройства, поскольку именно на носителе данных хранится информация об используемом программном обеспечении, а сетевая карта обеспечивает ее идентификацию клиентов интернет-провайдеров по MAC-адресам. Таким образом, в ходе осмотра в обязательном порядке необходимо установить IP-адрес (для идентификации технического средства в сети) и MAC-идентификатор устройства.

На рабочей стадии осмотра фиксируется вид неправомерного деяния, например, уничтожение, блокирование, модификация, копирование информации, нарушение правил эксплуатации или функционирования технических средств,

³⁹⁷ Менжега М. М. Методика расследования создания и использования вредоносных программ для ЭВМ. М. : Юрлитинформ, 2009. С. 116.

информационно-телекоммуникационных сетей или сетей связи, определяется информация, которая подверглась модификации вредоносным программным обеспечением и пр. Для этого с помощью специалиста анализируется процесс эксплуатации программ, содержимое файлов и баз данных.

Важно установить, не содержится ли на компьютере информация, которая может способствовать более плодотворному и целенаправленному осмотру (учетные данные, схемы размещения технических средств, базы данных и прочая информация, имеющая доказательственное значение). Для этого специалистом проводится экспресс-анализ компьютерной информации путем просмотра содержимого носителей информации. Если выясняется, что имел место неправомерный доступ в помещение, то необходимо выявить следы пальцев рук, микрочастиц на клавиатуре и корпусе средства вычислительной техники, мониторе и периферийном оборудовании. Целесообразно также просмотреть результаты работы средств защиты информации, программ контроля доступа к техническим средствам, системам протоколирования действий и пр.

На заключительном этапе следственного осмотра принимается решение об изъятии компьютера, при этом все разъемы устройства опечатываются в соответствии с требованиями ст. 82 УПК РФ.

При осмотре компьютера необходимо зафиксировать визуальную информацию с применением правил криминалистического фотографирования и (или) составления структурной схемы соединений входящих в него устройств. В ходе детального осмотра следует отразить выявленное (запущенное) на технических средствах программное обеспечение, зафиксировать съемкой наличие всех внешних подключений (кабелей). Целесообразно проверить буфер обмена компьютера в целях выявления хранящейся в оперативном запоминающем устройстве криминалистически значимой информации.

В протоколе осмотра компьютера фиксируют³⁹⁸:

- его тип (назначение), марку (название), конфигурацию, цвет и заводской номер (серийный, инвентарный или учетный номер изделия);
- вид (назначение), цвет и другие индивидуальные признаки соединительных и электропитающих проводов;
- состояние на момент осмотра (выключено или включено);
- техническое состояние (целостность корпуса, комплектность, наличие и

³⁹⁸ Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, З. И. Харисова, В. Р. Гайнельзянова и др. Уфа : Уфимский ЮИ МВД России, 2023. С. 41.

работоспособность необходимых блоков, узлов, деталей и правильность их соединения между собой), тип и состояние используемых электронных носителей информации;

- наличие и техническую возможность подключения к компьютеру периферийного оборудования и (или) самого компьютера к такому оборудованию либо к каналу связи;

- имеющиеся повреждения, конструктивные изменения в архитектуре компьютера, ее отдельных деталей (частей, блоков), особенно тех, которые могли возникнуть в результате преступления, а равно могли спровоцировать возникновение происшествия;

- следы преступной деятельности (следы орудий взлома корпуса компьютера, проникновения внутрь корпуса, пальцев рук, несанкционированного подключения к компьютеру сторонних устройств или компонентов и др.);

- расположение компьютера в пространстве относительно периферийного оборудования и других технических устройств;

- категорию обрабатываемой информации (общего пользования, конфиденциальная и др.);

- наличие или отсутствие средств защиты информации.

Фотографирование и маркирование элементов компьютерной системы необходимо, в частности, для правильной сборки и подключения всех ее элементов в условиях лаборатории. При фотографировании следует подготовить также снимки передней и задней частей системы крупным планом. Фотографирование и маркирование элементов изымаемого компьютера также дает возможность воссоздания состояния технического средства в условиях экспертного исследования.

Следователь должен иметь в виду, что для исследования больших по объему массивов данных или сложных по топологии компьютерных сетей требуется значительное время. В случае невозможности изъятия средства вычислительной техники (например, если компьютер является сервером или рабочей станцией компьютерной сети) после осмотра целесообразно заблокировать соответствующее помещение, отключить источники электропитания. При изъятии носителей информации нужно помнить, что они должны перемещаться в пространстве и храниться в специальных опломбированных и экранированных контейнерах либо в алюминиевых футлярах, исключающих разрушающее воздействие электромагнитных полей и направленных излучений.

Одним из наиболее распространенных объектов осмотра по делам рассматриваемой категории выступает мобильный телефон, с которого зачастую осуществляется обмен данными о месте или способе совершения преступления. Сложность его осмотра в ряде случаев обусловлена, во-первых, отсутствием знаний, необходимых для описания его программного обеспечения (операционной системы устройства, установленных и запущенных на устройстве программных процессов, в частности, скрытых), во-вторых, отсутствием навыков и умений извлечения криминалистически значимой информации с использованием программных технико-криминалистических средств (или из-за их отсутствия), дополнительные трудности при осмотре телефона возникают в связи с необходимостью определения процессуального порядка доступа к тем или иным сведениям, поскольку в ряде случаев при помощи телефона сотрудники получают доступ к сведениям, расположенным на удаленном сервере, что не позволяет именовать такое следственное действие осмотром предмета. Кроме того, в отдельных случаях может потребоваться получение судебного решения в связи с ограничением тайны связи³⁹⁹.

Фотофиксации подлежит сама упаковка, внешний вид устройства, его повреждений (при наличии), всех разъемов, марка, модель, абонентский номер и IMEI-код телефона, SIM-карт, карт памяти, батареи (при съемном варианте аккумулятора), чехла (при наличии).

Произвести осмотр мобильного средства связи наиболее эффективно позволяют специальные программные технико-криминалистические средства, которые могут обходить функции блокировки устройств, извлекать из него криминалистически значимую информацию, адаптировать и систематизировать извлеченную информацию в структурированный отчет⁴⁰⁰. Так, например, программное обеспечение «Мобильный Криминалист Эксперт Плюс» поддерживает извлечение информации из широкого ряда цифровых источников, среди которых: мобильные устройства, облачные сервисы, дроны и компьютеры под управлением операционных систем «Windows», «macOS» и «OpenGNU» или

³⁹⁹ Земцова С. И., Суров О. А., Галушин П. В. Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий. М. : Юрлитинформ, 2019. С. 50.

⁴⁰⁰ Свидетельство о государственной регистрации программы для ЭВМ № 2024661082 Российская Федерация. MACDEV V.1.0 [Mobile and Computer Devices Inspection] – производство осмотра компьютерной техники и мобильных устройств при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий : № 2024619987 : заявл. 06.05.2024 : опубл. 15.05.2024.

«Linux»; физические образы жестких дисков в форматах «E01», «Ex01», «RAW», «DMG», «ISO»; логические образы носителей информации в форматах «L01», «Lx01», «AD1», «ZIP», «7Z», «RAR», «TAR»; файлы виртуальной машины «VitrualBox», «VMware»; диски виртуальной машины «VDI», «VHD», «VMDK»; резервные копии «Time Machine» для «macOS». Стоит отметить, что извлеченная информация защищается одним из выбранных хеш-алгоритмов в соответствии с ГОСТ Р 34.11–12⁴⁰¹, «MD5», «SHA-2» и т. п., которые подтверждают, что данные не были изменены после извлечения из технических средств. Помимо модуля извлечения данных в программу встроены аналитические инструменты, которые позволяют производить анализ полученной информации по различным параметрам (например, находить связи между контактами или просматривать все события устройства в хронологическом порядке). Встроенный механизм поиска позволяет искать данные по различным критериям, в том числе по списку ключевых слов. Таким образом, использование программных технико-криминалистических средств с участием специалиста позволяет в рамках осмотра предметов получить адаптированную и удобную для восприятия информацию, содержащую сведения о технических средствах.

Следует отметить, что алгоритм действий приглашенного специалиста и следователя при внешнем осмотре телефона обусловлен состоянием телефона. Так, если на момент осмотра он выключен, то включать его не рекомендуется, так как при включении при наличии возможности передачи данных возможно дистанционное управление устройством или удаление криминалистически значимой информации и (или) полная блокировка его работы⁴⁰².

Не останавливаясь на особенностях каждого из этапов осмотра мобильных средств связи (поскольку в целом они идентичны этапам осмотра компьютера) стоит отметить, что в случае нахождения телефона во включенном состоянии можно руководствоваться следующим алгоритмом действий:

- перевести мобильный телефон в «авиарежим» для недопущения изменения текущего состояния устройства и удаленного стирания информации с него;
- подключить устройство к сети питания (по возможности);

⁴⁰¹ ГОСТ Р 34.11–2012 Информационная технология. Криптографическая защита информации. Функция хэширования; дата введения: 01 января 2013 г. М.: Стандартинформ, 2013. С. 6.

⁴⁰² Харисова З. И. Изъятие криминалистически значимой информации с мобильных средств связи в рамках расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Вестник Института права Башкирского государственного университета. 2023. № 1 (17). С. 59.

- установить (со слов задержанного либо иным способом) и внести в протокол пароль доступа к устройству;
- провести в присутствии понятых сброс паролевой защиты для обеспечения дальнейшего свободного входа в мобильное устройство;
- проверить наличие на устройстве дополнительных «рабочих пространств», предварительно определив расположение в них мессенджеров и прочих сервисов;
- осуществить проверку сервисов и мессенджеров, функционирующих на момент осмотра, отключить в настройках функцию автоматического удаления сообщений (при обнаружении защищенных паролем сервисов и мессенджеров установить пароль и внести его в протокол);
- зафиксировать переписку и другую значимую информацию путем создания снимков экрана или фотосъемки изображений на экране осматриваемого устройства;
- проверить историю установленных на устройстве браузеров в целях определения посещаемых веб-ресурсов;
- при выявлении запрещенных веб-ресурсов установить и зафиксировать в протоколе пользовательские учетные данные для доступа к ним;
- осуществить проверку устройств на наличие программного обеспечения, способного отслеживать действия пользователя, в случае обнаружения принять меры для его отключения;
- осмотреть перечень программного обеспечения, фиксирующего заметки пользователя, календарей, ежедневников, файлов и документов на наличие в них учетных данных, а также другой значимой информации;
- проверить хранилище графических изображений на предмет наличия фотоизображений, а также иной информации, способствующей изобличению преступника⁴⁰³.

При описании внешнего вида телефона в протоколе осмотра следует отразить: наименование, марку, размеры, цвет, конструкцию, материал, из которого изготовлено устройство; модель и ее характеристики; фоновый

⁴⁰³ Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров : методические рекомендации. М. : ЭКЦ МВД России, Следственный департамент МВД России, ГУНК МВД России, 2020. С. 17.

рисунок или иные особенности визуального отображения; имя владельца на дисплее; наличие повреждений. При проведении следственного действия следует отметить о возможностях установления:

- IMEI-кода устройства, путем набора на мобильном устройстве комбинации «*#06#»;

- абонентского номера, идентифицирующего элемент сети связи или подключенное к информационно-телекоммуникационной сети абонентское устройство с установленным в ней идентификационным модулем, путем набора комбинации клавиш, определенную оператором связи;

- информации о соединениях между абонентскими устройствами, например, путем создания личного кабинета пользователя, использования приложения от оператора связи, либо веб-версии личного кабинета абонента с целью извлечения детализации разговоров и обмена сообщениями (с письменного согласия владельца);

- данных об IP-адресе и MAC-идентификаторе, количестве слотов для SIM-карты, видах операторов, определенных устройством, и IMEI-кодах путем детального осмотра технического средства встроенными средствами операционной системы;

- сохраненных данных о беспроводных устройствах и подключениях (в разделе расширенных свойств имеются данные о MAC-адресе устройства, с которого происходила раздача и выделенный IP-адрес);

- данных об аккаунте и привязанных банковских картах, в том числе виртуальных электронных кошельках (в приложениях, мессенджерах).

Установленный IMEI-код сразу же в ходе осмотра можно проверить путем использования специальных сервисов (например на сайте <https://www.imei.info> и т. п.). Широкий спектр возможностей позволяет не только удостовериться в действительности IMEI-кода технического средства в отсутствие постороннего вмешательства в программное обеспечение, но и перепроверить в базах данных информацию об утере или его хищении. Полученная информация отражается в протоколе с описанием процедуры получения сведений.

Информация о соединениях между абонентами может быть получена в ходе как осмотра сотового телефона путем использования подключенного личного кабинета, так и направления запроса оператору связи. При направлении запроса следует требовать информацию о базовых станциях с указанием азимутов обслуживания абонента. Кроме того, возможно использование сайтов по предоставлению возможности установления координат базовых станций и

определения с помощью карт, размещенных в сети «Интернет», расположения абонента на местности. По окончании осмотра лицо, производящее следственное действие, подводит его итоги, представляет участникам изъятые объекты в упакованном виде, обозначает время и дату окончания следственного действия, устанавливает возникшие вопросы, замечания, ходатайства, жалобы по ходу, способу и организации проведения осмотра, знакомит с протоколом и результатами фиксации хода следственного действия, устанавливает замечания, ходатайства, заявления, жалобы к качеству и порядку составления протокола.

В рамках производства следственных действий, существенное значение имеют именно поиск, обнаружение, фиксация и изучение различных следов и вещественных доказательств, что позволяет осуществлять доказывание в целях установления обстоятельств в соответствии со ст. 73 УПК РФ. При этом эффективность поиска и сбора криминалистически значимых объектов довольно часто зависит от уровня использования следователем технических средств и информационно-телекоммуникационных технологий. Отличительной особенностью расследования преступлений в сфере компьютерной информации является то, что при проведении ряда следственных действий целесообразно применение программных технико-криминалистических средств, что, в свою очередь, требует привлечения специалиста. Указанные средства позволяют наиболее эффективно обнаружить, зафиксировать и предварительно исследовать цифровые следы, имеющие криминалистическое значение, одновременно способствуя выявлению способа совершения преступления.

Так, при производстве следственных действий при расследовании преступлений в сфере компьютерной информации важно соблюдать следующие правила⁴⁰⁴:

- обеспечить неизменность цифровых следов, хранящихся на осматриваемых технических средствах;
- для работы с цифровыми доказательствами привлекать специалиста;
- протоколировать все проводимые действия с носителями информации и цифровыми доказательствами, хранящимися на них, обеспечивая их защиту и доступность для дальнейшего исследования.

Нередки случаи, когда произвести сбор доказательств без использования специальных знаний либо участия в следственном действии специалиста не

⁴⁰⁴ Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex Russica (Русский закон). 2021. № 74 (9). С. 107.

представляется возможным, что обусловлено, например, применением современных технологий при совершении преступлений и различных технических средств. Так, в отсутствие специальных знаний в области сбора и анализа цифровых доказательств алгоритм действий следователя может привести к утрате или упущению цифровых следов преступного деяния, однако организация работы по расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий в целом, подразумевает соблюдать очередность криминалистических методов сбора и изъятия доказательств, не допуская утраты криминалистически значимой информации в ходе проведения следственных действий.

Особенностью преступлений, совершаемых с использованием электронных носителей информации, является то, что для их успешного раскрытия и расследования необходимо знание их специфики, понимание основных принципов их функционирования. При производстве следственных действий с привлечением специалиста в случае необходимости изъятия или копирования электронных носителей информации следует учитывать, что требуется гарантия сохранности⁴⁰⁵ в неизменном виде самого носителя как в ходе следственных действий, так и в процессе исследования в дальнейшем, а также достоверности содержащихся на нем сведений. УПК РФ закрепляет определенный порядок работы с указанными объектами. Изъятие электронных носителей информации осуществляется в рамках производства следственных действий с привлечением специалиста⁴⁰⁶. По ходатайству законного владельца либо лица, обладающего правом на содержащуюся на носителе информацию, с задействованием специалиста производится клонирование носителя информации на иные электронные носители, предоставленные соответствующими субъектами (владельцем оригинального носителя или обладателем содержащихся на них данных).

При копировании информации с электронных носителей информации применяются специализированные программные технико-криминалистические средства, что в обязательном порядке отражается в протоколе, с указанием методики использования программного обеспечения, перечня копируемых носителей информации и сведений о результатах клонирования. Скопированные

⁴⁰⁵ Тактика обнаружения, изъятия и осмотра средств электронных носителей информации и их подготовки для назначения судебных экспертиз : учебно-практическое пособие / О. А. Гребенюк, Д. Н. Жидков, Е. Н. Макарова, О. Л. Романова. Санкт-Петербург : Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2020. С. 16.

⁴⁰⁶ Гриненко А. В. Уголовно-процессуальный кодекс Российской Федерации : постатейный научно-практический комментарий. М. : Проспект, 2019. С. 448.

цифровые данные, содержащиеся на носителях информации в порядке, предусмотренном законом, и технически воспроизведенные без искажений, обладают таким же доказательственным значением, как и первоисточник, то есть сам электронный носитель информации, подвергшийся изъятию.

Согласно ст. 164.1 УПК РФ при производстве по уголовным делам, указанным в ч. 4.1 ст. 164 УПК РФ, изъятие электронных носителей информации не допускается, за исключением случаев, когда: вынесено постановление о назначении судебной экспертизы в отношении носителя; изъятие электронных носителей информации производится на основании судебного решения; на электронных носителях содержатся данные, полномочиями на хранение и использование которыми владелец носителя не обладает, либо они могут быть использованы для совершения новых преступлений, либо их копирование по заявлению специалиста может повлечь за собой утрату или изменение. Таким образом, устанавливаются порядок изъятия электронных носителей информации, а также копирования с него информации, который распространяется в целом на все следственные действия, а в то же время ограничения в виде запрета на изъятие электронных носителей информации при производстве следственных действий по уголовным делам о преступлениях в сфере предпринимательской деятельности, за исключением ряда случаев, например, указанных в ч. 1 ст. 164.1 УПК РФ⁴⁰⁷. Стоит отметить, что согласно требованиям ч. 3 ст. 164 УПК РФ следователь в ходе производства следственного действия вправе осуществить «клонирование» носителей информации. Считается, что указанные дополнения в УПК РФ направлены на защиту субъектов предпринимательства от необоснованного изъятия электронных носителей информации, которое может привести к приостановке хозяйственной деятельности.

Осмотр электронных носителей информации, а равно и содержащейся на них компьютерной информации, может выступать как в качестве самостоятельного следственного действия, так и в качестве составного элемента иных следственных действий (например, при производстве обыска, выемки, осмотра места происшествия). Осмотр носителей информации проводят с участием специалиста, по принципу «от общего к частному», в протоколе при этом обязательно фиксируются следующие сведения: тип и вид электронного носителя информации (например, жесткий диск, USB-накопитель, карта памяти и т. п.); марка и модель (при наличии); параметры корпуса, заводской, инвентарный или иной

⁴⁰⁷ Ким А. В. Отдельные вопросы проведения осмотра и экспертизы электронных носителей информации // Юридические науки. 2019. № 1. С. 153.

идентификационный номер; наличие и особенности разъемов для подключения к электронному носителю информации; наличие систем защиты от несанкционированного доступа, копирования либо модификации информации; характеристики электронного носителя информации, в частности, серийный номер, метка тома, общий объем памяти, код или идентификатор (ID) носителя, а также иные сведения, позволяющие идентифицировать объект. Запрещается производить извлечение электронных носителей информации при включенной системе, извлекать или менять местами накопители. В случае работы компьютера необходимо скопировать файлы подкачки, сделать дампы оперативной памяти, зафиксировать содержимое веб-браузеров и корректно завершить работу операционной системы компьютера перед его упаковкой в целях изъятия. Дампы оперативной памяти сохраняются по усмотрению специалиста при наличии признаков присутствия в нем значимой информации.

Недопустимо извлекать электронные носители информации без выключения серверного оборудования, менять их местами. Целесообразно отразить в протоколе схему подключения оборудования или подсистем, входящих в систему хранения данных, а также их состояние функционирования. Копирование со значительных размеров носителей информации рекомендуется осуществлять без их непосредственного изъятия с привлечением администратора, обеспечивающего их эксплуатацию. Недопустимо упаковывать включенные устройства с SIM-картами без отключения связи. Кроме того, необходимо избегать оставления электронных носителей информации в разъемах технических средств, при их осмотре использовать блокировку записи, устанавливая режим исследования «только для чтения»⁴⁰⁸.

В связи с повсеместной цифровизацией и вводом в эксплуатацию различных технологий обработки и передачи информации, расширением использования технических средств, развитием рынка цифровых услуг, интеллектуальной обработки данных возникают новые виды преступлений, которые часто требуют от следователя как применения специальных знаний, так и профессиональных умений грамотного формулирования вопросов для разрешения экспертом. Хорошо организованные преступные группы и сообщества для достижения корыстных целей активно и высокопрофессионально применяют в своей деятельности новые методы, подходы, специальные программно-аппаратные

⁴⁰⁸ Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, З. И. Харисова, В. Р. Гайнельзянова. М. : ГУРЛС МВД России, 2024. С. 22.

средства, системы удаленного доступа и криптографического шифрования, высокотехнологичную технику, а нередко и интеллектуальные комплексы принятия решений⁴⁰⁹.

Подобно осмотру места происшествия, подготовка к обыску должна включать, в соответствии с требованиями ч. 2 ст. 164.1 УПК РФ, предварительный поиск специалиста, обладающего специальными знаниями в сфере информационно-телекоммуникационных технологий, с последующим совместным составлением плана проведения следственного действия. Разработка плана обыска требует максимального сбора исходной информации, включая сведения о месте предстоящего следственного действия, технических средств, находящихся на месте обыска, о поведенческих характеристиках подозреваемого, а также об используемых им средствах вычислительной техники. Значимую для планирования и организации обыска информацию можно получить посредством проведения оперативно-розыскных мероприятий, а также анализа статистических данных о сетевых подключениях, предоставленных поставщиком услуг доступа к сети «Интернет» и (или) оператором связи⁴¹⁰. Традиционно, в рамках проведения обыска целесообразно предложить добровольно выдать технические средства и носители информации, использовавшиеся для преступных целей.

Все технические средства и сопутствующие электронные носители информации, а также иные предметы, изъятые в ходе обыска, должны быть упакованы с соблюдением требований, исключающих возможность их физического повреждения, утраты цифровых следов или удаленного доступа к этим устройствам. Все изъятые предметы, а также содержащиеся на них цифровые следы, подлежат последующему криминалистическому исследованию. До назначения судебной экспертизы допустимо проведение предварительного анализа, осуществляемого в рамках осмотра предметов с участием специалиста и с использованием программных технико-криминалистических средств.

Обыск по преступлениям в сфере компьютерной информации может начинаться с личного обыска лица, в отношении которого проводится следственное действие. В ходе данного этапа изымаются все технические средства и потенциальные носители информации.

⁴⁰⁹ Системная модель интеллектуальной предметно-ориентированной профайлинг-системы / В. В. Антонов, З. И. Харисова, З. Р. Мансурова [и др.] // Онтология проектирования. 2020. Т. 10. № 3. С. 338.

⁴¹⁰ Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях. Указ. соч. С. 112.

Процесс обыска разделяют на четыре стадии – подготовительная, обзорная, детальная, стадия фиксации. На подготовительной стадии необходимо решить организационные вопросы, а также получить информацию об условиях и обстановке места, где предстоит произвести обыск. Обыск производится обычно в местах нахождения технических средств: непосредственного их использования с целью осуществления неправомерного доступа к компьютерной информации или, например, создания, использования или распространения вредоносного программного обеспечения, а также хранения добытой при помощи него информации из других технических средств, информационных систем или информационно-телекоммуникационных сетей на носителе информации и пр.

В рамках обзорной стадии необходимо осмотреть помещение и технические средства, не останавливаясь на общих положениях обыска помещений, стоит подробнее рассмотреть обыск непосредственно технических средств. Следовательно необходимо при этом выяснить состояние, количество и расположение средств, подлежащих обыску, наличие телекоммуникационных подключений. Стоит особое внимание уделить объединенным в локальную сеть техническим средствам, которые встречаются как по месту проведения обыска в организациях, так и по месту проживания подозреваемого (как правило, это объединенные в локальную сеть средства в виде домашних компьютеров, мобильных средств связи, мультимедийных и периферийных устройств, IoT-датчиков и пр.).

Целесообразно определить месторасположение наиболее вероятного нахождения криминалистически значимой информации в технических средствах для выявления способа и места начала обыска, установить характер исполняемого программного обеспечения и процессов, при необходимости обеспечивая завершение их функционирования.

На стадии детального обыска необходимо определить способ совершения неправомерного деяния, выявить цифровые доказательства, зафиксировав результаты обыска.

На заключительном этапе следователь с помощью специалиста определяет объекты, подлежащие изъятию (выемке) с соблюдением правил их упаковки и транспортировки.

При проведении обыска и последующем изъятии технических средств, в целях фиксации следов преступной деятельности, необходимо:

- отключить компьютер от сети передачи данных, мобильное устройство перевести в «авиарежим»;
- зафиксировать и (или) снять код блокировки (при наличии);

- произвести с задействованием специалиста (с применением программных технико-криминалистических средств) снятие электронных образов хранящейся на носителе информации;
- зафиксировать имеющиеся на устройстве учетные данные и сведения о программном обеспечении либо интернет-сервисах, посредством которых, например, происходит активация либо пересылка оповещений для доступа к информации пр.;
- зафиксировать IP-адреса и лог-файлы соединений, используемых для управления устройством, включая подключение к облачным хранилищам или управление техническими средствами посредством программного обеспечения для удаленного доступа, MAC-идентификатор сетевой карты (зафиксировать IMEI-идентификаторы мобильных устройств, IMSI-коды SIM-карт, находящихся внутри них);
- произвести изъятие всех средств вычислительной техники, электронных носителей информации и прочих предметов.

Во многом по схожим с обыском правилам осуществляется выемка. Для случая нарушения правил эксплуатации средства вычислительной техники или информационно-телекоммуникационной сети процесс выемки сопровождается изъятием документов, необходимых для установления факта нарушения, в том числе: документация от производителя технического средства; локальные акты, регулирующие порядок работы с техническим средством и информационно-телекоммуникационной сетью, а также журналы учета их функционирования и технического обслуживания; материалы проверки, касающейся выявленных нарушений; приказы о назначении лиц, ответственных за эксплуатацию технических средств, информационных систем, информационно-телекоммуникационных сетей, программного обеспечения и пр.; должностные инструкции сотрудников, включая лиц, допустивших нарушения.

При проведении допроса подозреваемых либо обвиняемых по уголовным делам, связанным с преступлениями в сфере компьютерной информации, выясняются способы и средства совершения преступного деяния, каналы получения сведений о способах реализации противоправных действий, уровень знаний в области информационно-телекоммуникационных технологий, а также цели, мотивов и причин совершения преступного деяния.

Допрос включает в себя стадии подготовки (предварительная стадия), непосредственно допроса, состоящего из стадии свободного рассказа и последующих уточняющих вопросов, а также заключительной части с

оформлением результатов допроса. При расследовании преступлений, совершаемых в сфере компьютерной информации, на этапе подготовки к допросу следователю необходимо: установить сведения, сформировав план допроса и обозначив круг лиц, подлежащих допросу; изучить личность допрашиваемых лиц; определить время, место и порядок вызова допрашиваемых лиц (что в целом не отличается от общих правил проведения допроса по иным категориям уголовных дел). Начинать допрос, безусловно, следует с очевидцев совершенного преступления, т. е. тех, кто непосредственно может свидетельствовать о неправомерном доступе к компьютерной информации, создании, использовании или распространении вредоносного программного обеспечения или нарушении правил эксплуатации технических средств, информационно-телекоммуникационных сетей и пр., либо о тех последствиях, которые возникли в результате этих действий. Подготовка к допросу подозреваемого или обвиняемого по рассматриваемым делам в ряде случаев требует привлечения специалиста, поскольку профессиональной компетенции следователя может быть недостаточно для всестороннего анализа ситуации.

В ходе допроса подозреваемого (обвиняемого) подлежат установлению:

- уровень его образования и профессиональной подготовки, наличие практических навыков работы со средствами вычислительной техники;
- место работы (учебы), занимаемая должность, выполняемые операции с компьютерной информацией, правомерность доступа к компьютерной информации, программному обеспечению, информационной системе, информационно-телекоммуникационной сети и сетевым ресурсам;
- сведения о имеющихся персональных учетных данных, закрепленных за ним на рабочем месте (учебы), о правилах их задействования и пр.

Особенности проведения допроса лиц, подозреваемых в нарушении правил эксплуатации средств хранения, обработки, передачи информации либо доступа к сетям передачи данных, заключаются в установлении:

- даты назначения на должность;
- уровня профессионального образования;
- наличия навыков обращения с техникой;
- фактов ознакомления с регламентом эксплуатации оборудования, формами документального закрепления такого ознакомления;
- проведения инструктажей, их периодичности, содержания, лиц, их осуществлявших, а также документов, подтверждающих этот факт;

- временных рамок и места совершения нарушения, продолжительности эксплуатации оборудования с отклонениями от регламента;

- характера и механизма допущенных нарушений (несоблюдение предписанных действий, отклонение от технологических процедур, совершение действий, не предусмотренных инструкциями);

- последствий нарушения (возникновение критических ситуаций, уничтожение, изменение или несанкционированное копирование информации, блокировка функционирования информационных систем или технических средств, нарушение стабильности функционирования объектов управления и связи и пр.).

В рамках проведения допросов свидетелей и потерпевших по уголовным делам, связанным с преступлениями в сфере компьютерной информации, подлежат выяснению следующие обстоятельства:

- особенности организации функционирования информационно-телекоммуникационной сети и обработки компьютерной информации до и в период реализации противоправных действий, в том числе порядок установления и контроля режимов доступа к данным;

- меры по обеспечению защиты информации;

- наличие регламента по распределению полномочий между субъектами, наделенными доступом к ресурсам информационной системы;

- порядок приобретения, внедрения и эксплуатации программного обеспечения, круг лиц, имевших к нему доступ, а также характер допущенных нарушений, установленных правилами эксплуатации программ, технических средств или информационно-телекоммуникационной сети;

- факт наличия подключения к информационно-телекоммуникационной сети на момент совершения преступления;

- перечень посещенных веб-ресурсов, представляющих интерес с точки зрения анализа преступной деятельности;

- используемые в процессе функционирования и эксплуатации информационные системы или технические средства, методы передачи данных, применяемые сетевые протоколы и информационно-телекоммуникационные технологии;

- признаки, указывающие на подготовку при совершении противоправного деяния, фактические обстоятельства посягательства (время, место, выявленные аномалии в функционировании программного обеспечения, технических средств или информационно-телекоммуникационной сети);

- сведения о действиях допрашиваемого и иных сотрудников организации по нейтрализации и ликвидации последствий совершенного посягательства;
- возможность наступления описанных последствий вследствие непредвиденных факторов, включая стихийные бедствия, техногенных аварий и иных обстоятельств;
- информация о предполагаемом субъекте преступления;
- круг лиц, которым могла быть доступна конфиденциальная информация, в том числе сведения о способах аутентификации в информационно-телекоммуникационной сети или программном обеспечении;
- объем причиненного ущерба, в том числе с учетом стоимости восстановительных мероприятий.

К следственным действиям, применяемым в ходе расследования преступлений в сфере компьютерной информации, относится также следственный эксперимент, который в ряде случаев занимает значимое место. Его основной целью выступает проверка возможности применения конкретных информационно-телекоммуникационных технологий, технических средств или программного обеспечения для реализации конкретного способа совершения преступного деяния, проверки возможности преодоления средств защиты информации и воспроизведения элементов механизма криминального события.

Учитывая характер производимых действий при проведении следственного эксперимента по преступлению, связанному с использованием информационных технологий, при необходимости анализа цифровых следов обязательным является участие специалиста, обладающего специальными знаниями в сфере компьютерной информации. Производство действий с применением технических средств может осуществляться как самим специалистом, так и непосредственно лицом, чьи действия подлежат проверке. Если эксперимент направлен на воспроизведение поведения подозреваемого, предпочтительно, чтобы он лично осуществлял демонстрацию действий в присутствии участников следственного мероприятия. Недопустимо использование оригинальных вещественных доказательств, изъятых в ходе расследования, электронных носителей информации и технических средств, поскольку это может повлечь изменение цифровых следов, хранящихся на них. В таких случаях необходимо применять функционально аналогичные технические средства, характеристики которых позволят достоверно смоделировать проверяемые обстоятельства⁴¹¹.

⁴¹¹ Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях. Указ. соч. С. 116.

Фиксация хода и результатов следственного эксперимента осуществляется с обязательным внесением соответствующих сведений в протокол. Дополнительно возможна регистрация эксперимента с использованием фото- и видеосъемки, средств протоколирования действий, записи экрана, сохранения лог-файлов и других технических способов документирования.

В рамках уголовного процесса могут быть проведены и иные следственные действия, направленные на получение сведений о соединениях между абонентами или их устройствами, а также контроль и запись переговоров. Эффективность данных мероприятий зависит от полноты сведений о применяемых средствах связи, которые часто оформлены на номинальных (подставных) лиц, функционируют анонимно или используют методы шифрования. Такие данные выявляются при производстве обыска, осмотра, допроса, выемки, проведении экспертиз и в рамках оперативно-розыскной деятельности. После сбора такой информации следователь систематизирует полученные сведения и передает их органу, осуществляющему реализацию указанных мероприятий. Результаты контроля и записи переговоров требуют привлечения специалиста для интерпретации зафиксированной лексики, профессионального сленга, анализа условий получения информации, объяснения роли тех или иных сведений по установлению местонахождения устройства.

Использование технических средств при совершении преступлений влечет за собой применение устройств, в состав которых, как правило, входит носитель информации. По этой причине особое значение при расследовании преступлений имеют компьютерные экспертизы электронных носителей информации. В современных условиях собирание цифровых следов наиболее эффективно можно осуществить только в процессе производства судебной компьютерно-технической экспертизы⁴¹². В составе судебных компьютерно-технических экспертиз выделяют следующие направления⁴¹³: аппаратно-компьютерная; программно-компьютерная; компьютерно-сетевая и информационно-компьютерная. Выделение этих подвидов экспертиз обуславливается характером объектов, которые представляются к анализу, и вопросами, решаемыми в рамках каждой конкретной экспертизы.

Аппаратно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием технической (аппаратной) части компьютерных средств. Как правило, эти вопросы носят диагностический характер. Программно-

⁴¹² Россинская Е. Р. Особенности оценки и использования в доказывании результатов судебных экспертиз в условиях цифровизации. Указ. соч. С. 6.

⁴¹³ Россинская Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии. Указ. соч. С. 35.

компьютерная экспертиза направлена на решение вопросов, связанных с исследованием программного обеспечения. В рамках указанной экспертизы исследуются процедуры, алгоритмы, принципы разработки программ, а также его использование, текущее состояние, структурные особенности, особенности их эксплуатации. Компьютерно-сетевая экспертиза обеспечивает исследование обстоятельств и фактов, связанных с применением информационно-телекоммуникационных сетей и сетевых технологий. Ключевым видом при расследовании преступлений в сфере компьютерной информации является информационно-компьютерная экспертиза, которая решает задачи, связанные с поиском, обнаружением, оценкой и анализом информации, содержащейся в компьютерной системе, в том числе на электронном носителе информации. Именно данный вид исследования позволяет обеспечить завершение процесса целостного формирования доказательственной базы в результате формулирования ответов на большинство вопросов, в той или иной степени связанных с цифровыми следами⁴¹⁴.

Среди технических средств объектами исследования могут выступить компьютеры и периферийные устройства, сетевые аппаратные средства, мобильные телефоны, встроенные системы на основе микропроцессорных контроллеров (иммобилайзеры, транспондеры и иные комплектующие технических средств (платы расширения, микросхемы и прочие запоминающие устройства и носители данных)). К программным средствам можно отнести системное (операционные системы) и вспомогательное программное обеспечение (утилиты), средства разработки и отладки программного обеспечения, прикладное программное обеспечение (текстовые и графические редакторы, системы управления базами данных, электронные таблицы и пр.), приложения специального назначения для решения задач в определенной области науки, техники или экономики, исходные тексты программного обеспечения, автоматизированные системы и иные программы, а также документация на них⁴¹⁵.

Цифровые следы, технические средства, информационные системы и программное обеспечение, как носители доказательственной криминалистически значимой информации, являются основными объектами теории цифровизации судебно-экспертной деятельности, входящей в состав теории информационно-

⁴¹⁴ Вещественные доказательства: информационные технологии процессуального доказывания / под ред. В. Я. Колдина. М. : Норма, 2002. С. 570.

⁴¹⁵ Справочник по подготовке, организации, назначению и производству судебных экспертиз в судебно-экспертных учреждениях Минюста России : справочник. М. : ФБУ РФЦСЭ при Министерстве юстиции Российской Федерации, 2024. С. 70.

компьютерного обеспечения криминалистической деятельности, в которой обоснована криминалистическая дефиниция цифровых следов, описаны их виды, а также способы собраний⁴¹⁶.

В настоящее время активно ведется разработка программного обеспечения для проведения компьютерных экспертиз в виде программных технико-криминалистических средств, например, «Belkasoft», «Мобильный криминалист», «Forensic Toolkit (FTK)», «Autopsy Digital Forensics», «EnCase Forensic» и пр. Однако в условиях реализации программ импортозамещения, а также недостаточного финансирования на приобретение программных продуктов важной задачей является использование доступных методов анализа цифровых устройств⁴¹⁷.

Для сбора доказательственной информации с различных типов цифровых устройств можно использовать следующую схему:

- идентификация технических средств и выявление потенциальных источников цифровых доказательств на нем (определение типа средства, фиксация его содержимого, запись серийного номера, модели и других данных);
- физическая изоляция устройства и контроль за обеспечением безопасности данных на техническом средстве, отключение устройства от сети для предотвращения к нему удаленного доступа, использование специальных контейнеров или экранирующих пакетов для защиты данных (пакеты Фарадея);
- клонирование данных с использованием специализированного программного обеспечения с применением блокировщиков записи для предотвращения изменения исходных данных, проверка целостности образа с помощью хеш-сумм;
- анализ цифровых доказательств с использованием программных технико-криминалистических средств;
- производство судебной компьютерно-технической экспертизы (при необходимости).

Рассматривая указанную категорию преступлений, следователь сталкивается с информацией, зафиксированной в электронной форме, экспертное исследование которой позволяет предоставить в распоряжение сотрудника сведения,

⁴¹⁶ Россинская Е. Р., А. И. Семикаленова Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. 2020. Т. 11. № 3. С. 753.

⁴¹⁷ Сбор и анализ цифровых следов преступления. Указ. соч. С. 22.

отражающие механизм совершенного преступления, дает возможность определить параметры технических средств, их отношение к обнаруженной информации и друг к другу, а также иные важные обстоятельства. При таких обстоятельствах на первоначальном этапе расследования актуальной задачей является определение уровня защищенности исследуемых информационных систем, общего алгоритма расследования (в зависимости от параметров сложившейся ситуации), от реализации которого, в частности, будет зависеть ход раскрытия и расследования преступного деяния.

Анализ уголовных дел и материалов следственной практики позволил выявить наиболее часто встречающиеся ошибочные действия при проведении следственных действий по преступлениям в сфере компьютерной информации:

- осуществление действий на осматриваемом устройстве, приводящее к модификации хранящейся на нем информации;
- нецелесообразное назначение судебной компьютерно-технической экспертизы при наличии возможности осмотра и выявления криминалистически значимой компьютерной информации непосредственно на месте происшествия совместно со специалистом (часто не предпринимаются какие-либо попытки осмотра лог-файлов и журналов протоколирования действий в системе, метаданных изображений, скрытых файлов и каталогов, редактора реестра в операционной системе и пр.);
- отсутствие подготовки к проведению допроса, либо непривлечение к нему специалиста, вследствие чего следственное действие проводится бессистемно, неструктурированно, соответственно применяемые следователем тактические приемы при любом раскладе являются неэффективными, при этом не устанавливаются технические особенности способа совершения преступления (обусловлено, как правило, недостаточным уровнем грамотности сотрудника в области информационных технологий и отсутствием способности выстраивания цепочек формируемых событий в различных технических средствах, информационных системах, программном обеспечении и пр.);
- формальное отношение к процедуре допроса, что довольно часто встречается в случаях, когда по преступлению выявлен, например, абонентский номер или банковский счет, оформленный на паспортные данные пользователя, проживающего в другом регионе, при этом направление поручений в районные отделы полиции по месту жительства владельца номера или счета часто не приводит к результату, поскольку допрос провести не представляется возможным ввиду отсутствия проживающего по месту жительства;

- неправильная упаковка и опечатывание технических средств и электронных носителей информации, направляемых на экспертизу, что влечет за собой опровержение в суде идентичности предъявленного на процессе объекта тому, которое находилось в момент изъятия;

- формирование технически неграмотных вопросов, которые дают допрашиваемому представление о недостаточной квалификации сотрудника в области информационных технологий и позволяют «уйти» от ответа;

- формирование узких границ проведения обыска;

- довольно часто размывается грань между процедурой получения объяснений как процессуального действия и допросом как следственного действия;

- формальное отношение к процессу получения объяснений от потерпевших, в частности, при проверке заявлений (сообщений) о преступлениях, что обусловлено отсутствием законодательной регламентации порядка получения объяснений и, как следствие, возникновением ситуаций нежелания или агрессивного отказа от дачи объяснений лица ввиду нормативного отсутствия ответственности за отказ от дачи объяснений, в то же время, тщательный подход при получении объяснений от потерпевшего нередко приводил к тому, что в суде они не принимались как полноценные доказательства, не в полной мере оценивались в совокупности с иными доказательствами, вызывали сомнения в достоверности данных ввиду отсутствовавшей угрозы наступления ответственности за дачу заведомо ложных объяснений;

- игнорирование наличия технических средств с возможностью удаленного хранения информации и синхронизации данных на сторонних серверах (облачные сервисы, распределенные реестры и пр.).

Отдельно стоит отметить то, что деятельность сотрудников правоохранительных органов на этапе доследственной проверки зачастую сводится к принятию процессуальных решений об отказе в возбуждении уголовного дела, что исключает дальнейшее проведение оперативно-розыскных мероприятий, позволяющих выявить имеющую значение для раскрытия преступления информацию, например, о принадлежности конкретному пользователю MAC-идентификатора или IP-адреса, абонентского номера, банковского счета или криптокошелька, используемых преступником для взаимодействия с потерпевшим.

Анализ процессуальных документов, формируемых по уголовным делам, связанным с преступлениями в сфере компьютерной информации, показал, что в протоколах осмотра места происшествия, обыска и выемки часто допускаются

ошибки, связанные с отсутствием информации об имеющейся по месту проведения следственного действия информационной инфраструктуре, в частности, не указывается вид реализованной телекоммуникационной сети, формат доступа к ней. В протоколах осмотра предметов часто отсутствует информация об установленной операционной системе осматриваемого технического средства.

В ряде случаев полученные в ходе расследования результаты не признавались судом в качестве допустимых ввиду отсутствия сведений о применяемых технико-криминалистических средствах при обнаружении компьютерной информации, при изъятии носителей информации с доказательственной информацией.

Кроме того, часто в материалах дела отсутствовали схемы топологии сети в организации, телекоммуникационных средств и узлов, что могло бы способствовать лучшему пониманию обстоятельств дела и выдвижению новых следственных версий.

Весьма важными являются проблемы поверхностного осмотра специалистом или исследования экспертом носителей информации, ввиду их высокой нагруженности и нехватки времени, а также подключения накопителей информации после проведения судебной компьютерно-технической экспертизы без использования программных технико-криминалистических средств, что может повлечь нарушение целостности содержимого электронного носителя информации. Несмотря на дискуссионность вопроса о необходимости проведения криминалистических экспертиз на месте происшествия (ситуационных или ситуалогических экспертиз)⁴¹⁸ можно предположить, что их вполне можно рассматривать как метод исследования в рамках разрешения диагностических задач по преступлениям в сфере компьютерной информации, что, например, вполне обоснованно, когда вещественные доказательства (серверное оборудование) не могут быть доставлены с места происшествия в криминалистическую лабораторию из-за громоздкости либо вследствие опасности искажения или порчи следов при транспортировке⁴¹⁹. Также это решает проблему невозможности клонирования распределенного хранилища данных большого объема.

Учесть все варианты способов совершения преступлений в сфере компьютерной информации, которые часто являются многоэтапными, либо

⁴¹⁸ Грановский Г. Л. Криминалистическая ситуационная экспертиза места происшествия // Теоретический семинар – криминалистические чтения : сборник материалов теоретического семинара. М. : ВНИИСЭ МЮ СССР, 1977. С. 5.

⁴¹⁹ Белкин Р. С. Курс криминалистики. Указ. соч. С. 20.

включающими комбинации нескольких способов (тактик, техник и подтехник) совершения преступного деяния с целью разработки частной методики его расследования, без использования программных технико-криминалистических средств практически невозможно.

Так, для примера можно привести число возможных комбинаций совершения преступлений в сфере компьютерной информации с учетом количества всех известных на текущее время техник (427 ед.) и подтехник (529 ед.) базы угроз безопасности информации «Mitre Att&ck».

При сочетании хотя бы двух техник число возможных комбинаций совершения преступлений составит более 90 тыс. вариаций, а при сочетании двух техник хотя бы с одной подтехникой превалирует миллион комбинаций. По этой причине целесообразно отдельное внимание уделять не только следственным ситуациям, но и формирующим их обстоятельствам. При этом, число вариантов этих обстоятельств при описании следственных ситуаций будет увеличиваться в геометрической прогрессии по мере увеличения учитываемых обстоятельств⁴²⁰.

На основе анализа взаимосвязей между алгоритмами расследования и следственными ситуациями можно сделать предположение, что типовая следственная ситуация обуславливает соответствующий ей типовой алгоритм расследования с выделением на каждом из этапов соответствующих ключевых признаков. Так, на этапе возбуждения уголовного дела возможно выявление ключевых признаков, входящих в материал проверки сообщения (заявления) о преступлении. В целях выявления дополнительных признаков для построения информационно-компьютерной модели преступления исследуемого вида необходимо рассмотрение соотношения следственных ситуаций и их особенностей с алгоритмами расследования, как основы для дальнейшего развития криминалистической методики расследования преступлений и формирования информационных систем, моделирующих поведение эксперта при выработке рекомендаций или решении проблем в определенной области, т. е. классической экспертной системы⁴²¹.

⁴²⁰ Герасимова Е. Ю. Следственные ситуации, возникающие на первоначальном и последующем этапах расследования создания, распространения и использования вредоносных компьютерных программ // Актуальные проблемы российского права. 2024. № 1 (158). С. 172.

⁴²¹ Принципы и алгоритмы искусственного интеллекта : монография / Э. А. Бабкин, О. Р. Козырев, И. В. Куркина. Н. Новгород : Нижегородский гос. техн. ун-т. 2006. С. 56.

ГЛАВА 4. ОРГАНИЗАЦИОННЫЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ АЛГОРИТМИЗАЦИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

4.1. Соотношение следственных ситуаций и алгоритмов расследования преступлений в сфере компьютерной информации

Проведенный анализ особенностей расследования преступлений в сфере компьютерной информации, в частности, организационно-тактических особенностей производства отдельных следственных действий, позволяет сделать вывод о том, что материалы проверки и следствия по каждому из составов преступного деяния, несмотря на ряд имеющихся общих составных элементов, довольно сильно отличаются как по количеству, так и по содержанию. При этом определяются отличительные признаки содержания элементов криминалистической характеристики по каждому из составов, что может свидетельствовать о том, что по каждому из рассматриваемых преступлений возможно сформировать методику его расследования (алгоритм)⁴²², например, в цифровом виде.

Методика расследования преступлений может условно представлять собой систему научно обоснованных закономерностей, отражающих особенности организации и деятельности по раскрытию, расследованию и предупреждению преступных посягательств. Указанные закономерности формируют содержание криминалистической характеристики преступлений и по своей сути могут выступить основой построения алгоритмов их расследования. Развитие криминалистической методики расследования преступлений осуществляется во взаимосвязи с иными направлениями криминалистических знаний, особенно в свете эволюции научного познания. За весь период становления криминалистической методики, как составной части криминалистики, появились существенные предпосылки для ее алгоритмизации и программирования, так, в числе отличительных признаков понятия «методика» криминалистами все чаще стал упоминаться ее программный характер⁴²³.

⁴²² Харисова З. И. Алгоритмы действий следователя (дознавателя) на стадии возбуждения уголовного дела о преступлениях в сфере компьютерной информации // Вестник Московского университета МВД России им. Кикотя. 2025. № 4. С. 147.

⁴²³ Корноухов В. Е., Богданов В. М., Закатов А. А. Основы общей теории криминалистики. Красноярск : Издательство Красноярского университета, 1993. С. 108; Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты : монография. М. : Лига Разум, 2000. С. 9.

Как известно, при разработке той или иной методики можно руководствоваться:

- типовыми способами совершения преступных деяний, выявленными на основе эмпирических данных о раскрытии конкретного вида преступлений;
- следовоспринимающими и слеодообразующими объектами, а также способами фиксации следов преступлений, изъятия, исследования и оценки их достоверности;
- способами идентификации круга лиц, в числе которых может находиться субъект преступного посягательства, а также свидетели;
- способами анализа криминалистически значимой информации, осмысление которой обеспечивает установление истины по уголовному делу;
- возможностями сочетания производства следственных действия с оперативно-розыскными мероприятиями в целях повышения эффективности их расследования;
- особенностями порядка фиксации и проверки криминалистически значимой доказательственной информации с акцентом на специфику расследуемой категории дел;
- апробированными ранее, а также потенциально возможными для применения в области расследования конкретных категорий преступлений специализированными научными знаниями⁴²⁴.

Одним из универсальных научных методов познания является моделирование, с помощью которого по выдвинутой ранее гипотезе возможно изучение механизма преступного деяния, а также учет связей между элементами его криминалистической характеристики. Моделирование в криминалистической методике может использоваться для замещения материалов сложных, трудно поддающихся расследованию уголовных дел, схематическими моделями (изображениями), позволяющими устанавливать интересующие исследователя отношения⁴²⁵. Увеличение количества преступлений, связанных с использованием информационно-телекоммуникационных технологий и различных технических средств, закономерно требует формирования новых криминалистических рекомендаций и алгоритмов расследования, в частности по обнаружению и фиксации цифровых доказательств с использованием программных технико-

⁴²⁴ Голунский С. А. Криминалистика : методика расследования отдельных видов преступлений / под ред. А. Я. Вышинского. М. : Юриздат, 1939. С. 25.

⁴²⁵ Возгрин И. А. Криминалистическая методика расследования преступлений. Минск : Высшая школа, 1983. С. 44.

криминалистических средств.

Изученный по настоящее время опыт расследования преступлений в сфере компьютерной информации и множество иных разрозненных, но научно-обоснованных данных, связанных с повышением эффективности раскрытия такого рода преступлений, в частности, с использованием технико-криминалистических средств, закономерно привели к необходимости систематизации и обобщения всех имеющихся сведений, содержащихся в существующих частных криминалистических методиках с возможностью их трансформации в алгоритмы или программы расследования.

Развитие современной науки в целом характеризуется углубляющейся специализацией и одновременным разделением ранее существовавших отраслей научного знания на новые. Несмотря на то, что новые научные положения, связанные с применением в расследовании информационных технологий, не в полной мере вмещаются в структуру криминалистики, их все же вполне можно рассматривать.

Рассмотрение теоретических и методологических основ создания и использования типовых моделей преступной деятельности, выявление присущих ей закономерностей, а также практика ее типизации и моделирования послужили импульсом для новых криминалистических разработок, объектом изучения которых стал метод моделирования⁴²⁶, что создало предпосылки формирования и развития метода ситуационного подхода к расследованию преступлений (теории криминалистической ситуалогии)⁴²⁷.

Однако отказ от универсализации схем расследования для всех категорий преступлений обуславливает необходимость разработки частных криминалистических методик, ориентированных на типовые следственные ситуации, характерные для конкретных видов и моделей преступных деяний, и предусматривающих дифференцированные подходы к организации их расследования. Соответственно, любая частная криминалистическая методика может быть представлена набором криминалистических алгоритмов (программ) расследования⁴²⁸ и моделей, формализованных на основе современных подходов к обработке данных.

⁴²⁶ Грибунов О. П., Агафонов А. С. Концептуальные идеи В. Я. Колдина в криминалистике и судебно-экспертной деятельности // *Baikal Research Journal*. 2022. 13 (1). С. 3.

⁴²⁷ Волчецкая Т. С. Криминалистическая ситуалогия. Указ. соч. С. 18.

⁴²⁸ Шаталов А. С. Алгоритмизация и программирование расследования преступлений в системе криминалистической методики // *Журнал Высшей школы экономики*. 2017. № 2. С. 164.

Выявленные в ходе проведенного исследования признаки, определяющие минимально необходимые элементы, входящие в материал проверки сообщения (заявления) о преступлении, а также в материалы первоначального и последующего этапов расследования могут быть аналогичным образом заложены в основу предлагаемой информационно-компьютерной модели преступного деяния (цифрового двойника преступления), совершенного в сфере компьютерной информации.

Вышеуказанные признаки могут выступить набором данных для формирования прогноза раскрываемости смоделированного преступления⁴²⁹, а также наиболее подходящего и эффективного алгоритма его расследования.

Признаки преступлений, выявленные в рамках исследования материалов уголовных дел, могут относиться к любому элементу состава преступления, но чаще всего соотносимы со способом совершения преступного деяния и оставляемыми следами преступления либо способами их сокрытия, что подтверждается множеством теоретических исследований ученых-криминалистов⁴³⁰. На современном этапе развития науки и техники находить и исследовать информацию, обладающую доказательственной ценностью, позволяет использование технико-криминалистических средств. Важно учитывать при этом степень научности применяемых приемов, методов и технико-криминалистических средств, рекомендуемых для внедрения в практику, которая должна складываться из: оценки научной обоснованности предложений о целесообразности и полезности их внедрения; научности методики их применения и формулируемых на основе полученных результатов их использования выводов; достоверности результатов их применения⁴³¹.

В отношении традиционных видов преступности на сегодняшний день разработано и успешно применяется множество криминалистических методик расследования, не раз прошедших научную апробацию. В большинстве из них

⁴²⁹ Barrenechea M. M., Lengua M. A. A systematic literature review on the use of artificial intelligence for cybercrime rate forecasting // Bulletin of electrical engineering and informatics. 2025. №. 14 (3). P. 2043.

⁴³⁰ Митричев С. П. Методика расследования отдельных видов преступлений. М. : Всесоюз. юрид. заоч. ин-т, 1973. С. 13.; Густов Г. А., Танасевич В. Г. Признаки хищений социалистической собственности // Вопросы совершенствования предварительного следствия. 1971. С. 89; Курс криминалистики : сборник научных трудов : в 3 томах / под ред. О. Н. Коршуновой : Т. 2 : Общие положения криминалистической методики. Методика расследования преступлений против личности. Методика расследования преступлений против собственности. М. : Юридический центр, 2024. С. 30.

⁴³¹ Эксархопуло А. А. Криминалистическая теория: формирование и перспективы развития в условиях научно-технического прогресса : дис. ... докт. юрид. наук. СПб, 1993. С. 174.

применение современных технико-криминалистических средств научно обоснованно с точки зрения полезности их внедрения, повышения оперативности собирания доказательств, что сокращает сроки расследования.

Современные условия развития информационно-телекоммуникационных технологий и повсеместная цифровизация, способствующие широкому распространению преступлений в сфере компьютерной информации, диктуют объективную необходимость в разработке и внедрении новых криминалистических методик их расследования, в том числе приемов, методов и программных технико-криминалистических средств⁴³².

Несмотря на то, что работа по систематизации и типологизации следственных ситуаций проводится давно⁴³³, на сегодняшний день отчетливо прослеживается их принципиальная значимость для построения эффективных программных технико-криминалистических средств, однако в полной мере ресурс их не воплощен⁴³⁴. Обусловлено это необходимостью реализации сложных динамичных (самообучающихся) алгоритмов расследования, что возможно лишь на основе технологий искусственного интеллекта (машинного обучения), в основу которых заложены математические методы (математический анализ, линейная алгебра и матричные вычисления, теория вероятностей и математической

⁴³² Свидетельство о государственной регистрации программы для ЭВМ № 2021665929 Российская Федерация. Алгоритмический комплекс процессуальных действий при дистанционном мошенничестве «АКПД Дистант» : № 2021662179 : заявл. 29.07.2021 : опубл. 05.10.2021; Свидетельство о государственной регистрации программы для ЭВМ № 2023667143 Российская Федерация. Тактика производства отдельных видов осмотра при расследовании преступлений, совершенных с использованием информационных технологий : № 2023666488 : заявл. 04.08.2023 : опубл. 10.08.2023; Свидетельство о государственной регистрации программы для ЭВМ № 2025682277 Российская Федерация. CyberCodex [КиберКодекс] – Программное технико-криминалистическое средство «Киберпреступность» с кодификатором преступлений в сфере компьютерной информации : № 2025680136 : заявл. 31.07.2025 : опубл. 22.08.2025; Свидетельство о государственной регистрации программы для ЭВМ № 2025682275 Российская Федерация. Blockchain & CFA analytics [Аналитика блокчейна и ЦФА] – Расследование преступлений, связанных с использованием цифровых финансовых активов и сети блокчейн : № 2025680132 : заявл. 31.07.2025 : опубл. 22.08.2025; Свидетельство о государственной регистрации программы для ЭВМ № 2025682276 Российская Федерация. MaCDEV TechView [Осмотр технических средств] – Производство осмотра компьютерной техники и мобильных устройств при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий : № 2025680135 : заявл. 31.07.2025 : опубл. 22.08.2025.

⁴³³ Селиванов Н. А. Математические методы в собирании и исследовании доказательств : монография. М. : Юридическая литература, 1974. С. 10.

⁴³⁴ Бессонов А. А. О некоторых вопросах использования математических методов в криминалистике и расследовании преступлений // Математические методы и информационно-технические средства : материалы XVII Всероссийской научно-практической конференции. Краснодар: Краснодарский университет МВД России, 2021. С. 33.

статистики, численные методы оптимизации, теория графов, логика и алгоритмы⁴³⁵ и пр.). Алгоритм – это пошаговое описание (предписание, инструкция или правило), выполняемого шаг за шагом и опирающегося на конечное множество правил решения конкретной задачи из какого-либо класса задач определенного типа⁴³⁶. Преимуществами применения алгоритмов, очевидно, является повышение эффективности решения задач за счет снижения временных и трудовых затрат. Решение задачи с помощью алгоритма разбивается на простые операции и осуществляется автоматически или автоматизированно. Во всех случаях, когда процесс решения той или иной задачи формализуется, т. е. выявляется некая последовательность правил, подразумевают алгоритмизацию решения задачи.

Проведенный библиографический поиск с учетом морфологии слов свидетельствует о широкой распространенности подхода алгоритмизации процесса расследования преступлений в целом. Так, расширенный поиск с использованием ключевых слов, операторов поиска и ранжирования результатов в международной библиографической базе данных «Google Scholar»⁴³⁷, индексирующей научные работы из различных источников, включая академические издательства, репозитории и прочие источники по фразе «алгоритм* расслед* преступлен*» выдает более 16 тыс. наименований научных изданий (на русском языке) и более 21 тыс. результатов по фразе «*crim* investigat* algorithm**» на английском.

Поиск с учетом морфологии в российской научной электронной библиотеке, интегрированной с Российским индексом научного цитирования, «Elibrary»⁴³⁸ по вышеуказанным фразам предоставляет более 29 тыс. результатов на русском языке и более 2 тыс. источников на английском языке соответственно. В настоящее время при расследовании различных преступлений могут применяться алгоритмы с жестко детерминированными предписаниями⁴³⁹ в виде методик расследования (методических рекомендаций), однако, в условиях неочевидности следственной версии или принимаемого решения целесообразнее применять криминалистические алгоритмы эвристического типа, которые допускают в рамках

⁴³⁵ Николенко С. И. Машинное обучение: основы. СПб. : Питер, 2025. С. 49.

⁴³⁶ Кондаков Н. И. Логический словарь-справочник. М. : Наука, 1975. С. 30.

⁴³⁷ Библиографическая база данных Google Scholar (Академия Google) // Академия Google : офиц. сайт. URL: <https://scholar.google.com> (дата обращения: 27.05.2025).

⁴³⁸ Российская научная электронная библиотека, интегрированная с российским индексом научного цитирования Elibrary.ru // Научная электронная библиотека Elibrary.ru : офиц. сайт. URL: <https://www.elibrary.ru> (дата обращения: 27.05.2025).

⁴³⁹ Свидетельство о государственной регистрации программы для ЭВМ № 2020610510 Российская Федерация. БАЗИС – базовый анализ защищенности информационных систем : № 2019666679 : заявл. 17.12.2019 : опубл. 15.01.2020.

системы предписаний автоматизированный⁴⁴⁰ или автоматический поиск оптимальных путей⁴⁴¹, в частности на основе искусственного интеллекта⁴⁴², оценку предпринятых действий и их корректировку при необходимости⁴⁴³.

Криминалистический алгоритм – это обусловленная законом система последовательно выполняемых предписаний, направленных на эффективное решение задач по раскрытию, расследованию и предупреждению преступлений⁴⁴⁴. Деление процесса расследования на этапы само по себе представляет схожий с дискретностью или процессом деления алгоритма на итерации процесс (итерация от англ. «iteration» – повторение, представляет собой композицию (К) из нескольких алгоритмов действий, например, (1) и (2), при которых для любого входного воздействия (3) соответствующая композиция (К) получается в результате последовательного или многократного применения алгоритма (1) до получения результата, преобразуемого алгоритмом (2)⁴⁴⁵.

Исходной целью систематизации криминалистических алгоритмов является процесс программирования расследования. Под программой расследования при этом понимается совокупность предназначенных для реализации в деятельности по раскрытию и расследованию преступлений криминалистических алгоритмов, а также научных рекомендаций, содержащих типовую криминалистически значимую информацию⁴⁴⁶. Дискретный характер процесса расследования позволяет выделить отдельные его этапы, алгоритмизировав, например, следственные действия, которые отличаются особенностями, определяемыми

⁴⁴⁰ Свидетельство о государственной регистрации программы для ЭВМ № 2024661188 Российская Федерация. Blockchain analytics [аналитика блокчейна] расследование преступлений, связанных с использованием криптовалют и сети блокчейн : № 2024619990 : заявл. 06.05.2024 : опубл. 16.05.2024.

⁴⁴¹ Свидетельство о государственной регистрации программы для ЭВМ № 2022661783 Российская Федерация. Оптимизация базы данных на основе символьного анализа : № 2022660010 : заявл. 01.06.2022 : опубл. 27.06.2022.

⁴⁴² Свидетельство о государственной регистрации программы для ЭВМ № 2023667481 Российская Федерация. BIOSCAN – Интеллектуальная система распознавания биометрических данных на основе машинного обучения (ML), компьютерного зрения (CV) и искусственного интеллекта (AI) : № 2023666662 : заявл. 08.08.2023 : опубл. 15.08.2023.

⁴⁴³ Свидетельство о государственной регистрации программы для ЭВМ № 2022611631 Российская Федерация. Система мониторинга киберинцидентов Local SIEM : № 2022610610 : заявл. 19.01.2022 : опубл. 28.01.2022.

⁴⁴⁴ Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. Указ. соч. С. 70; Вандер М. Б. Схемы криминалистических алгоритмов. Санкт-Петербург : СПбЮИ, 1998. С. 3.

⁴⁴⁵ Соловьева Т. Н. Информатика. Основы алгоритмизации и программирования. Пермь : Пермский государственный национальный исследовательский университет, 2018. С. 15.

⁴⁴⁶ Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. Указ. соч. С. 77.

законом и криминалистической тактикой.

Для того чтобы реализовать алгоритм с помощью компьютера необходима запись решения задачи на машинном (математическом) языке в виде последовательности команд, оформленных с помощью символов определенной системы счисления (чаще двоичной), которая в разрезе интеллектуальных технологий сводится к так называемому машинному обучению (набор специальных алгоритмов, воплощающих ключевое свойство нейронных сетей – способность самообучения на основе получаемых данных)⁴⁴⁷. Выражение задачи на математическом языке (языке формализации) позволяет использовать для ее последующего решения определенный эвристический алгоритм.

Таким образом, в последующем под алгоритмом расследования будет пониматься детерминированный в машиночитаемой форме порядок деятельности, учитывающий динамику следственной ситуации и возможные ее трансформации, с представленными в ней сведениями о криминалистически значимых признаках и их корреляционных и вероятностных связях в виде математических категорий. Под программами расследования будет, соответственно, пониматься набор описанных алгоритмов расследования.

Стоит также отметить, что программы расследования преступлений, представляя собой многовариантные системы следственных действий, оперативно-розыскных мероприятий, организационно-технических и иных действий, не всегда описывают тактику их подготовки и проведения⁴⁴⁸. Характерной особенностью криминалистического алгоритма является его приближение к эвристическому типу алгоритмизации, что позволяет их использовать в условиях неопределенности исходных данных при необходимости оперирования субъекта деятельности признаками объектов познания, не всегда поддающимися количественной характеристике⁴⁴⁹.

В структуру методики расследования преступлений любого вида, как правило, включают⁴⁵⁰: особенности возбуждения уголовного дела; обстоятельства, подлежащие установлению в процессе расследования преступления; типичные следственные ситуации, складывающиеся на первоначальном и последующем

⁴⁴⁷ Постолиит А. В. Основы искусственного интеллекта в примерах на Python. Указ. соч. С. 76.

⁴⁴⁸ Возгрин И. А. Криминалистическая методика расследования преступлений. Указ. соч. С. 211

⁴⁴⁹ Полевой Н. С Криминалистическая кибернетика. М. : Изд-во МГУ, 1982. С. 131.

⁴⁵⁰ Криминалистика: методика расследования преступлений / под ред. И. В. Александрова. Т. 5. М. : Юрайт, 2025. С. 32.

этапах расследования; систему следственных действий и оперативно-розыскных мероприятий; особенности применения специальных знаний по делам рассматриваемого вида; криминалистическую характеристику преступлений. Для криминалистической методики особенно важным является изучение аспектов, необходимых для разработки частных методик расследования преступлений. По этой причине довольно часто исследуются только наиболее значимые факторы, влияющие на успешное раскрытие, расследование и предотвращение преступлений⁴⁵¹.

Содержание криминалистической методики расследования преступлений на сегодняшний день отличается неоднородностью и имеет довольно развитую систему. Составными элементами, образующими научные основы организации расследования преступлений, являются криминалистическая теория программирования расследования и криминалистическое учение о реализации частных методик расследования преступлений⁴⁵², развитие которых позволит систематизировать планирование следственных действий по преступлениям в сфере компьютерной информации, отличающихся своим многообразием и сложностью в определении подхода к их расследованию, а также опосредованностью с цифровой формой информации.

Сфера компьютерной информации, определяющая сходство объекта преступного посягательства, способов совершения преступлений, характеристик личности преступника и потерпевшего позволяет сформировать общие рекомендации, позволяющие устанавливать обстоятельства расследования, входящие в предмет доказывания.

Основным критерием систематизации частных криминалистических методик выступает вид преступления в соответствии с его уголовно-правовым значением. Элементы состава преступления, являясь основой соотнесения конкретного наказуемого по УК РФ деяния в отдельности, не позволяют полноценно сформировать методику расследования, что объясняется существованием различных по содержанию методик расследования преступлений, предусмотренных одной нормой уголовного права, но существенно отличающихся друг от друга.

⁴⁵¹ Возгрин И. А. Криминалистическая методика расследования преступлений. Указ. соч. С. 213; Tical G. M. Artificial intelligence and big data analysis in crime prevention and combat // Annals academy of romanian scientists series on military sciences. 2025. №17 (1). P. 40.

⁴⁵² Курс криминалистики. Указ. соч. Т. 2. С. 35.

По этой причине систематизацию частных криминалистических методик целесообразно строить на основе характеристик преступлений, различаемых не по уголовно-правовому, а по криминалистическому основанию⁴⁵³.

Именно поэтому информационной базой для разработки типовой методики расследования служит криминалистическая характеристика преступлений, при этом также учитываются наиболее распространенные следственные ситуации. В методике расследования особое значение имеют теоретические положения уголовного права, связанные с квалификацией преступления.

В ходе расследования может измениться квалификация преступления, признаки которого были выявлены на момент возбуждения уголовного дела, при этом методика расследования должна учитывать точное установление признаков определенного состава преступления, разрабатывая для этой цели систему следственных и иных действий, рассчитанную на различные ситуации расследования⁴⁵⁴.

Структуру частной криминалистической методики расследования преступлений в сфере компьютерной информации (Таблица 1) могут составить обстоятельства, подлежащие установлению при расследовании (установление признаков определенного состава преступления, обстоятельств, подлежащих доказыванию, и иных обстоятельств, выяснение которых требуется при расследовании преступлений данного вида), криминалистическая характеристика преступлений (как научная абстракция, содержащая в себе общие черты, свойственные криминалистическим характеристикам рассматриваемой группы преступлений, или система данных, способствующих раскрытию и расследованию преступлений⁴⁵⁵), а также криминалистическая характеристика расследования преступлений⁴⁵⁶ (в виде алгоритмической системы обобщенных сведений, раскрывающих основные закономерные черты механизма расследования преступлений по различным следственным ситуациям).

⁴⁵³ Эксархопуло А. А. Криминалистика. Указ. соч. С. 677.

⁴⁵⁴ Гавло В. К. Теоретические проблемы и практика расследования отдельных видов преступлений. Томск, 1985. С. 114.

⁴⁵⁵ Ищенко Е. П., Колдин В. Я. Указ. соч. С. 133.

⁴⁵⁶ Гавло В. К. Теоретические проблемы и практика расследования отдельных видов преступлений. Указ. соч. С. 215; Ким Д. В. Криминалистическая характеристика расследования преступлений как результат разрешения следственных ситуаций // Известия Алтайского государственного университета. 2000. № 2 (16). С. 45.

Таблица 1. – Структура частной методики расследования преступлений в сфере компьютерной информации

Структура частной криминалистической методики расследования преступлений в сфере компьютерной информации		
1. Обстоятельства, подлежащие установлению при расследовании	2. Криминалистическая характеристика преступления и доказательства по уголовному делу	3. Криминалистическая характеристика расследования преступления (программы расследования)
1.1. Квалификация преступного деяния (в соответствии с главой 28 УК РФ) (перечень)	2.1. Элементы криминалистической характеристики преступления (в соответствии с проведенным анализом материалов уголовных дел и судебно- следственной практики)	3.1. Особенности возбуждения уголовного дела
		3.2. Типичные следственные ситуации
3.3. Особенности первоначального этапа расследования преступления		
3.4. Особенности последующего этапа расследования преступления		
1.2. Обстоятельства, подлежащие доказыванию (в соответствии со ст. 73. УПК РФ)	2.2. Доказательства (в соответствии со ст. 74. УПК РФ)	3.5. Особенности заключительного этапа расследования преступления и подготовки обвинительного заключения
1.3. Иные обстоятельства, выяснение которых требуется при расследовании преступлений (в соответствии с УПК РФ)		

Предлагаемый элементный состав методики расследования позволит построить информационно-компьютерную модель (цифровой двойник), преступного деяния с автоматизированной выдачей по нему наиболее эффективного алгоритма расследования и вероятности раскрытия смоделированного преступления.

В предмет познания по уголовному делу в целом входят все обстоятельства, образующие состав преступления и подлежащие доказыванию⁴⁵⁷. По преступлениям в сфере компьютерной информации указанные обстоятельства устанавливаются в соответствии с содержанием статей, входящих в главу 28

⁴⁵⁷ Лузгин И. М. Расследование как процесс познания. М. : Высшая школа МВД СССР, 1969. С. 29.

УК РФ, и определяются соответствующими составами (п. 1.1. Таблицы 1).

При расследовании преступлений в соответствии со ст. 73 УПК РФ выявляются и фиксируются подлежащие доказыванию обстоятельства, перечень которых индивидуален и не является исчерпывающим, но, в основном, представлен следующими элементами (п. 1.2. Таблицы 1):

- событие преступления (объективные признаки состава преступления (объект и объективная сторона) – т. е. необходимо определить общественное отношение, на причинение вреда которому было направлено деяние, а также предмет преступления и обстоятельства, характеризующие личность и действия потерпевшего (что может оказаться важным для квалификации деяния и назначения наказания, в частности, при совершении преступления под влиянием сильного душевного волнения, вызванного неправомерными действиями потерпевшего и пр.), признаки объективной стороны преступления (время, место, обстановка и способ совершения преступления, а также другие обстоятельства совершения преступления при наличии) также входят в предмет доказывания и учитываются при квалификации деяния и назначении наказания);

- виновность лица в совершении преступления (форма вины (умысел (прямой, косвенный, легкомыслие или небрежность), неосторожность, вменяемость)) и мотивы совершения преступления;

- обстоятельства, характеризующие личность обвиняемого;

- характер и размер вреда, причиненного преступлением;

- обстоятельства, исключающие преступность и наказуемость деяния (например, физическое или психическое принуждение, исполнение приказа или распоряжения и пр.);

- обстоятельства, смягчающие (в соответствии со ст. 61 УК РФ) и отягчающие наказание (в соответствии со ст. 63 УК РФ);

- обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания;

- обстоятельства, связанные с подлежащим конфискации имуществом.

Стоит, однако, отметить, что обстоятельства, исключающие преступность и наказуемость деяния, смягчающие и отягчающие наказание, обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания, а также обстоятельства, связанные с конфискацией имущества, являются факторами, которые учитываются при назначении наказания судом, и влияют на его особенности, а не на описание самого преступления. Они влияют на вид или размер наказания, но не меняют криминалистическую характеристику

преступления, которая способна описать само преступление.

Криминалистическая характеристика преступления, будучи комплексом фактических данных и признаков преступления, как правило, не включает в себя правовую квалификацию и юридические оценки, в том числе обстоятельства, смягчающие наказание и пр. Это связано с тем, что данные обстоятельства являются предметом правовой квалификации и оценки суда. Однако в практике расследования и следствия сведения о факторах, которые впоследствии могут быть признаны судом смягчающими наказание (например, признание вины, активное содействие раскрытию преступления, раскаяние и пр.), могут фиксироваться в материалах дела как обстоятельства, влияющие на личность преступника или подозреваемого и его поведение, что имеет значение для методики расследования.

Подлежат выяснению также обстоятельства, способствовавшие совершению преступления, например, выявление уязвимости (наличие у потерпевшего уязвимости по предмету посягательства (в области эксплуатации компьютерной информации, технических средств, информационных систем, программного обеспечения и пр.)), обстоятельства, характеризующие личность и поведение потерпевшего, причины, в силу которых деяние не было доведено до конца, и степень осуществления противоправных намерений⁴⁵⁸, а также обстоятельства, которые подлежат установлению по делам, связанным с какими-либо конкретными обстоятельствами. Так, например, по уголовным делам, связанным с несовершеннолетними, необходимо учесть обстоятельства в соответствии со ст. 421 УПК РФ (п. 1.3. «Иные обстоятельства, выяснение которых требуется при расследовании преступлений» Таблицы 1) и т. п.

Систему значимой для раскрытия преступного деяния информации содержит криминалистическая характеристика преступления (п. 2.1. Таблицы 1). Содержание элементов криминалистической характеристики преступлений в сфере компьютерной информации было предложено ранее и включает в себя в совокупности:

- способ совершения преступления (тактика и техника в соответствии с базой угроз безопасности информации «Mitre Att&ck»);
- способ сокрытия следов преступления;
- типичные следы преступления;
- вероятные места нахождения типичных следов преступления;
- распространенность (серийность) преступного деяния;
- обстановку совершения преступления;

⁴⁵⁸ Белкин А. Р. Теория доказывания в уголовном судопроизводстве. Указ. соч. С. 40.

- место (среду) совершения преступления;
- время совершения преступления;
- прочие обстоятельства, связанные с обстановкой совершения преступления;
- личность преступника;
- личность потерпевшего;
- предмет посягательства (при наличии).

В процессе установления обстоятельств, подлежащих доказыванию, в соответствии со ст. 74 УПК РФ, выявляются и фиксируются доказательства (п. 2.2. Таблицы 1), которыми в уголовном процессе признаются любые сведения, полученные в порядке, установленном законом, на основании которых суд, прокурор, следователь, дознаватель устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных значимых для уголовного дела обстоятельств в виде:

- показаний подозреваемого, обвиняемого, потерпевшего, свидетеля;
- заключений и показаний эксперта;
- заключений и показаний специалиста;
- вещественных доказательств;
- протоколов следственных и судебных действий;
- иных документов.

Развитие систем электронного документооборота все чаще вызывает проблемы, связанные с использованием в доказывании документов, обрабатываемых в цифровом виде. Указанные документы по содержанию и связи с преступлением могут быть подразделены на вещественные доказательства и иные документы⁴⁵⁹.

Криминалистическая характеристика расследования преступлений (п. п. 3.1–3.5 Таблицы 1) как комплекс сведений, отражающих основные закономерности механизма расследования в складывающихся следственных ситуациях, раскрывает особенности:

- проведения доследственной проверки, необходимой для принятия решения о возбуждении уголовного дела (поводы к проведению проверки, способы и средства проверки сообщений о преступлении в сфере компьютерной информации);
- первоначального этапа расследования, задачей которого является

⁴⁵⁹ Белкин А. Р. Теория доказывания в уголовном судопроизводстве. Указ. соч. С. 218.

подтверждение криминального характера проверяемого события и обнаружение доказательств, достаточных для предъявления обвинения (включает в себя выдвижение и проверку типичных версий по делу, первоначальные следственные действия и оперативно-розыскные мероприятия, направленные на выяснение характера имевшего место события и сбор доказательств, действия, направленные на получение данных о личности преступника, его розыск и задержание, а также конкретизацию версий и составление развернутого плана расследования для их проверки);

– последующего этапа расследования, задачей которого является проверка собранных доказательств вины конкретных лиц, привлекаемых к уголовной ответственности, подтверждение или опровержение их показаний (включает в себя проведение следственных действий и оперативно-розыскных мероприятий в соответствии с развернутым планом расследования с целью завершения сбора доказательств, изобличающих конкретное лицо в совершении преступления, предъявление обвинения и допрос обвиняемого, а также проведение следственных действий, имеющих цель проверить собранные на первоначальном этапе расследования доказательства, подтвердить или опровергнуть показания обвиняемого, полученные на допросе);

– завершающего этапа расследования, включающего в себя рассмотрение заявленных ходатайств о проведении дополнительных следственных действий, выяснение причин и условий, способствовавших совершению преступления, оценку всех собранных по делу доказательств, требующую принятия дополнительных мер, и составление обвинительного заключения с учетом состава конкретного преступления, а также перечисления санкций (видов, размеров наказаний) за их совершение⁴⁶⁰.

Несмотря на дискуссионность соотнесения предмета доказывания с криминалистической характеристикой преступления, стоит отметить, что базой для построения криминалистической характеристики определенного вида преступления может являться предмет доказывания⁴⁶¹, однако, предмет доказывания определяет конечную цель расследования преступления, а криминалистическая характеристика помогает найти конкретные пути и способы ее достижения⁴⁶². Таким образом, правильное их соотносить друг с другом как

⁴⁶⁰ Эксархопуло А. А. Криминалистика. Указ. соч. С. 682.

⁴⁶¹ Каневский Л. Л. Криминалистические проблемы расследования и профилактики преступлений несовершеннолетних. Указ. соч. С.78.

⁴⁶² Шабанов В. Б., Ермолович В. Ф. Соотношение криминалистической характеристики преступлений со следственными ситуациями, предметом доказывания, версиями и задачами расследования преступления. Указ. соч. С. 81.

средство, соотносимое с целью (т. е. используя элементы криминалистической характеристики преступления и их взаимосвязи можно установить обстоятельства, подлежащие доказыванию)⁴⁶³.

Содержание криминалистической характеристики в полной мере охватывающее все элементы предмета доказывания с теми их особенностями, которые присущи расследованию конкретной категории преступлений, избавляет от выделения в качестве самостоятельного структурного элемента конкретной частной методики перечня обстоятельств, подлежащих доказыванию (установлению) по данной категории уголовных дел⁴⁶⁴. Это приводит к мысли о том, что в качестве обучающих данных для реализации информационно-компьютерной модели преступного деяния (цифрового двойника преступления) в виде системы на основе искусственного интеллекта исчерпывающим будет набор данных, основанный на совокупности элементов криминалистической характеристики преступного деяния.

Криминалистическая методика устанавливает наиболее важные особенности организации расследования преступлений, которые обуславливают⁴⁶⁵:

- порядок формирования исходной информации о событии преступления;
- связи и зависимости расследования преступлений от особенностей преступных деяний;
- организационные особенности проверки сообщения (заявления) о преступлении;
- определение круга вопросов, подлежащих исследованию и установлению при расследовании;
- разработку наиболее эффективных программ расследования.

Таким образом, сформированные ранее криминалистические характеристики преступлений в сфере компьютерной информации могут выступить источником формирования исходной информации о событии преступления (п. 1), а элементы, входящие в криминалистическую характеристику преступлений, способствовать определению связей и зависимостей хода расследования преступлений от особенностей преступных деяний (п. 2).

С учетом того, что ранее были выявлены особенности проверки сообщений (заявлений) о преступлении (п. 3) и обстоятельства, подлежащие исследованию и установлению (п. 4) в целях комплексного анализа закономерностей организации расследования рассматриваемых преступлений, закономерно встает вопрос о

⁴⁶³ Эксархопуло А. А. Криминалистика. Указ. соч. С. 590

⁴⁶⁴ Белкин А. Р. Теория доказывания в уголовном судопроизводстве. Указ. соч. С. 47.

⁴⁶⁵ Курс криминалистики. Указ. соч. Т. 2. С. 35.

необходимости разработки наиболее эффективных программ расследования (п. 5)⁴⁶⁶. Представленная выше совокупность закономерностей организации расследования составит предмет криминалистической методики расследования преступлений в сфере компьютерной информации. Таким образом, следственная ситуация выступит в роли исходного условия для формирования алгоритма расследования, в таком случае переход от анализа ситуации к формализации алгоритма и его практической реализации является сущностью применения криминалистической методики на практике.

Трансформация описательной формы изложения классических рекомендаций к нежестким алгоритмам (недетерминированные, вариативные, самообучающиеся алгоритмы машинного обучения) является существенным этапом развития частных методик расследования преступлений, особенно тех, признаки которых можно отразить в цифровой форме. Из одной следственной ситуации может вытекать необходимость разработки нескольких алгоритмов расследования (количество их может определяться в соответствии с предметом доказывания и выдвинутых следственных версий). Типичные следственные ситуации позволяют определить и типичные алгоритмы расследования преступлений, соответственно, при расследовании преступлений целесообразно рассматривать то количество алгоритмов, которое как минимум соотносимо с количеством этапов расследования, либо больше их, аналогично следует рассматривать и то количество групп соотношений следственных ситуаций с алгоритмами расследования. Разнообразие типичных следственных ситуаций порождает и множество типичных алгоритмов расследования преступлений⁴⁶⁷.

По этой причине, преступления в сфере компьютерной информации – это один из наиболее подходящих под критерий «оцифрованности» видов преступных деяний, позволяющих сформировать цифровой двойник преступного деяния с автоматизированной выдачей по нему наиболее эффективного алгоритма расследования и вероятности раскрытия. Включение алгоритмов расследования в структуру методических рекомендаций придает последним особую практическую значимость, поскольку, как было выявлено, изучение типичных следственных ситуаций и соответствующих им алгоритмов расследования создает прочную основу для дальнейшего развития криминалистической методики расследования преступлений.

⁴⁶⁶ Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. Указ. соч. С. 15.

⁴⁶⁷ Возгрин И.А. Криминалистическая методика расследования преступлений. Указ. соч. С. 163.

Не останавливаясь на данном этапе исследования на процедуре отбора типичных признаков для включения в наборы обучающих данных и формирования цифрового двойника преступления стоит отметить, что такого рода подход к формированию методик расследования преступлений возможно распространить и на другие родовые группы преступных деяний при условии аккумуляции сведений о типичных следственных ситуациях, совокупности элементов криминалистической характеристики преступления (типичных их признаках), а также имеющихся доказательствах, формализация сведений о которых позволит использовать их в качестве обучающих данных для реализации информационно-компьютерной модели преступного деяния и выявления наиболее эффективных алгоритмов его расследования.

Основной целью адаптации нормативного регулирования в области противодействия преступлениям в сфере компьютерной информации под современные тенденции развития и использования информационных технологий является формирование криминалистических методик расследования. Проведенный анализ позволяет сделать вывод, что выявление наиболее эффективных методик и инструментов противодействия преступлениям рассматриваемого вида возможно на основе кодирования преступлений (присвоения преступлениям уникальных кодов), что поможет «объединить» юридические, технологические и прогностические аспекты.

Методики расследования отдельных видов преступлений, как частные, так и типичные, направлены на оптимизацию процессуальных механизмов, обеспечивающих повышение эффективности их раскрытия и расследования. Соответственно, учитывая значительную распространенность и полиморфизм рассматриваемых преступлений, актуальной задачей выступает разработка системы присвоения кодов преступным деяниям, совершаемым в сфере компьютерной информации, с целью исключения дискретности принимаемых мер по противодействию им. Такое кодирование послужит основой для формирования криминалистических методик, адаптированных к специфике преступлений, и позволит дифференцированно применять инструменты расследования и предупреждения противоправных деяний. Систематизация указанных преступлений по юридически значимым признакам будет способствовать идентификации оптимальных криминалистических алгоритмов, что в конечном итоге минимизирует риски латентности и повысит результативность уголовно-процессуальной деятельности. Проводимое в дальнейшем криминалистическое кодирование позволит не только систематизировать объекты, но и исключить из сферы исследования объекты, не входящие в предмет исследования.

4.2. Криминалистическое кодирование преступлений в сфере компьютерной информации и его роль в формировании типовых алгоритмов расследования

Эволюция информационных технологий неизменно опережает темпы формирования правовых механизмов, что создает колоссальный разрыв между возможностями киберпреступников и инструментами, доступными правоохранительным органам. Указанный дисбаланс подчеркивает необходимость адаптации правовых механизмов к динамичной природе преступлений в сфере компьютерной информации, которая обеспечит гибкость системы уголовного правосудия в условиях стремительно развивающихся технологий. Очевидно, что в рассматриваемой области сформировалась потребность модернизации отдельных направлений криминалистики в соответствии со способами, средствами и условиями совершаемых преступлений. Так, в подготовленном полицейской службой Европейского союза (Европол) совместно с Агентством Европейского союза по сотрудничеству в области правоохранительной деятельности (Евроюст) отчете о борьбе с киберпреступностью отмечено, что расследования часто усложняются из-за образования огромных массивов данных, которые приходится обрабатывать в рамках уголовного дела⁴⁶⁸.

Материалы расследования могут включать терабайты или даже петабайты данных, что затрудняет хранение, управление и эффективный анализ без значительных вычислительных ресурсов и специализированных инструментов. Объем данных может быть непосильным для следователей и экспертов, приводя к увеличению временных затрат⁴⁶⁹ на их исследование, обработку, а также к невозможности их последующего хранения.

Аналогичная проблема затрагивает поставщиков услуг, которые должны обеспечивать сохранность указанных данных. Сложность доступа к цифровым доказательствам зачастую приводит в тупик, поскольку все чаще отсутствует возможность их своевременного изъятия и исследования. Кроме того,

⁴⁶⁸ Общие проблемы киберпреступности: аналитический отчет за 2024 год // Агентство Европейского союза по сотрудничеству в области правоохранительной деятельности (Евроюст) офиц. сайт. URL: <https://www.eurojust.europa.eu/publication/common-challenges-cybercrime> (дата обращения: 11.01.2025).

⁴⁶⁹ Аминев Ф. Г. Организационно-правовые вопросы взаимодействия суда и экспертных организаций при назначении и проведении судебных экспертиз // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции. Москва: Российский государственный университет правосудия. 2021. С. 66.

международные расследования в ряде случаев упираются в бюрократические преграды, когда запросы между странами осуществляются месяцами, либо не принимаются вообще по причине геополитического разлада.

Цифровые данные могут представлять собой как структурированные данные, такие как, например, базы данных на языке простых запросов SQL (от англ. «structured query language» – язык структурированных запросов), так и неструктурированные сведения в виде электронных писем, сообщений в социальных сетях и мессенджерах, массивы изображений и документов. Распространенной проблемой при исследовании больших и неструктурированных наборов данных является выбор метода их обработки и последующего анализа⁴⁷⁰. Существует множество различных способов структурирования, хранения и исследования баз данных. Они называются моделями данных и определяют, как специалист может работать с ними наиболее эффективно.

На сегодняшний день отсутствует единая модель данных, принятая на международном уровне, что закономерно приводит к длительным задержкам при обработке таких баз данных ввиду отсутствия взаимодействия между государствами, поскольку различие используемых моделей данных требуют дополнительных действий в виде переформатирования и реструктуризации цифровых данных для их последующей обработки.

Преступления в сфере компьютерной информации представляют собой эволюционирующий феномен, требующий не только адаптивных инструментальных решений противодействия им, но и правовых механизмов, являющихся основой для технической реализации таких инструментов.

Чтобы лучше понимать взаимосвязи при анализе цифровых доказательств, в частности, образующихся при использовании преступниками методов анонимизации своей личности или, например, обфускации вредоносного программного обеспечения и т. п., назрела необходимость в классификации преступлений в сфере компьютерной информации и разработке аналитических инструментов, позволяющих проводить эффективный сбор и анализ цифровых данных, образующихся при их расследовании.

Именно рассматриваемый вид преступлений благодаря своей опосредованности с цифровой формой информации может сформировать принципиально новую систему унификации процесса расследования благодаря

⁴⁷⁰ Усов А. И. Стандарты судебной экспертизы как инструмент цифровизации криминалистики. Указ. соч. С. 216.

присвоению криминальным актам уникальных кодов (кодирование), однозначно идентифицирующих как распространенные в настоящее время, так и вновь появляющиеся средства и способы совершения преступных деяний во всем их многообразии⁴⁷¹. Криминалистическая классификация преступлений есть опосредующая уголовно-правовую их классификацию систематика преступлений на основе единства механизма совершения отдельных видов и групп преступлений, других наиболее стабильных элементов криминалистической характеристики преступлений и соответствующего единства их отражения вовне⁴⁷². Именно в рамках классификации формируется наиболее полная и систематизированная форма криминалистических категорий, детерминирующих преступление как объект криминалистического познания. Такой подход служит основой для последующего анализа криминального деяния, обеспечивая системно-структурное представление результатов исследования, поиск аналогий, сравнение сложившихся обстоятельств с ранее возникающими следственными ситуациями, а также формирование наиболее подходящей методики расследования.

На фоне стабильного роста количества преступлений, совершаемых в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий, процессы синергии в криминалистике резко возросли, что обусловлено развитием теории информационно-компьютерного обеспечения криминалистической деятельности⁴⁷³ и появлением новых закономерностей и механизмов слеодообразования, современных информационных технологий, позволяющих собирать, анализировать и оценивать криминалистически значимую информацию с применением новых подходов криминалистической тактики и методики. Объектами указанной теории являются технические средства, информационные системы, как носители доказательственной информации, а также система действий и отношений в механизмах преступлений с использованием технических средств, информационных систем и информационных технологий, применяемых для обнаружения, фиксации, изъятия и исследования криминалистически значимой

⁴⁷¹ Харисова З. И. Криминалистическая кодификация преступлений в сфере компьютерной информации и ее роль в унификации процесса // Вестник Санкт-Петербургского университета МВД России. 2025. № 4 (108). С. 134.

⁴⁷² Баев О. Я. Основы методики уголовного преследования и профессиональной защиты от него: (на примере уголовно-процессуального исследования должностных и служебных преступлений) : научно-практическое пособие. М. : Эксмо, 2009. С. 20.

⁴⁷³ Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности : монография. М. : Проспект, 2022. С. 17.

информации, которое в рамках расследования преступлений в сфере компьютерной информации осложняется образованием значительных массивов данных, требующих современного подхода к их анализу.

Исходя из целостности предмета и системы криминалистики для исследования технических средств и информационных систем необходим особый комплекс специальных знаний. По этой причине выдвигается гипотеза о необходимости структурировать, классифицировать и присвоить уникальные коды рассматриваемым преступлениям (в значении упорядочивания, как одного из видов работ в области инженерии знаний) с целью последующего преодоления фрагментарности их учета, сложности обработки больших объемов цифровых данных, а также выдвижения адаптивной и унифицированной методики их расследования. Предлагаемая система кодирования позволит заложить основу универсальной концепции стандартизированного учета преступлений в сфере компьютерной информации, упростив процесс идентификации их составов. Основным недостатком, равно как и преимуществом, формируемого кодового набора является необходимость периодического обновления кодов системы, учитывающих появление новых способов совершения преступлений в сфере компьютерной информации. С этой целью необходимо рассмотреть имеющиеся в настоящее время критерии для предлагаемого кодирования.

Концепцией государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-телекоммуникационных технологий, рассматриваемые преступления с учетом критериев их квалификации классифицируются по трем основным типам:

- правонарушения и преступления в сфере компьютерной информации;
- правонарушения и преступления, криминообразующим или квалифицирующим признаком которых является их совершение с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»;
- правонарушения и преступления, при совершении которых применение информационно-телекоммуникационных технологий является альтернативным способом.

Рассматривая преступления в сфере компьютерной информации в контексте указания Генеральной прокуратуры Российской Федерации № 503/11 и МВД России № 1 от 28 июля 2025 г. квалифицирующее значение может иметь средство совершения указанных деяний в виде использования:

- информационно-телекоммуникационной сети «Интернет»;

- компьютерной техники и вспомогательного компьютерного оборудования;
- мобильных устройств связи;
- программного обеспечения, установленного на компьютере, мобильном устройстве или смартфоне и пр. вычислительной технике;
- социальных сетей и различных онлайн-сервисов;
- интернет-мессенджеров, установленных на компьютере и смартфонах;
- фишинговых ресурсов, либо веб-ссылок, ведущих на них;
- средств неправомерного доступа к компьютерной информации;
- вредоносных компьютерных программ (их созданием, распространением), «программ-шифровальщиков»;
- компьютерных сетей, состоящих из узлов, зараженных вредоносным программным обеспечением с возможностью централизованного управления без ведома владельцев узлов (ботнет-сетей);
- программное обеспечение для распределенных DDoS-атак типа «отказ в обслуживании»;
- методик синтеза аудио или визуальной информации, основанной на технологии искусственного интеллекта (дипфейков);
- анонимной сети с туннелированием (децентрализованной сети даркнет);
- систем расчета между финансовыми организациями и интернет-пользователями при покупке-продаже товаров и оплате услуг (электронных платежных систем);
- средств обращения цифровой валюты, цифровых финансовых активов и осуществления в отношении них различных действий;
- поддельных электронных платежных документов, имеющие равную юридическую силу с платежными документами на бумажных носителях;
- инструментов для неправомерного списания денежных средств с банковских счетов;
- средств и техники, предназначенных для компрометации банкоматов и терминалов (скиммеры и пр.);
- SIP-телефонии (от англ. «session initiation protocol» – протокол установления сеанса), организованной на базе IP-протоколов;
- зарубежных (в том числе стран – участников Содружества Независимых Государств) серверов (услуг хостинга и интернет-провайдеров, а также почтовых серверов), доменных зон и телефонных сетей.

Анализ обстановки совершения преступления, представленной в качестве самостоятельного элемента криминалистической характеристики, позволяет следователю получить информацию об обстоятельствах и условиях, непосредственно предшествовавших преступлению, о том, что в обстановке способствовало или препятствовало совершению преступления, каким образом обстановка повлияла на выбор способов, орудий, а также о личности потерпевшего и др.⁴⁷⁴ Средства совершения преступления и обстановка тесно взаимосвязаны и в целом образуют картину произошедшего события. Так, средство совершения преступления может указывать на применяемый преступником способ совершения преступления, а также на время и место его осуществления.

Переходя к рассмотрению способов совершения преступления, как одного из важнейших элементов криминалистической характеристики преступлений в сфере компьютерной информации, необходимо отметить, что повсеместное использование информационно-телекоммуникационных технологий и внедрение программного обеспечения за последние два десятка лет потребовало систематизации данных о всех имеющихся уязвимостях в информационной сфере.

Так, некоммерческая компания Mitre сформировала набор матриц тактик и техник киберпреступников, представляющий собой основанную на реально существующих наблюдениях баз данных инцидентов безопасности. Каждая матрица представляет собой таблицу с указанием угроз и соответствующих им тактик злоумышленников. Матрицы рассматриваемой базы данных описывают все возможные способы совершения преступлений, связанных с использованием информационно-телекоммуникационных технологий, и объединены в три группы: тактики и техники, применяющиеся злоумышленниками в ходе атак на операционные системы (в том числе корпоративные сети) «Windows», «macOS», «Linux», «Cloud», «Network» и пр. (группа «Enterprise») компьютеров; на мобильные устройства (группа «Mobile») и на промышленные системы управления (группа «ICS»).

Как ранее было отмечено, основу любой методики расследования составляет криминалистическая характеристика преступлений, которая базируется на типовой информационной модели, построение которой осуществляется путем обобщения сведений о криминалистически значимых признаках определенного вида преступления, которые, в свою очередь, формируются на основе анализа уголовных дел. Однако различные виды преступлений в сфере компьютерной

⁴⁷⁴ Яблоков Н. П. Обстановка совершения преступления как элемент его криминалистической характеристики. Указ. соч. С. 35.

информации могут совершаться одним и тем же способом, но с применением различных техник и тактик. С учетом сказанного, можно отметить, что матрица «Mitre Att&ck» по своей сути является отражением такого ключевого элемента криминалистической характеристики преступления в сфере компьютерной информации как «способ совершения преступления» и во всем своем многообразии техник, тактик совершения преступлений является полноценным отражением всех известных на текущий момент преступных деяний в сфере компьютерной информации.

Специалисты в области обеспечения информационной безопасности и противодействия рассматриваемым преступлениям используют вышеуказанные группы способов совершения преступлений для своевременного реагирования на инциденты, анализа существующей защиты на предмет соответствия реальным угрозам, а также оперативного расследования киберпреступлений, атрибуции атак, анализа деятельности преступников и отслеживания эволюции тактик и техник, которые применяют известные преступные группировки. Содержание матрицы «Mitre Att&ck» регулярно обновляется и служит фундаментальным источником актуальной информации о новых методах (способах) атак злоумышленников, позволяя адаптироваться к меняющемуся ландшафту киберугроз. На международном уровне матрицы «Mitre Att&ck» используют для декомпозиции преступлений на этапы, что позволяет систематизировать поиск и анализ цифровых доказательств (логи, артефакты памяти, данные сетевого трафика и пр.).

По этой причине выдвигается предположение о перспективности интеграции матриц «Mitre Att&ck» в инструменты анализа цифровых доказательств и системы противодействия преступлениям в сфере компьютерной информации, что позволит автоматически маркировать индикаторы компрометации и соотносить их с конкретными тактиками преступников. Кроме того, анализ повторяющихся атак способствует выявлению шаблонов совершения преступлений, что может использоваться для прогнозирования будущих атак и укрепления имеющихся средств защиты информации. В юридическом контексте это может служить доказательством систематичности противоправных действий. Использование матриц «Mitre Att&ck» обеспечивает соответствие требованиям допустимости доказательств (ст. 75 УПК РФ), так как структура матриц предоставляет стандартизированную методологию, признанную международным сообществом.

Таким образом, можно сделать вывод, что база данных «Mitre Att&ck» служит «мостом» между техническим анализом и юридической аргументацией и позволит сформировать кодовый набор, имеющий практическое значение для

правоприменения (позволяющий стандартизировать данные, автоматизировать анализ уголовных дел, точно квалифицировать противоправные деяния, обеспечить прозрачность и защиту обрабатываемых данных, а также предиктивный анализ).

В Российской Федерации ключевую роль в области обеспечения информационной безопасности играет ФСТЭК России. Указанная служба лицензирует деятельность в сфере защиты информации, сертифицирует средства защиты информации и с 2014 года и агрегирует банк данных угроз безопасности информации, который аккумулирует данные об уязвимостях программного обеспечения, используемого преимущественно в государственных структурах и на объектах критической информационной инфраструктуры РФ. Источниками пополнения данного банка являются публичные бюллетени производителей программного обеспечения. Реестр ориентирован на отечественных разработчиков и системных администраторов для оценки безопасности разрабатываемых ими продуктов.

Однако в сравнении с банком данных угроз безопасности информации ФСТЭК России матрицы «Mitre Att&ck» имеют ряд преимуществ: описывают тактики, техники и процедуры, используемые злоумышленниками на всех этапах кибератак, что позволяет прогнозировать их сценарии, укреплять защиту и эффективно расследовать инциденты, а не только перечислять возможные уязвимости; охватывают угрозы для информационной инфраструктуры всех стран (т. е. не только для программного обеспечения, используемого в Российской Федерации) и обновляется в режиме реального времени, отражая новейшие методы (способы) атак; интегрируются со многими разрабатываемыми в настоящее время инструментами расследования и моделирования атак, что позволяет автоматизировать обнаружение вторжений через сопоставление с тактиками матрицы и, соответственно, выстраивать проактивную защиту на основе анализа поведения злоумышленников.

Кроме того, матрица служит основой для обучения специалистов по кибербезопасности, помогая понять реальные сценарии атак, а не только выявлять уязвимости в программном обеспечении. Также она интегрирована со стандартом CVE⁴⁷⁵ (от англ. «common vulnerabilities and exposures» – база данных общеизвестных уязвимостей информационной безопасности корпорации Mitre) и

⁴⁷⁵ Стандарт наименования уязвимостей информационной безопасности «Common Vulnerabilities and Exposures – CVE» // Некоммерческая организация «Mitre» : офиц. сайт. URL: <https://msm.mitre.org/docs/cve-intro-handout.pdf> (дата обращения: 31.01.2025).

системой NIST Cybersecurity Framework⁴⁷⁶, что упрощает взаимодействие с глобальными базами угроз и расследование транснациональных киберпреступлений. Для юристов и правоведов матрица полезна при документировании атак, формировании доказательной базы (например, сопоставлении тактик с действиями конкретных хакерских групп) и оценке ущерба. Таким образом, база данных «Mitre Att&ck» является динамичным инструментом для оперативной работы со всеми возможными угрозами безопасности информации.

На основе вышеуказанного теоретико-правовыми основами классификации и последующего кодирования преступлений в сфере компьютерной информации могут выступить три уровня:

- уровень норм, представленных статьями, входящими в главу 28 УК РФ «Преступления в сфере компьютерной информации» (Таблица 2);
- уровень, представленный способами совершения противоправного деяния, в виде квалифицирующего признака, определяемого в соответствии с перечнем преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации (перечень 25), утвержденным указанием Генеральной прокуратуры Российской Федерации № 503/11 и МВД России № 1 от 28 июля 2025 г. (Таблица 3);
- уровень, отражающий тактику, приемы и методы (способы), используемые преступниками, а также возможности противодействия им, сформированный на базе матрицы «Mitre Att&ck» (Таблица 4).

Общий формат предлагаемой системы кодирования имеет вид:

[Категория преступления (Category Cx)] – [Метод (способ) совершения преступления (Method Mxxx)] – [Техника Mitre (Techniques Txxxx)] – [Подтехника Mitre (Sub-techniques Sxxx)] – [Способ обнаружения (вероятные места нахождения типичных следов преступления) (Detection Dxxxx)] – [Меры реагирования (меры противодействия, исключаяющие обстоятельства, способствовавшие совершению преступлений) (Reaction Rxxxx)].

⁴⁷⁶ Набор добровольных руководящих принципов кибербезопасности Национального института стандартов и технологий «NIST» // Национальный институт стандартов и технологий NIST: офиц. сайт. URL: <https://www.nist.gov/cyberframework> (дата обращения: 31.01.2025).

Таблица 2. – Система кодирования преступлений в сфере компьютерной информации

Статья УК РФ	Наименование преступления	Примеры преступлений	Код (Cx)
272	Неправомерный доступ к компьютерной информации	Взлом базы данных для кражи защищаемой информации, несанкционированный доступ к облачному хранилищу и пр.	C1
272.1	Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения	Сбор персональных данных граждан через фишинговые формы, продажа скомпрометированных персональных данных граждан на теневом рынке сети даркнет и пр.	C2
273	Создание, использование и распространение вредоносных компьютерных программ	Создание вируса-шифровальщика для атак на корпоративные сети, распространение ботнет-сетей и пр.	C3
274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	Утечка конфиденциальных из-за отсутствия шифрования данных, отказ в обслуживании из-за неправильной настройки сервера и пр.	C4
274.1	Неправомерное воздействие на критическую информационную инфраструктуру РФ	DDoS-атака на сервер объекта критической информационной инфраструктуры РФ, внедрение вредоносных программ в систему управления и пр.	C5
274.2	Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования	Отключение фильтров для блокировки запрещенного контента, манипуляции с настройками сетевых экранов и пр.	C6
274.3	Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции	Неправомерное использование GSM-шлюзов и SIM-боксов	C7
274.4	Организация деятельности по передаче абонентских номеров с нарушением требований законодательства РФ	Незаконный оборот SIM-карт	C8
274.5	Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям информационного ресурса	Незаконный оборот учетных данных (например, аккаунта WhatsApp и т. п.)	C9

Таблица 3. – Система кодирования методов (способов) совершения преступного деяния в соответствии с Перечнем преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации № 25

№ п/п	Метод (способ) совершения преступления	Код (Мxxx)
1.	Использование информационно-телекоммуникационной сети «Интернет»	М048
2.	Использование средств мобильной связи	М049
3.	Использование вредоносного программного обеспечения	М055
4.	Использование компьютерной техники	М057
5.	Использование программных средств (любое программное обеспечение, установленное на техническом средстве)	М059
6.	Использование фиктивных электронных платежей	М060
7.	Создание вредоносного программного обеспечения	М072
8.	Распространение вредоносного программного обеспечения	М073
9.	Использование социальных сетей	М086
10.	Использование интернет-мессенджеров	М087
11.	Использование электронных платежных систем	М088
12.	Операции с цифровой валютой	М089
13.	Использование SIP-телефонии	М092
14.	Неправомерный доступ к информации	М094
15.	Операции с цифровыми финансовыми активами	М095
16.	Использование сети даркнет	М126
17.	Фишинговые сайты и ссылки	М127
18.	Программы-шифровальщики	М128
19.	Бот-сети (ботнеты)	М130
20.	DDoS-атаки	М131
21.	Использование технологии «дипфейк»	М132
22.	Компрометация банковских устройств самообслуживания	М133
23.	Использование информационной инфраструктуры (зарубежных серверов (услуг хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменных зон, телефонных сетей и т. п.) иностранного государства	М134
24.	Использование информационной инфраструктуры стран-участников Содружества Независимых Государств	М135

Рассмотрим систему кодирования на примере преступления, связанного с несанкционированным завладением защищаемой информации (фишинг с утратой логина и пароля пользователя для доступа к интернет-мессенджеру с личного компьютера), в результате перехода по ссылке и установки владельцем аккаунта программного обеспечения, имитирующего в рассылке файл с его изображением (Таблица 4). Общий случай описания рассматриваемого преступления в соответствии с предлагаемой системой кодирования будет иметь вид: C1-M048-T1566-S001-D0015-R1021.

Расширенный вариант можно представить, например, следующим образом: C1 – [M048 / M049 / M055 / M059 / M073 / M087 / M094 / M127] – [[T1566-S001 - D0015 / D0022 / D0029 - R1021 / R1031 / R1049 / R1054 / R1017] / [T1586-S000 - D0021 / D0029 - R1056] / [T1659-S000 - D0009 / D0022 / D0029 - R1021 / R1041] / [T1528-S000 - D0002 - R1047 / R1017 / R1018 / R1021]].

Результаты проведенного сопоставления категорий преступлений в сфере компьютерной информации техникам матрицы «Mitre Att&ck» позволили сформировать систему универсального криминалистического кодирования преступлений (в значении упорядочивания и присвоения кодов), использование которой может выступить основой формирования эффективных методик их расследования в условиях эволюции способов совершения преступных деяний. Предлагаемая унификация как техника приведения к единообразию всех видов преступлений в сфере компьютерной информации также соответствует рекомендациям Будапештской конвенцией Совета Европы ETS 185, поскольку единые стандарты данных являются основой глобального противодействия киберугрозам.

Кодирование преступлений в сфере компьютерной информации представляет собой насущную необходимость в контексте динамично развивающегося цифрового пространства и создает предпосылки для ряда стратегически важных направлений развития уголовно-правовой практики. Таким образом, предлагаемая система кодирования преступлений способствует формированию единой системы, регулирующей не только ответственность за деяния, совершаемые в киберпространстве, выявление возможных связей личности преступника с предметом посягательства и личностью потерпевшего, но и возможные векторы атак, а также методы противодействия им. Обеспечивая предсказуемость правоприменения она создает основу для адаптации уголовного законодательства к постоянно меняющимся технологическим реалиям.

Таблица 4. – Пример описания фишинга с утратой логина и пароля пользователя в соответствии с системой кодирования

Уровень кодирования	Описание кода					
Код категории преступления (Category Cx)	C1 (неправомерный доступ к компьютерной информации)					
Метод (способ) совершения преступления * (Method Mxxx) *выявленные варианты	M048 Использование информационно-телекоммуникационной сети «Интернет», M-049 Использование средств мобильной связи, M-055 Использование вредоносного программного обеспечения, M-059 Использование программных средств) (любое программное обеспечение, установленное на техническом средстве), M-073 Распространение вредоносного программного обеспечения, M-087 Использование интернет-мессенджеров, M-094 Неправомерный доступ к информации, M-127 Фишинговые сайты и ссылки.					
Коды по матрице «Mitre Att&ck»	Техника (Techniques Txxxx)	Под-техника (Sub-technique Sxxx)	Способ обнаружения (вероятные места нахождения типичных следов преступления) (Detection Dxxxx)			Меры реагирования (меры противодействия, исключающие обстоятельства, способствовавшие совершению преступлений) (Reaction Rxxxx)
	T1566 фишинг	S001 целевой фишинг с вложением	D0015 журналы приложений (содержимое журналов приложений)	D0022 файл (создание файла)	D0029 сетевой трафик: содержимое сетевого трафика	R 1021 ограничения для веб-контента, R 1031 предотвращение сетевых вторжений, R 1049 антивирусное программное обеспечение, R 1054 изменение конфигурации программ, R1017 обучение пользователей
	T1586 компрометация учетных записей	S000	D0021 фиктивная личность (социальные сети, мессенджеры)	D0029 сетевой трафик (содержимое сетевого трафика)		R1056 пред-компрометация

Уровень кодирования	Описание кода					
	T1659 внедрение контента	S000	D0009 процесс (создание процесса)	D0022 файл (создание файла)	D0029 сетевой трафик: содержимое сетевого трафика	R1021 ограничения для веб-контента, R1041 шифрование важной информации
	T1528 кража токена доступа к приложению	S000	D0002 учетная запись пользователя (изменения в учетной записи)			R1047 аудит, R1017 обучение пользователей, R1018 управление учетными записями, R1021 ограничения для веб-контента.

В основе кодирования лежат признанные на международном уровне принципы, заложенные в матрице угроз безопасности информации, которая на постоянной основе обновляется путем внесения новых потенциально возможных тактик или техник (способов совершения преступления (с описанием типичных следов преступления, способов их сокрытия, вероятных мест их нахождения и распространенности (серийности) преступного деяния)). Таким образом, появляется механизм учета новых видов преступлений. Наличие подобного единообразного набора правил по учету преступлений может упростить международное сотрудничество в сфере борьбы с киберпреступностью, позволяя эффективнее обмениваться унифицированной информацией. Кроме того, возможно формирование аналогичных национальных матриц, раскрывающих техники и тактики (способы совершения преступлений), основанных на реально существующих инцидентах безопасности конкретной страны.

Предлагаемое решение (под которым здесь и далее по тексту в широком смысле понимается решение в области искусственного интеллекта в виде совокупности аппаратных и программных средств, предназначенных для выполнения с использованием технологий искусственного интеллекта прикладных задач, повышения эффективности определенного вида деятельности (расследования преступлений), а также для повышения производительности труда в контексте Указа Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации») позволяет обеспечить взаимосвязь обозначенных ранее структурных элементов криминалистической характеристики преступлений в сфере компьютерной информации (способа совершения

преступления (с описанием типичных следов преступления, способа их сокрытия, вероятных мест их нахождения и распространенности (серийности) преступления), обстановки совершения преступления, личности преступника, личности потерпевшего и предмета посягательства. Описываемое решение возможно реализовать в виде программного технико-криминалистического средства⁴⁷⁷, реализованного на основе:

1. Технологий искусственного интеллекта, в том числе на базе машинного обучения (метод глубокого обучения (сверточные нейронные сети (для анализа фото- и видеоданных, например, в целях распознавания лиц, объектов, выявления ключевых доказательств), рекуррентные сети (для исследования сетевого трафика, выявления подозрительной активности и пр.), трансформеры (для анализа текстовых данных, выявления контекста)), графовые сети (для детекции вредоносного программного обеспечения); обучение без учителя (кластеризация (для группирования схожих по структуре или содержанию данных) и аномальное обнаружение (для выявления отклонений от стандартного поведения в сети); обучение с подкреплением (для автоматизации расследования преступлений путем использования программных агентов, анализирующих инциденты безопасности); генеративный искусственный интеллект (для прогнозирования исхода расследования); объяснимый искусственный интеллект (для повышения уровня доверия к выдаваемым системой заключениям) и пр.);

2. Распределенных вычислений и облачных технологий (платформы для обработки больших данных (для исследования значительных объемов криминалистически значимой информации); облачные платформы (для анализа и хранения электронных доказательств, последующего масштабирования вычислительных ресурсов) и пр.);

3. Технологиях анализа данных: визуализация данных (для представления результатов анализа электронных доказательств в наглядном графическом виде, выявления взаимосвязей между файлами, сетевыми соединениями и пр.; реализация интерактивных информационных панелей (дашбордов), наглядно отображающих динамику изменений данных и т. п.

Предлагаемая система кодирования преступлений в сфере компьютерной информации, закладываемая в программное технико-криминалистическое

⁴⁷⁷ Свидетельство о государственной регистрации программы для ЭВМ № 2025682277 Российская Федерация. CyberCodex [КиберКодекс] – Программное технико-криминалистическое средство «Киберпреступность» с кодификатором преступлений в сфере компьютерной информации: № 2025680136 : заявл. 31.07.2025 : опубл. 22.08.2025.

средство, может представлять собой не только средство структурирования данных о преступных деяниях и упорядочения существующих их вариаций, но выступать стратегически важным шагом в создании эффективной системы противодействия преступности, способной оперативно адаптироваться к новым вызовам цифрового пространства. Система такого рода в дальнейшем сможет заложить новый вектор развития направления борьбы с преступлениями в сфере компьютерной информации в виде комплекса специальных знаний, сформированного на основе частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности и позволяющего определить наиболее подходящую, в соответствии со сложившимися обстоятельствами преступного деяния, методику расследования.

Стоит также отметить, что предлагаемый подход обеспечит процесс унификации расследования преступлений в сфере компьютерной информации благодаря заложенным в набор данных интеллектуальной системы алгоритмов действий для любой комбинаций тактик и техник совершения преступного деяния. Одновременно предлагаемая унификация может выступить базой данных для разработки программных технико-криминалистических средств, позволяя сформировать новый подвид криминалистического учета цифровых доказательств по аналогии с платформой «ТелекомЦерт»⁴⁷⁸ с возможностью учета векторов голосовых данных телефонных мошенников в виде уникальных математически преобразованных числовых форм. Кодирование рассматриваемых преступлений, одновременно выступая катализатором эволюции и развития технико-криминалистических средств, может создать условия для внедрения передовых методов и технологий, обеспечивающих достоверность, целостность и допустимость цифровых доказательств в суде. Также оно может способствовать стандартизации процедур поиска и собирания доказательств и обеспечению их юридической значимости.

Всякая исследовательская деятельность, связанная с систематизацией, направлена на выявление в объекте исследования элементов, структур и связей, что может значительно облегчить его изучение в целях решения поставленных задач. Основными объектами систематизации в криминалистике выступают знания, полученные в результате изучения преступной деятельности как в целом, так и ее

⁴⁷⁸ Единая государственная платформа по противодействию мошенничеству «ТелекомЦерт» // Информационно-аналитический центр стратегии использования радиочастотного спектра : офиц. сайт. URL: <https://rspectr.com/novosti/golosa-moshennikov-soberut-v-biometricheskoj-baze> (дата обращения: 04.04.2025).

отдельных видов механизма образования криминалистически значимой информации, а также совокупность разработанных на основе полученных знаний рекомендаций по выявлению, раскрытию, расследованию и предупреждению преступлений⁴⁷⁹. Криминалистическое кодирование, как процесс систематизации преступлений в сфере компьютерной информации, может являться основой формирования систем на основе искусственного интеллекта, которые объединят в себе юридические и технические аспекты расследования.

В качестве подтверждения выдвинутых гипотез необходимо дальнейшее рассмотрение особенностей расследования преступлений в сфере компьютерной информации с использованием программных технико-криминалистических средств, основ криминалистического исследования цифровой информации, а также типичных проблем и перспективных путей совершенствования деятельности по поиску и сбору цифровых доказательств. Изучение цифровой информации с применением специализированного программного обеспечения позволит выявить и исследовать следы преступной деятельности, тем самым обеспечивая доказательственную базу для уголовного преследования. Последовательное рассмотрение проблем и путей совершенствования деятельности по поиску и сбору цифровых доказательств приведет к формированию эффективной и адаптивной системы, способной противодействовать современным угрозам информационной безопасности, гарантируя соблюдение прав и законных интересов личности, общества и государства в цифровой среде.

Предлагаемый подход будет способствовать разработке новых и совершенствованию существующих программных технико-криминалистических средств на основе перспективных информационных технологий, а также методических рекомендаций по их применению в целях эффективного обнаружения, фиксации, изъятия и исследования цифровых доказательств, выявлению криминалистических средств, приемов и методов предупреждения преступлений, базирующихся на использовании цифровой информации, технических средств, средств защиты информации и пр., а также усовершенствованию тактики производства следственных действий и методик расследования преступлений, связанных с использованием компьютерной информации, средств ее обработки и защиты, что в совокупности является основными задачами в области противодействия преступлениям в сфере компьютерной информации.

⁴⁷⁹ Головин А. Ю. Криминалистическая систематика. Указ. соч. С. 40.

4.3. Правовые, методические, организационные и технические основы применения типовых алгоритмов расследования преступлений в сфере компьютерной информации

Процесс расследования, как разновидность поисково-познавательной деятельности, реализуется субъектами расследования путем производства следственных действий, проведения криминалистических операций, а также реализации оперативно-розыскных мероприятий. Без надлежащего планирования и организационного обеспечения указанная деятельность теряет свою направленность и структурированность, становясь малоэффективной.

Планирование расследования опирается на принципы индивидуальности (учет как общих, так и уникальных особенностей конкретного преступления, а также профессиональных навыков следователя), динамичности (необходимость постоянной адаптации плана к изменяющейся следственной ситуации), гипотетичности (построение и проверка следственных версий как основа познавательной деятельности) и реальности (обеспечение выполнимости запланированных мероприятий с использованием доступных ресурсов в установленные законом сроки)⁴⁸⁰.

К функциям планирования в уголовно-процессуальной деятельности можно отнести: моделирование, реализуемое в построении мысленной и материальной модели расследования, включающей следственные версии, задачи, способы их достижения, оперативно-розыскные мероприятия и криминалистические рекомендации; организационное управление, обеспечивающее возможность руководства ходом расследования, координации действий и контроля исполнения; упорядочение доказательств, направленное на сбор, систематизацию и логическую взаимосвязь доказательственной информации.

Как ранее было выявлено, при изучении методики расследования отдельных видов преступлений следует обращать внимание на типичные их признаки, имеющие криминалистическое значение⁴⁸¹ и на особенности конкретного вида преступного деяния, выражающиеся в способах их совершения, оставляемых при этом следах, профессиональных навыках преступника, особенностях личности потерпевшего и пр. т. е. на все то, что включается в криминалистическую

⁴⁸⁰ Яблоков Н. П., Александров И. В. Криминалистика : учебник. М. : Норма ИНФРА-М, 2017. С. 119.

⁴⁸¹ Возгрин И. А. Введение в криминалистику: история, основы теории, библиография. Санкт-Петербург, 2003. С. 293.

характеристику преступления⁴⁸².

Особенностью рассматриваемого вида преступлений является то, что начальная стадия их досудебного расследования, особенно в условиях неочевидности преступного события, характеризуется выраженным дефицитом исходной информации, необходимой для выдвижения и проверки следственных версий, позволяющих раскрыть содержание события и идентифицировать лицо, причастное к его совершению. Для восполнения указанного дефицита данных могут использоваться массивы сведений, содержащиеся в информационной модели (криминалистической характеристике) преступления, аналогичного расследуемому. Эти сведения, обладающие репрезентативностью в типологии, играют ключевую роль при формировании типичных следственных версий⁴⁸³. Как ранее было указано, невозможность формирования единого алгоритма расследования для всех преступлений одного вида требует создания частных методик, которые смогут учесть типичные следственные ситуации для каждого вида преступного деяния и в зависимости от них рекомендовать тот или иной вариант организации расследования.

Криминалистическая характеристика преступления с момента возбуждения уголовного дела и на протяжении всего расследования является ключевым инструментом организации деятельности следователя (дознателя), поскольку помогает выдвигать следственные версии, которые послужат основой планирования расследования, определять источники криминалистически значимой информации о преступлении и пр. Использование типовой криминалистической характеристики преступления требует от следователя (дознателя) высокого уровня профессиональных знаний, умений и навыков, которые могут, например, отсутствовать у молодых специалистов (следователей), что приведет к неэффективности соотнесения типовой криминалистической характеристики преступления и сообщения (заявления) о преступлении. Использование типовых следственных версий, выработанных в рамках криминалистической науки, позволяет следователю опираться на проверенные алгоритмы действий при планировании дальнейших этапов расследования. Корректное определение и классификация типичных следственных ситуаций в процессе разработки частных криминалистических методик расследования определенного вида преступления

⁴⁸² Митричев С. П. Методика расследования отдельных видов преступлений. Указ. соч. С. 13.

⁴⁸³ Грибунов О. П. Особенности версионной работы по делам о преступлениях против собственности, совершаемых на транспорте // Библиотека криминалиста. 2016. № 4 (27). С. 140.

дает возможность выработать более точные и практически применимые рекомендации, отчасти в виде алгоритмов. Это обеспечивает вариативность подходов к расследованию, их адаптацию под конкретные обстоятельства и повышает практическую ценность разработанных рекомендаций для следственной деятельности.

Чтобы грамотно спланировать расследование необходимо выстроить логически упорядоченную, целенаправленную и информационно-обоснованную структуру деятельности. Планирование расследования является весьма сложным вариативным мыслительным процессом, в ходе которого следователь формирует оптимальную модель достижения целей, а также определяет комплекс мероприятий, необходимых для их реализации. В криминалистической теории планирование признается универсальным методом рационализации следственной деятельности. Организационная и управленческая деятельность при расследовании преступлений базируется на компетентной оценке следственной ситуации, готовности участников расследования к деятельности и взаимодействию и требует наличия различных технико-криминалистических средств.

Все уровни организации и управления деятельности при расследовании взаимосвязаны, взаимозависимы и составляют организационно-управленческую сторону деятельности по расследованию преступлений как системы⁴⁸⁴, отвечающей принципам согласованности всех организационных действий, осуществляемых на различных уровнях системы расследования, соответствия компетенции следователя сложности расследуемого преступления, эффективного и рационального сочетания организационных, следственных, управленческих и иных действий.

С точки зрения теории алгоритмов общепринятым способом его записи являются графическая форма с помощью блок-схем, а также соответствующая им символьная запись с помощью алгоритмического языка⁴⁸⁵. Но, например, применительно к алгоритмам на основе искусственного интеллекта в настоящее время чаще всего используются языки программирования, такие как «Python», «R», «Java», «C++», «Julia» и др. Большим преимуществом интеллектуальных систем является возможность их построения на основе алгоритмов прогрессивного обучения, которые выступают в процессе работы классификатором или

⁴⁸⁴ Яблоков Н. П., Александров И. В. Криминалистика. Указ. соч. С. 215.

⁴⁸⁵ Трофимов В. В., Павловская Т. А. Алгоритмизация и программирование : монография. М. : Юрайт, 2024. С. 8.

предикатором⁴⁸⁶, что, например, может быть довольно важно в условиях острого недостатка информации о событии преступления и лицах его совершивших, а также при необходимости поддержания динамичности программы расследования (переобучения алгоритма) при появлении новой криминалистически значимой информации.

С точки зрения материального выражения информационно-компьютерной модели преступления план расследования может воплощаться в виде алгоритма действий в графическом виде, представляющего собой логическую модель предпринимаемых действий. Планирование расследования ориентировано на построение логической схемы расследования, при этом реализацией этого плана с учетом сложившихся условий является организация расследования. В практике расследования моделирование преступного деяния и его планирование осуществляются на основе следственной ситуации.

В свете построения информационной модели преступления с позиции криминалистической ситуалогии и теории принятия решений алгоритм построения плана расследования сводится к рассмотрению конкретной сложившейся ситуации, подбору типовой информационной модели преступления, максимально схожей с условиями сложившейся ситуации, выбору в наибольшей степени соответствующей обстоятельствам конкретного дела типовой методики его расследования, а также типовой следственной ситуации и версий, на базе которых выдвигается рабочая версия и составляется план расследования⁴⁸⁷.

По аналогии, планирование расследования в машиночитаемой форме может представлять собой алгоритмизацию работы программы. Так, например, обеспечить процесс эффективного принятия решения в той или иной следственной ситуации возможно на основе алгоритма «дерева решений»⁴⁸⁸, который позволяет наглядно представить вариант решения задачи методами машинного обучения в виде древовидной структуры и помогает систематизировать варианты выбора, а также возможные их последствия.

Разновидностью так называемых «мягких вычислений» (от англ. «soft computing» – методология использования неточных и «нестрогих» обоснованных

⁴⁸⁶ Остроух А. В. Введение в искусственный интеллект : монография. Красноярск : Научно-инновационный центр, 2020. С. 22.

⁴⁸⁷ Ищенко Е. П., Колдин В. Я. Типовая информационная модель преступления как основа методики расследования. Указ. соч. С. 132.

⁴⁸⁸ Venkateshwarprasad K. Sashirekha K. Efficient prediction of cybercrime breaches using decision tree compared with Naive Bayes with improved accuracy // AIP Conf. Proc. 2025. №3270 (1). P. 20.

математически методов и алгоритмов решения задач, для которых не существует строгих подходов, позволяющих получить точный результат за ограниченное время) являются эволюционные алгоритмы, которые включают в себя интеллектуальные методы обработки данных, нечеткую логику и вероятностные рассуждения, что соответствует по своей сути эвристическим криминалистическим алгоритмам.

Основной проблемой алгоритмизации процесса расследования преступлений в сфере компьютерной информации является то, что в основу функционирования алгоритма необходимо заложить предписание, которое задает вычислительный процесс, начинающийся с совокупности возможных для данного алгоритма исходных данных, и направленный на получение полностью определяемого этим исходным данным результата. Исходными данными для алгоритмизации рассматриваемого вида преступлений должны выступить выявленные элементы их криминалистической характеристики.

По преступлениям в сфере компьютерной информации способ совершения преступления, как исходный вектор, влияет на тип оставляемых цифровых следов. Цифровые следы, в свою очередь, обнаруживаются использованием программных технико-криминалистических средств, которые определяют методику расследования, алгоритм действий для поиска и собирания доказательств и их дальнейшей юридической интерпретации. По этой причине из всей совокупности элементов криминалистической характеристики преступного деяния основной упор при алгоритмизации необходимо делать на способ совершения преступления в соответствии с матрицей угроз безопасности информации, например, «Mitre Att&ck», которая на постоянной основе обновляется путем внесения новых потенциально возможных уязвимостей в технических средствах, что является их большим преимуществом, т. к. благодаря постоянной актуализации указанной базы данных появляется механизм учета вновь появляющихся видов преступлений.

Как показал проведенный структурно-содержательный анализ элементы криминалистических характеристик преступлений в сфере компьютерной информации могут в некоторой степени совпадать, но отличаться частностями, которые существенно позволяют повысить точность алгоритма работы интеллектуальных моделей и выдачи ими результатов. Это объясняется тем, что при обучении систем на основе искусственного интеллекта используются наборы данных, которые содержат сведения с результатами решения поставленных задач, при этом отбираются наиболее значимые для выдачи результата критерии.

Качество алгоритма зависит от данных, на которых он обучен, что говорит о важности разнообразия в наборе обучающих данных. В общем случае алгоритмы искусственного интеллекта используют обучающий набор в качестве входных данных, который содержит совокупность переменных в виде значимых признаков.

Каждый обучающий пример в датасете содержит переменную результата, которая отражает верное решение.

Чем больше и разнообразнее набор обучающих данных (за исключением эффекта переобучения), тем лучше она распознает закономерности в них и тем точнее она выдает решения.

Выделение элементов криминалистических характеристик преступлений выступает важнейшим этапом машинного обучения, который требует значительных усилий, связанных с получением данных для моделирования, извлечением и компоновкой наиболее значимых признаков. Кроме того, элементы криминалистических характеристик могут выступить основой для структурирования обучающего датасета, позволяющего получить более полную информационную модель преступного деяния, что будет способствовать формированию более точного алгоритма его расследования.

Детализация способов совершения преступлений, в свою очередь, формирует основу для построения цифровой модели преступления в сфере компьютерной информации (цифрового двойника преступления), которая позволит моделировать полную структуру преступной деятельности (подготовка, совершение и сокрытие преступления), а также ход расследования в цифровом виде, на основе предварительно обученных алгоритмов искусственного интеллекта, при этом анализируя взаимосвязи путем сопоставления способов совершения преступлений (тактик) со средствами совершения преступлений (техниками и подтехниками), оставляющими цифровые следы.

Проведенный обзор имеющейся научной литературы в области алгоритмизации и программирования процесса расследования преступлений позволил сделать вывод, что в большинстве своем (за исключением ряда авторов) под алгоритмом и программой понимают порядок деятельности (план) в словесной форме, учитывающий динамику следственной ситуации и возможные ее трансформации.

Формы плана расследования, в свою очередь, могут быть мысленными, письменными и графическими, в то время как наиболее известными способами представления алгоритмов являются формы в виде ⁴⁸⁹:

- словесного описания (на естественном языке);
- программы (на языке программирования);
- псевдокода (на неформальном императивном языке программирования с использованием ключевых слов и исключением несущественных для понимания подробностей);
- графической блок-схемы или диаграммы (структурной блок-схемы).

Наиболее наглядной из всех описанных выше форм является форма представления алгоритма в виде блок-схемы. Действия преступника определяют способ совершения преступления, который выражается определенным набором тактик, техник и подтехник по матрице «Mitre Att&ck». Тот или иной набор тактик и техник совершения преступления в совокупности (в качестве описания средства и механизма совершения преступления) определяет сложившуюся следственную ситуацию, состав преступления (базу расследования) и предмет доказывания по нему (цель расследования). Кроме того, способ совершения преступного деяния определяет соответствующие ему следы, методы реагирования на компьютерный инцидент в целом и, соответственно, методику обнаружения, фиксации, собирания и исследования цифровых доказательств (изложено в соответствии с предложенной системой кодирования преступлений в сфере компьютерной информации). При этом важна первоочередность выявления категории преступного деяния в предлагаемой системе кодирования, что вполне объясняется разницей в объекте преступного посягательства и тем, что одним и тем же набором техник и подтехник можно совершить, например, неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также незаконный сбор или использование информации, содержащей персональные данные граждан (ст. 272.1 УК РФ).

В таком случае, общим для всех преступлений определенной группы выступит алгоритм расследования в соответствии с делением на категории преступлений в родовой группе (Сх), способы совершения этих преступлений (техники (Тхxxx) и подтехники (Sxxx)), способы обнаружения следов преступления (Dxxxx) и меры противодействия (Rxxx) расследованию (Рисунок 1) [уровень 0].

⁴⁸⁹ Cormen T. H., Leiserson C. E., Rivest R. L. Introduction to algorithms. London : Massachusetts institute of technology. P. 6.



Рисунок 1 – Общий алгоритм расследования преступлений
в сфере компьютерной информации [уровень 0]

Для дальнейшего анализа целесообразно также учесть, что способы совершения преступления в сфере компьютерной информации условно можно классифицировать по объекту воздействия, по доступу к объекту воздействия, уровню автоматизации и мотиву воздействия и т. д. (подробно эти способы раскрыты в параграфе 1.2), что в совокупности определит четыре отдельных направления ветвления алгоритма расследования преступления (например, древовидной или простой разветвляющейся формы) с соответствующими им техниками и подтехниками совершения преступлений [уровень 1] или их совокупности (Рисунок 2).

Как было указано ранее, систематизацию частных криминалистических методик целесообразно строить на основе криминалистических характеристик преступлений. Именно поэтому информационной базой для разработки методики расследования послужил один из важнейших элементов криминалистической характеристики преступлений – способ совершения преступлений.

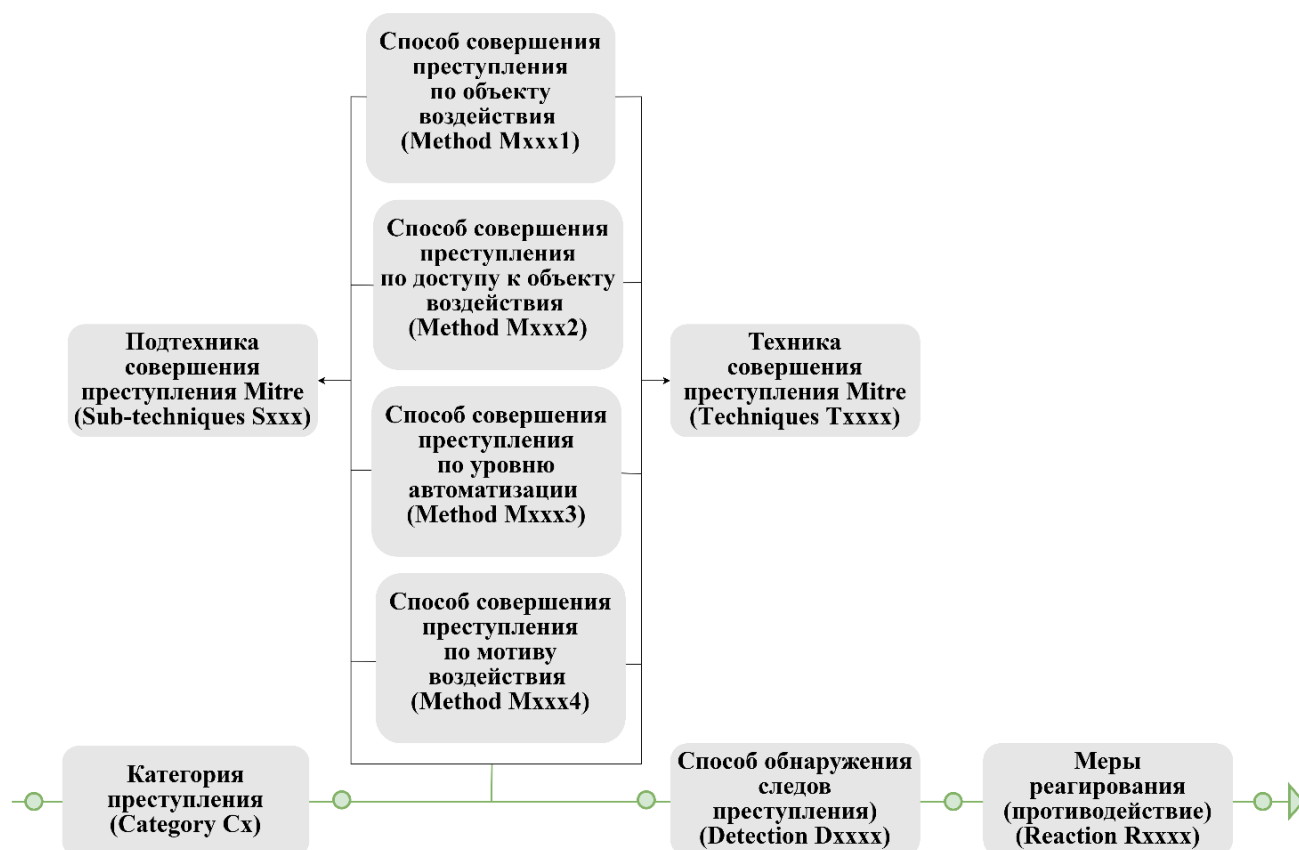


Рисунок 2 – Алгоритм расследования преступлений с учетом способов совершения преступления [уровень 1]

Дальнейший процесс алгоритмизации необходимо выстраивать как с учетом уголовно-правового основания, так и отличительной особенности преступления в сфере компьютерной информации, заключающейся в том, что состав элементов криминалистических характеристик рассматриваемых преступных деяний может в некоторой степени совпадать (Рисунок 3) [уровень 2].

Последним определяющим алгоритмом для цифровой модели преступного деяния выступает алгоритм расследования в соответствии с известными методиками расследования конкретного преступного деяния [уровень 3], которые были рассмотрены ранее. В основе реализуемой информационной системы в виде цифровой модели преступного деяния должен лежать датасет (от англ. «dataset» – набор данных) в виде структурированного (с четкой определенной организацией данных), неструктурированного или гибридного типа набора данных, организованного для целей расследования, по сути представляющего из себя некий классификатор проблемных ситуаций⁴⁹⁰, позволяющих адекватно описывать следственную обстановку, следственную ситуацию и возможные направления расследования преступлений.

⁴⁹⁰ Волчецкая Т. С. Криминалистическая ситуалогия. Указ. соч. С. 198.

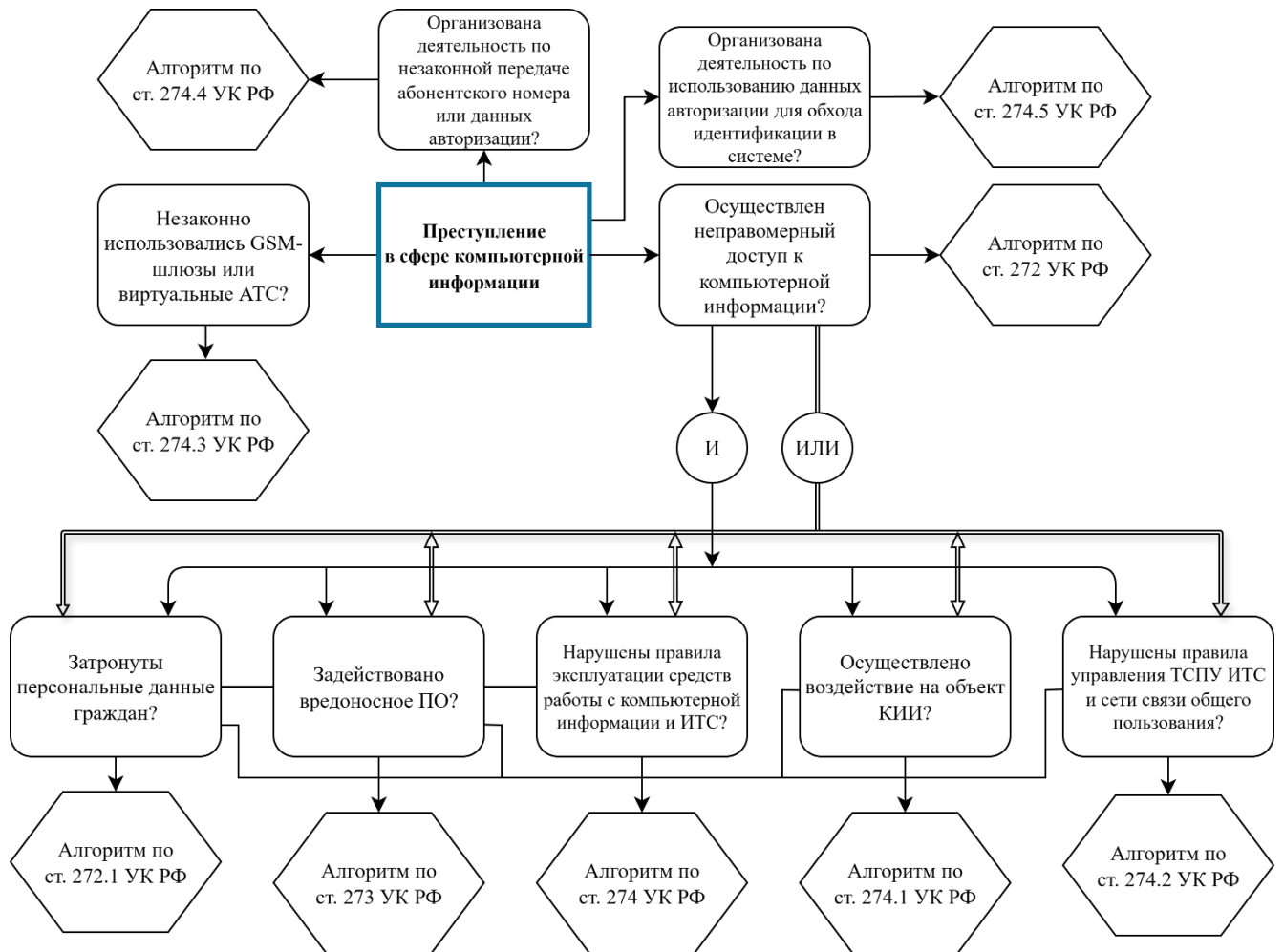


Рисунок 3 – Алгоритм расследования с учетом уголовно-правового основания [уровень 2]

Создание набора данных для формируемой информационно-компьютерной модели преступного деяния является важным этапом на пути к оцифровке признаков преступления и последующего их анализа на основе искусственного интеллекта и соответствует процедуре кодирования преступлений в сфере компьютерной информации.

Согласно теории криминалистической ситуалогии создание такого рода классификаторов (наборов кодов) является важной задачей, способной сформировать единый «междисциплинарный» язык взаимодействия между криминалистикой, логикой, математикой, математической статистикой, анализом данных, теорией принятия решений, машинным обучением, программированием, системным анализом и пр.

Использование единого междисциплинарного языка взаимодействия позволит объединить результаты большого количества разнородных исследований сформированных по настоящее время в области криминалистики в одну систему криминалистического знания и использовать ее на базе средств вычислительной техники для инженерного проектирования сложных информационных систем с возможностью поддержки принятия решений на основе искусственного интеллекта, последующей динамичной оптимизацией процесса расследования преступлений, выявления корреляционных связей между элементами криминалистической характеристики преступлений, моделирования следственных версий, типичных следственных ситуаций и алгоритмов расследования⁴⁹¹, формирования значительного массива криминалистически значимой информации, новых криминалистических учетов, их обработки и использования в профессиональной деятельности следователей, дознавателей, оперативных сотрудников и экспертов.

Отправной точкой алгоритмизации процесса расследования преступлений в сфере компьютерной информации и процесса поддержки принятия решений по уголовному делу должностным лицом может стать, например, процесс получения объяснений. Не преумалая достоинства такого следственного действия как допрос, требующего тщательной предварительной подготовки и затрат времени, в целях оперативного получения информации о преступном деянии от потерпевших по преступлениям в сфере компьютерной информации предполагается допустимым получение объяснений по факту совершения преступления и возможности их альтернативного представления удаленно посредством сети «Интернет» по специально разработанной форме, отражающей типичные следственные ситуации, и реализованной в виде информационной системы на основе искусственного интеллекта. Такой подход, по аналогии с алгоритмизацией процесса допроса⁴⁹², позволит не только снизить временные затраты на процесс подачи заявления о

⁴⁹¹ Волчецкая Т. С. Криминалистическая ситуалогия. Указ. соч. С. 203.

⁴⁹² Скоревич А. С., Кулаевский А. В. Теоретическое и эмпирическое исследование алгоритмизации тактики проведения коммуникативных следственных действий // Вестник Томского государственного университета. 2023. № 490. С. 207; Долинин В. Н. Гибкие алгоритмы применения тактических приемов в процессе допроса в бесконфликтной и конфликтной ситуациях // Вклад Л. Я. Драпкина в криминалистическую науку. Екатеринбург : ФГБОУ ВО Уральский государственный юридический университет, 2019. С. 111; Головин М. В., Шпак Н. М. Алгоритмизация следственных действий на первоначальном этапе расследования вымогательства // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2016. № 123. С. 935; Глоба В. В. Допустимость использования тактических приемов допроса обвиняемого (подозреваемого) : 5.1.4 «Уголовно-правовые науки» : дис. ... канд. юрид. наук. Краснодар, 2025. С.13.

преступном деянии, но и автоматизировать процесс обработки криминалистически значимой информации. Однако для снятия противоречий и разрешения дискуссионных вопросов, связанных с получением объяснений, необходимо четко определить порядок получения объяснений. Следует при этом закрепить, что объяснения могут быть получены от лиц как в устном и письменном виде⁴⁹³, так и в альтернативном электронном.

Устные объяснения при этом должны заноситься в протокол, а письменная и электронная их форма требует введения отдельной нормы, регламентирующей порядок получения таких объяснений, что в значительной степени позволило бы урегулировать процедуру получения криминалистически значимой информации.

Так, допрашиваемое лицо может представлять интерес для следователя как личность, как слеодообразующий объект, как участник или очевидец преступного деяния и пр. При установлении категорий, входящих в предмет вербального следственного действия по конкретному преступлению, можно сформировать универсальный алгоритм его проведения. Разнородность данных при этом можно учесть методами семантического анализа больших языковых моделей⁴⁹⁴ (от англ. «large language model» – большая языковая модель) для интерпретации смысла текста, учета контекста и генерации контекстно-адекватных ответов, алгоритмами мультимодальных нейросетей и ХАИ-систем (объяснимого искусственного интеллекта)⁴⁹⁵, методами обработки естественного языка и распознавания контекстуальных связей. Указанным устанавливается цель перевода хотя бы части вербальных действий в невербальные, а именно в невербально-цифровые с возможностью их дальнейшей обработки в цифровом виде.

Таким образом, сложившаяся ситуация, связанная со сложностью раскрытия преступлений в сфере компьютерной информации, благодаря своей опосредованности с цифровой формой информации может выступить катализатором внедрения технологии искусственного интеллекта в практику расследования благодаря не только количественной обработке данных (анализ числовых данных с помощью статистических методов и численных алгоритмов), но и технологии распознавания и обработки устной и письменной человеческой

⁴⁹³ Герасенков В. М. Объяснения как источник доказательств в уголовном процессе // Экономика. Социология. Право, 2023. № 3 (31). С. 97.

⁴⁹⁴ Xiao T., Zhu J. Foundations of large language models. NLP lab. Boston : Northeastern university & Niutrans research, 2025. P. 36.

⁴⁹⁵ Мишра П. Объяснимые модели искусственного интеллекта на Python. Модель искусственного интеллекта. Объяснения с использованием библиотек, расширений и фреймворков на основе языка Python. М. : ДМК Пресс, 2022. С. 17.

речи NLP (от англ. «natural language processing» – обработка естественного языка)⁴⁹⁶.

Примером алгоритмизации такого действия как получение объяснений может выступить процесс обработки данных, предоставляемых заявителем по факту совершенного преступления в сфере компьютерной информации в специально разработанной информационной системе. При этом приобщаемыми к заявлению цифровыми данными могут являться текстовая информация, аудио- и видеозаписи, метаданные, программное обеспечение и т. д.)⁴⁹⁷.

Стоит прежде отметить зарубежный опыт функционирования систем, обеспечивающих прием сообщений от потерпевших по делам о киберпреступлениях, например, Центр приема заявлений о преступлениях в сети «Интернет» в подразделениях Федерального бюро расследований США IC3⁴⁹⁸. Главной задачей центра IC3 является оказание помощи потерпевшим в составлении и подаче сообщения о преступлении посредством специальной электронной формы, представляющей из себя алгоритм, по которому лицо, потерпевшее от преступления, должно изложить сведения об обстоятельствах произошедшего и криминалистически значимых фактах (Приложение 5). Поступившее в Центр IC3 заявление после первичной автоматизированной обработки данных анализируется профильными специалистами и при наличии достаточных оснований перенаправляется в компетентные органы по подследственности.

Подобные системы функционируют и в ряде стран Европы, например в едином центре по борьбе с киберпреступностью ЕС3⁴⁹⁹, а также в Национальном центре по борьбе с мошенничеством и киберпреступностью «Action Fraud» Великобритании⁵⁰⁰, центре кибербезопасности Австралии «ACSC»⁵⁰¹, который, выступая в роли негосударственной организации,

⁴⁹⁶ Гольдберг Й. Нейросетевые методы в обработке естественного языка. М. : ДМК Пресс, 2019. С. 13.

⁴⁹⁷ Смушкин А. Б. Концепция дистанционной криминалистики: монография / под ред. В. Б. Вехова. М. : Юрлитинформ, 2024. С. 175.

⁴⁹⁸ Центр приема сообщений о преступлениях в сети «Интернет» Internet crime complaint center (IC3) // Центр IC3 Федерального бюро расследований США : офиц. сайт. URL: <https://www.ic3.gov> (дата обращения: 07.05.2025).

⁴⁹⁹ Центр приема сообщений о преступлениях Европейского центра по борьбе с киберпреступностью (ЕС3) // Центр ЕС3 полицейской службы Европейского союза (Европол) : офиц. сайт. URL: <https://www.europol.europa.eu/report-a-crime> (дата обращения: 07.05.2025).

⁵⁰⁰ Национальный центр по борьбе с мошенничеством и киберпреступностью Action Fraud // Центр Action Fraud Великобритании : офиц. сайт. URL: <https://www.actionfraud.police.uk> (дата обращения: 07.05.2025).

⁵⁰¹ Центр кибербезопасности Australian Cyber Security Centre // Центр ACSC Австралии : офиц. сайт. URL: <https://www.cyber.gov.au/acsc/report> (дата обращения: 27.05.2025).

содействует реализации прав потерпевших, обеспечивая первичную обработку поступающих сведений.

Аналогичный координационный центр по борьбе с киберпреступлениями функционирует в Индии (I4C)⁵⁰², который включает в себя национальный портал по отчетности о преступлениях. Входящие в его состав аналитические и судебно-экспертные подразделения используют технологии искусственного интеллекта для анализа поступающих сообщений о преступлениях от граждан посредством интеллектуального чат-бота, что позволяет сократить время ожидания рассмотрения обращений и повысить эффективность реагирования на киберпреступления⁵⁰³.

Таким образом, подобные информационные системы эффективно выполняют ряд насущных для современного положения сферы противодействия преступности в сфере компьютерной информации задач, включающих:

- упрощение процедуры подачи сообщения (заявления) о преступлении в формате 24/7, предоставляя доступные алгоритмы действий для потерпевших относительно того, какие именно сведения необходимо изложить, и в какой последовательности;
- снижение нагрузки на правоохранительных органы;
- аккумулярование значительного массива криминалистически значимой компьютерной информации, которая подвергается обработке с применением алгоритмов искусственного интеллекта и позволяет практически мгновенно выявлять взаимосвязи между элементами криминалистической характеристики схожих преступных деяний, распространенность преступлений по определенным признакам и пр.

Процесс подачи заявления по факту совершения преступного деяния для потерпевшего может состоять из следующих этапов (Приложение 5):

1. Переход на официальный сайт системы подачи заявления о преступлении в сфере компьютерной информации;
2. Заполнение сведений о преступлении (выбор категории из выпадающего

⁵⁰² Координационный центр по киберпреступлениям Indian Cybercrime Coordination Centre I4C // Центр Министерства внутренних дел правительства Индии : офиц. сайт. URL: <https://i4c.mha.gov.in> (дата обращения: 07.05.2025).

⁵⁰³ О вводе в эксплуатацию интеллектуального чат-бота AI на горячую линию по принятию заявлений о киберпреступности // Портал Indiatimes группы компаний Times Group : офиц. сайт. URL: https://timesofindia.indiatimes.com/city/hyderabad/telangana-adds-ai-chatbot-to-cybercrime-helpline-193Q-to-speed-up-help-in-golden-hour/articleshow/120939276.cms?utm_source=chatgpt.coir (дата обращения: 07.05.2025).

меню);

3. Заполнение сведений о заявителе (контактные данные, сведения об идентификационных данных технических средств, программном обеспечении, электронных средствах платежа и пр. (при наличии));

4. Заполнение сведений о возможном преступнике и механизме преступления (сведения об идентификационных данных технических средств, программном обеспечении, электронных средствах платежа, абонентских номерах, информационных ресурсах, веб-адресах, задействованных со стороны субъекта преступления и пр.);

5. Заполнение сведений о последствиях преступления, нанесенном заявителю ущербе, о совершенных транзакциях и манипуляциях (по категориям);

6. Заполнение текстовой формы о компьютерном инциденте в свободной форме;

7. Заполнение дополнительных сведений (о свидетелях или очевидцах преступления, о наличии цифровых доказательств (копии переписки с преступником, аудиозаписи телефонного звонка, фотографии и видеозаписи с камер видеонаблюдения, лог-файлы функционирования программного обеспечения или информационных систем, чеки и справки о транзакциях и финансовых операциях, иные документы в электронном виде, имеющие криминалистическое значение) по факту совершенного преступного деяния и пр. с возможностью их оперативной загрузки в систему);

8. Подписание соглашения о конфиденциальности, объективности и полноте представленных данных;

9. Направление заявления (сообщения) о преступлении с получением копии направленного обращения на указанный заявителем электронный адрес.

По аналогии с действующими за рубежом системами целесообразно рассмотреть возможность подачи анонимного заявления в случае нежелания раскрытия информации о потерпевшем, что, например, снизит приоритет в расследовании, но обеспечит учет полученных сведений, сопоставление новых сведений о преступлениях с существующими делами и формирование данных о серийности преступлений. Эффективность деятельности подобных систем и служб, обеспечивающих их функционирование, подтверждается конкретными эмпирическими данными, так, было установлено, что уровень регистрации сообщений о киберпреступлениях, где функционируют такого рода информационные системы, существенно выше, чем в странах, не имеющих

аналогичной практики⁵⁰⁴.

В аналитическом отчете центра IC3 Федерального бюро расследований США отмечено⁵⁰⁵, что за 25-летний период деятельности организацией было получено свыше 9 млн. сообщений о киберпреступлениях, а за 2024 год поступило более 859 тыс. сообщений. При этом, если на момент становления системы Центр IC3 получал около 2 тыс. жалоб каждый месяц, то за последние пять лет сохраняется тенденция получения более 2 тыс. жалоб в среднем ежедневно. Таким образом, основной целью подобных систем является создание удобного механизма для приема и анализа информации о предполагаемых преступлениях. С учетом вышеизложенного, подобная практика представляется весьма эффективной, при этом стоит отметить, что ее взаимосвязь с подачей заявлений о преступлении с единого портала государственных и муниципальных услуг «Госуслуги»⁵⁰⁶ и предоставлением информации путем первичной авторизации на указанном сайте не всегда будет эффективна, что подтверждает проведенный анализ судебно-следственной практики и статистической отчетности, который показал наиболее часто встречающийся вид неправомерного доступа к компьютерной информации, представляющий собой взлом аккаунта на портале (около 90 % от всех зарегистрированных преступлений, предусмотренных ст. 272 УК РФ в 2024 году)⁵⁰⁷ с последующей утерей доступа к нему.

По этой причине предлагаемая информационная система может быть схожей с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) Национального координационного центра по компьютерным инцидентам, но представленной в упрощенном виде, обеспечивающем прием и обработку сообщений (заявлений) о преступлениях в сфере компьютерной информации, а

⁵⁰⁴ Жижина М. В., Завьялова Д. В. Возбуждение уголовного дела по факту преступления в сфере компьютерной информации: российский и зарубежный опыт // Актуальные проблемы российского права. 2021. № 12 (133). С. 158.

⁵⁰⁵ Отчет о преступности в сети «Интернет» : аналитический обзор Центра приема сообщений о преступлениях в сети «Интернет» IC3 // Центр IC3 Федерального бюро расследований США: офиц. сайт. URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3_Report.pdf (дата обращения: 07.05.2025).

⁵⁰⁶ О возможности подачи заявления о киберпреступлении через портал «Госуслуги» // Акционерное общество Интерфакс : офиц. сайт. URL: <https://www.interfax.ru/russia/1021371> (дата обращения: 07.05.2025).

⁵⁰⁷ О раскрываемости преступлений со взломом аккаунтов // Федеральное государственное унитарное предприятие «Информационное телеграфное агентство России (ИТАР-ТАСС)» : офиц. сайт. URL: <https://tass.ru/obschestvo/24104331> (дата обращения: 07.05.2025).

также первичный их анализ в автоматическом виде и последующий – в автоматизированном виде с задействованием специалиста узкого профиля, сонаправленного технике совершения преступления. Указанное позволило бы оказывать действенную поддержку потерпевшим наряду с минимизацией процессуальных ошибок, допускаемых на стадии доследственной проверки, например, из-за возможной некомпетентности сотрудника.

Далее необходимо рассмотреть ряд организационно-технических особенностей, связанных с реализацией систем, обеспечивающих прием заявлений (сообщений) о преступлениях, а также дальнейшую их интеллектуальную обработку, построение на основе первичных полученных данных типичной следственной ситуации и прототипа (первоначальный образ, прообраз) цифрового двойника преступного деяния и формирование на его основе наиболее эффективного алгоритма расследования. Одной из основных целей информационных технологий является получение и предоставление информации для ее анализа и дальнейшего использования человеком при принятии решений. Все технологии представлены многоуровневым распределением известных подходов к работе с цифровыми данными, а также технических средств, предназначенных для работы с электронной информацией, по мере их усложнения, которые с учетом развития науки и техники постоянно развиваются и совершенствуются⁵⁰⁸.

На первом (нижнем) уровне многоуровневой классификации информационных технологий представлены простейшие технологии взаимодействия человека с электронной вычислительной машиной, которые обеспечивают ввод и представление данных в электронном виде (операционные системы, технологии алгоритмизации, программирования и тестирования, шифрования и кодирования данных).

На втором уровне располагаются технологии, служащие задачам регистрации и хранения данных, а также информационные технологии, возникшие в результате развития сети «Интернет», в том числе облачные технологии и технологии мультимедиа (технологии создания баз данных, систем управления базами данных (СУБД), технологии формирования хранилищ данных и пр.).

На последующих двух уровнях (3 и 4) размещены технологии поиска и обработки цифровых данных в различном их представлении, в том числе OLTP-технологии (от англ. «online transaction processing» – обработка транзакций

⁵⁰⁸ Моделирование систем и процессов. / под ред. В. Н. Волкова. М. : Юрайт, 2025. С. 33.

в реальном времени) для реализации информационных систем, обеспечивающих постоянное обновление баз данных.

На пятом уровне представлены ИТ, обеспечивающие сложную обработку информации и ее подготовку для принятия решений: «OLAP»-технологии (от англ. «online analytical processing» – оперативная аналитическая обработка данных), обеспечивающие анализ данных в реальном времени и формирование наборов структурированных данных (витрин данных); технологии «data science», как междисциплинарная область на стыке аналитики, статистики, математики, программирования, системного анализа и машинного обучения, охватывающая все этапы работы с данными (от англ. «data science» – раздел компьютерных наук, изучающий проблемы анализа, обработки и представления данных в цифровой форме), в том числе технологии извлечения знаний из баз данных и поиска значимых сведений в неструктурированных данных «KDD» (от англ. «knowledge discovery in databases» – обнаружение знаний в базах данных) и технологии извлечения полезной информации из больших объемов данных data mining (от англ. «data mining» – добыча данных); технологии структурного анализа и проектирования функциональных моделей объекта какой-либо предметной области «SADT» (от англ. «structured analysis and design technique» – методология структурного анализа и проектирования) и разработанные на ее основе концепции оперативной разработки программного обеспечения «RAD» (от англ. «rapid application development» – быстрая разработка приложений) и автоматизации разработки программного обеспечения на базе «CASE»-технологий (от англ. «computer-aided software engineering» – автоматизированная разработка программного обеспечения); технологии имитационного моделирования для анализа и прогнозирования поведения сложных информационных систем, трудно описываемых с помощью аналитических методов.

На шестом уровне размещены технологии различного рода и назначения, например, для реализации классических информационных систем, автоматизированных информационных систем, автоматизированных систем управления, предметно-ориентированных и корпоративных систем, информационно-поисковых систем, документальных, фактографических, а также, например, гибридных документально-фактографических, автоматизированных документально-фактографических информационно-поисковых систем, автоматизированных систем нормативно-методического обеспечения управления и пр. Необходимо отметить, что в настоящее время в области криминалистики

имеется достаточно технико-криминалистических средств, функционирующих на основе указанных технологий, в отличие от последующего (верхнего) уровня.

На верхнем для текущего этапа развития науки и техники уровне расположены так называемые «эмерджентные технологии» (от англ. «emerging technologies» – появляющиеся технологии), сформированные появлением новых свойств в результате объединения существующих информационных технологий на нижестоящих уровнях рассматриваемой классификации, к которым относятся технологии обработки данных, приближающиеся к интеллектуальным функциям человека.

Данный уровень представлен также интернет-технологиями, конвергентными НБИК-технологиями (по первым буквам областей от англ. и русс. «nano(technology)» – нанотехнологии, «bio(technology)» – биотехнологии, «info(technology)» – информационные технологии, «cogno(technology)» – когнитивные технологии), а также интеллектуальными информационными технологиями, которые выступают средством разработки интеллектуальных систем.

Под интеллектуальными информационными системами понимают автоматизированные системы, основанные на некой базе знаний, или комплексе программных, лингвистических и логико-математических средств для реализации основной задачи – осуществления поддержки деятельности человека и поиска информации в режиме продвинутого диалога на естественном языке⁵⁰⁹. Соответственно, любая информационная система, решающая интеллектуальную задачу или использующая методы искусственного интеллекта, является интеллектуальной. Таким образом, объединенные совокупностью большинства существующих на сегодняшний день технологий, интеллектуальные технологии позволяют формировать интеллектуальные информационные системы.

Основными достоинствами интеллектуальных информационных систем в области противодействия преступлениям в сфере компьютерной информации являются способность решения задач, сложность которых значительно превышает возможности задействованного в их решение специалиста, а также эффективное рассмотрение проблем, решение которых требует экспертных знаний в нескольких предметных областях (криминалистика, анализ данных, статистический анализ, математический анализ, системный анализ, программирование, машинное обучение). Типология интеллектуальных систем на современном этапе их развития

⁵⁰⁹ Остроух А. В. Интеллектуальные системы : монография. Красноярск: Научно-инновационный центр, 2020. С. 13.

представлена такими категориями как «экспертные системы» и «искусственные нейронные сети». Экспертные системы – это сложные программные комплексы, предназначенные для имитации работы экспертов в определенной области знаний, использующие базу данных, содержащую факты, правила и логические выводы для решения сложных задач и требующих для этого большого опыта⁵¹⁰. Экспертные системы основаны на жестких алгоритмах и подходят преимущественно для задач с жесткими правилами, логика работы которых всегда понятна и объяснима. Основанные на принципе машинного обучения искусственные нейронные сети анализируют значительные по объему данные и адаптируются к возникновению новых условий⁵¹¹ на основе недетерминированных, вариативных алгоритмов.

Главным отличием между ними является способность к самообучению, так искусственные нейронные сети способны к самообучению путем самостоятельного поиска зависимостей между входными и выходными данными, представленными в обучающей выборке, а экспертные системы работают исходя из заложенного в них конечного алгоритма решения задачи специалистом в конкретной области знаний. Развитие систем, способствующих принятию человеком решения, началось именно с появления экспертных систем, на смену которым пришло машинное обучение. Такой переход позволил современным информационным системам самостоятельно формировать правила и выявлять правильное решение на основе анализа зависимостей, на базе исходного набора данных (т. е. без предварительного составления экспертом перечня возможных вариантов решений), что позволило говорить о появлении технологии искусственного интеллекта. По решаемым задачам все интеллектуальные системы можно условно разделить на системы: обработки и поиска информации; поддержки принятия решений; управления; прогнозирования ситуаций, процессов или действий; автоматизированного проектирования⁵¹². Рассматривая экспертную систему статического типа (работающую с неизменными на протяжении всего процесса решения задачи данными), как наиболее простую из интеллектуальных систем, стоит отметить, что она состоит из решателя (интерпретатора), рабочей памяти в виде базы данных,

⁵¹⁰ Остроух А. В. Введение в искусственный интеллект. Указ. соч. С. 110.

⁵¹¹ Применение искусственных нейронных сетей и системы остаточных классов в криптографии / под ред. Червяков Н. И. М. : Физматлит, 2012. С. 7.

⁵¹² Станкевич Л. А. Интеллектуальные системы и технологии : практикум. М. : Юрайт, 2025. С. 85.

базы знаний, компонентов приобретения знаний, «объяснительного» и диалогового компонентов⁵¹³.

Применительно к информационным системам на основе искусственного интеллекта, формируемой в целях расследования преступлений, база данных в такого рода системе будет обеспечивать хранение исходных и промежуточных данных решаемой в текущий момент задачи расследования конкретного преступного деяния, а база знаний – хранение долгосрочных данных (набор экспертных знаний и правил в виде алгоритмов расследования преступлений, построенных на основе имеющихся рекомендаций и методик расследования). Решатель, используя исходные данные из базы данных по текущему уголовному делу и набору экспертных знаний о методиках расследования подобных преступлений, формирует возможность выдачи результата, способствующего решению поставленной задачи (расследованию).

Компонент приобретения знаний экспертной системы обеспечивает процесс наполнения базы знаний, осуществляемый пользователем-экспертом, при этом расшифровку действий на каждом из этапов решения задач обеспечивает «объяснительный» компонент. Диалоговый компонент служит для организации взаимодействия с пользователем как в ходе решения задач, так и в процессе наполнения базы знаний. Таким образом, можно подтвердить все выдвигаемые ранее гипотезы о возможности реализации информационной системы для целей криминалистики, которые по решаемым задачам будут относиться преимущественно к информационным системам обработки и поиска информации, поддержки принятия решений, управления, прогнозирования ситуаций, процессов или действий.

По этой причине на текущий момент сформировалась объективная необходимость аккумуляирования всех имеющихся знаний экспертов (ученых-криминалистов) в области расследования преступлений различного рода для построения такого рода экспертных (алгоритмизированных)⁵¹⁴ и интеллектуальных систем, позволяющих наиболее эффективно объединить в себе все информационные технологии. Для этого необходима совместная работа экспертов в конкретных предметных областях для обеспечения полноты и правильности введенных в информационную систему знаний, инженеров по знаниям

⁵¹³ Боровская Е. В. Давыдова Н. А. Основы искусственного интеллекта : учебное пособие М. : Лаборатория знаний, 2020. С. 28.

⁵¹⁴ Смушкин А. Б. Криминалистические аспекты использования киберпространства и обеспечения кибербезопасности: монография / под ред. В. Б. Вехова. М. : Русайнс, 2024. С. 147.

(разработчиков экспертных систем, которые выявляют и структурируют знания, необходимые для работы системы, осуществляя выбор наиболее подходящих информационных технологий и средств для данной проблемной области, определяющих способ представления знаний) и программистов (разработчиков программного обеспечения, которые могут осуществить сопряжение систем с той средой, в которой они будут использованы в дальнейшем).

Рассматривая результаты экстраполяции научных знаний и междисциплинарного синтеза (использования достижений смежных наук) в целях формирования новых криминалистических методов и средств необходимо разграничивать методологию теоретического и практического познания ввиду имеющихся различий в поставленных перед ними изначально задачах. Но смешение продуктов научного и практического познания в одном понятии является методологической ошибкой, что может быть равнозначно смешению правовых задач и фактических результатов расследования и, как следствие, приведет, например, к вынесению судебного решения или приговора, основанных на некорректных или неполных результатах расследования⁵¹⁵. По этой причине в настоящей работе в первую очередь исследуются теоретические вопросы построения информационно-компьютерной криминалистической модели преступления в сфере компьютерной информации, обосновывается реальность ее формирования с учетом имеющихся данных в смежных областях науки и техники и осуществляется апробация на тестовых данных. Не останавливаясь подробно на технических аспектах реализации интеллектуальных систем в целом, стоит лишь отметить готовность современного уровня развития научного познания реализовать предлагаемое решение.

Так, имеется достаточно исследований о:

- методах обеспечения аудита технических средств при расследовании компьютерных инцидентов⁵¹⁶;
- возможностях анализа цифровых данных, используемых в ходе расследования преступлений, а также моделях и методах выявления преступных

⁵¹⁵ Ищенко Е. П., Колдин В. Я. Типовая информационная модель преступления как основа методики расследования. Указ. соч. С. 132; Ковалев С. А., Вехов В. Б. Особенности компьютерного моделирования при расследовании преступлений в сфере компьютерной информации : монография. М. : Буки-Веди, 2015. С. 47.

⁵¹⁶ Пантюхин И. С. Методика и методы обеспечения аудита средств вычислительной техники для расследования компьютерных инцидентов : 2.3.6 : дис. ... канд. техн. наук : Санкт-Петербург, 2023. С. 35; Левшун Д. С. Архитектура системы обнаружения и прогнозирования уязвимостей информационных систем на основе методов искусственного интеллекта // Информатизация и связь. 2024. № 3. С. 91.

действий, выявления корреляционных связей между элементами криминалистической характеристики преступлений⁵¹⁷;

– взаимосвязях между атрибутами различных признаков в интеллектуальных системах⁵¹⁸;

– реализации отдельных методов обработки цифровых данных, в том числе больших данных⁵¹⁹;

– реализации систем поддержки принятия решений и анализа разнородных данных⁵²⁰ и пр.

В заключение необходимо отметить, что в целях повышения уровня раскрываемости преступлений в сфере компьютерной информации актуальными могут стать следующие направления деятельности:

– создание специализированной системы приема заявлений (сообщений) от

⁵¹⁷ Видонов Л. Г. Криминалистические характеристики убийств и системы типовых версий о лицах, совершивших убийство без очевидцев : методические рекомендации к использованию систем типовых версий. Горький : Прокуратура Горьк. Обл., 1978. С. 17; Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Указ. соч. С. 10; Денисов Е. В., Вечерин А. В., Коростелева Е. Ю. Иерархический кластерный анализ паттернов поведения серийных насильственных преступников // Вестник Воронежского государственного университета. 2022. № 3 (50). С. 316; Россинская Е. Р., Семикаленова А. И. Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа»). Указ. соч. С. 69.

⁵¹⁸ Голембиовский М. М., Рытов М. Ю., Кондрашова Е. В. Формализация процесса определения вероятности реализации компьютерных преступлений при их расследовании // Промышленные АСУ и контроллеры. 2023. № 5. С. 20; Маликов А. В. Авраменко В. С., Саенко И. Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы. 2019. № 6 (103). С. 32; Свидетельство о государственной регистрации программы для ЭВМ № 2024610017. Программа обнаружения угроз безопасности моделей искусственного интеллекта, использующихся в интеллектуальных системах поддержки принятия решения автоматизированных систем управления : № 2023684809 : заявл. 20.11.2023 : опубл. 09.01.2024; Бортникер П. В. Сравнительный анализ применения вейвлетов Хаара, Добеши и «Мексиканская шляпа» для обнаружения вторжений в информационные системы // Актуальные проблемы инфотелекоммуникаций в науке. Санкт-Петербург : СПбГУТ, 2024. С. 127.

⁵¹⁹ Кубасов И. А., Лекарь Л. А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России // Труды Академии управления МВД России. 2023. № 3 (67). С. 157; Аналитическая обработка больших массивов данных о событиях кибербезопасности с применением суперкомпьютерных вычислений / И. В. Котенко, И. Б. Саенко, И. Б. Паращук и др. // Программные продукты и системы. 2024. № 4. С. 488; Десницкий В. А. Подход к обнаружению атак в реальном времени на основе имитационного и графо-ориентированного моделирования // Информатизация и связь. 2021. № 7. С. 31.

⁵²⁰ Коробко А. В. Технология информационно-аналитической поддержки принятия решений на основе федерализации разнородной информации в концепции многомерного представления данных : 2.3.8 : дис. ... докт. техн. наук : Красноярск, 2024. С. 67.

потерпевших о преступлении с целью первичной обработки данных от заявителя и дальнейшего оперативного обмена информацией между заинтересованными лицами (правоохранительными органами, операторами связи, поставщиками интернет-услуг, финансово-кредитными организациями в Российской Федерации и пр.)⁵²¹ в целях своевременного установления обстоятельств противоправных деяний и лиц, их совершивших, фундаментальной основой которой будет являться глобальная криминалистическая база данных (по принципу функционирования центров IC3, EC3 и т. п.⁵²²);

– повышение уровня осведомленности граждан о методах совершения преступлений, а также способах защиты от них (по принципу реализации информационной кампании «Think Twice» повышения осведомленности граждан о растущих киберугрозах (от англ. – «подумай дважды») Международной организации уголовной полиции (Интерпол)⁵²³);

– противодействие незаконному обороту цифровых финансовых активов в целях легализации (отмывания) денежных средств, полученных преступным путем, а также для совершения транснациональных экономических преступлений, финансирования экстремизма, терроризма и пр. (по принципу реализации платформы «crypto-fraud», как аналога системы «anti-fraud»⁵²⁴);

– использование новых технологий как результата организации и проведения научно-исследовательских и опытно-конструкторских работ по разработке и применению криминалистических средств и методов выявления, раскрытия и расследования преступлений в сфере компьютерной информации, а также поиска цифровых доказательств (по принципу «DeerTech» – использования новейших информационных технологий, принятых на вооружение преступниками,

⁵²¹ О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 24 июня 2025 г. № 156-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_508287 (дата обращения: 25.06.2025).

⁵²² Европейский центр по борьбе с киберпреступностью // Полицияская служба Европейского союза EC3 (Европол) : офиц. сайт. URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (дата обращения: 11.01.2025).

⁵²³ Информационная кампания «Подумай дважды» по повышению осведомленности граждан о растущих киберугрозах «Think Twice before falling victim to online scams» // Международная организация уголовной полиции (Интерпол) : офиц. сайт. URL: <https://www.interpol.int/news-and-events/news/2024/interpol-campaign-warns-against-cyber-and-financial-crimes> (дата обращения: 11.01.2025).

⁵²⁴ Энциклопедия «Касперского»: глоссарий «Антифрод-системы (Anti-fraud)» // Акционерное общество «Лаборатория Касперского» : офиц. сайт. URL: <https://encyclopedia.kaspersky.ru/glossary/antifraud> (дата обращения: 11.01.2025).

и используемых в противовес правоохрательными и иными регулирующими органами для борьбы с ними);

- выстраивание оперативного сотрудничества с правоохрательными органами и кредитно-финансовыми организациями иных государств в области противодействия противоправным деяниям, совершаемым с использованием информационно-телекоммуникационных технологий (по принципу «PoliceTech» – в целях использования широкого спектра научных и технологических методов, приемов и аналитики, задействуемых в работе полицейских органов);

- адаптация нормативного регулирования в области противодействия преступлениям в сфере компьютерной информации под современные тенденции развития и использования информационных технологий, обеспечения информационной безопасности и защиты информации, а также совершенствование уголовного законодательства в части определения разновидностей преступлений и рекомендаций по их расследованию (по принципу «LawTech» – нормативного регулирования безопасного использования новейших информационных технологий, в том числе искусственного интеллекта).

Кроме того, необходимо комплексное обеспечение безопасности инфраструктуры связи и телекоммуникаций в Российской Федерации, что предусматривает в перспективе⁵²⁵:

- выявление юридически значимых механизмов оценки последствий от совершения преступлений в сфере компьютерной информации;

- создание технологии защищенного оператора сети подвижной радиотелефонной связи, обеспечивающего надлежащий уровень безопасности информации об абонентах;

- возможность категорирования информационно-телекоммуникационной сети связи, составляющих единую сеть электросвязи РФ, установление уровней доверия к телекоммуникационному оборудованию и использование в единой сети электросвязи РФ только доверенных программно-аппаратных комплексов, в том числе телекоммуникационного оборудования;

- рассмотрение требований к доверенным программно-аппаратным комплексам, применяемым на значимых объектах критической информационной

⁵²⁵ Об утверждении плана мероприятий по реализации Стратегии развития отрасли связи Российской Федерации на период до 2035 года : распоряжение Правительства Российской Федерации от 24 мая 2025 г. № 1312-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_506116/f62ee45faefd8e2a11d6d88941ac66824f848bc2 (дата обращения: 27.05.2025).

инфраструктуры РФ, в том числе требований к используемому в их составе телекоммуникационному оборудованию;

- утверждение требований об обязательном наличии у средств защиты информации встроенных функций для взаимодействия со средствами ГосСОПКА (государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ) в целях повышения эффективности защиты пользователей услугами связи от сетевых компьютерных атак;

- организации производства российского оборудования сетей подвижной радиотелефонной связи стандарта LTE и 5G, а также SIM- и USIM-карт с учетом выполнения требований по обеспечению информационной безопасности;

- определение подходов к регулированию технологий Интернета вещей и учета использования устройств со встроенными идентификационными модулями подвижной радиотелефонной связи;

- формирование правовых механизмов использования виртуальных телефонных станций и SIM-боксов;

- утверждение правил применения универсальных модулей идентификации абонентов в сетях подвижной радиотелефонной связи стандартов GSM/UMTS/LTE/5G/IMT-2020;

- нормативное регулирование применения электронных идентификационных модулей абонента (eSIM);

- внедрение технологии квантового распределения ключей на основе российского оборудования в интересах государственного сектора и корпораций;

- разработка всеобъемлющей международной конвенции о противодействии использованию информационно-телекоммуникационных технологий в преступных целях.

Стоит также рассмотреть ряд проблемных вопросов, связанных с применимостью получаемых в ходе работы алгоритмов (в том числе реализованных на основе искусственного интеллекта), результатов. Как известно, информационные системы и алгоритмы, особенно построенные на основе интеллектуальных технологий, должны подвергаться предшествующей оценке допустимости применения результатов их функционирования, что объясняется возможной предвзятостью алгоритмов, дискриминацией при обучении (когда алгоритмы содержат скрытые предубеждения, основанные на ограниченном

количестве данных, некорректно размеченных или некачественных сведениях) и отсутствием прозрачности в ходе рассуждений⁵²⁶.

На примере основных положений учения судебной экспертологии об экспертном прогнозировании можно описать проблему возникновения ошибок гносеологического и деятельностного характера, например, при производстве судебных экспертиз, что соответствует проблеме вероятностного характера большинства результатов, выдаваемых искусственным интеллектом.

Несмотря на массовое обсуждение указанных проблем и этики применения технологий искусственного интеллекта в целом, существуют решения, способные исключить такого рода негативные явления, которые заключаются в использовании ХАИ-систем (интеллектуальных систем, способных объяснять свои действия, ход и последовательность принимаемых решений, а также их представление в понятной для человека форме), обеспечении разнообразия и репрезентативности обучающих данных, тестирования и валидации разрабатываемых интеллектуальных моделей, а также введения стандартов для разработки и использования систем на основе искусственного интеллекта.

Следующая проблема применения алгоритмов связана с невозможностью использования рядом ведомств зарубежных программных технико-криминалистических средств, в том числе разработанных на базе когнитивных технологий, что объясняется необходимостью соблюдения требований программ импортозамещения⁵²⁷, допуская к задействованию в практику только программные средства, входящие в реестр отечественного программного обеспечения. Данная проблема решается лишь наращиванием собственного технологического потенциала, координацией усилий российских ИТ-компаний и инвестициями в научно-исследовательские проекты по предметным областям.

Отдельного внимания заслуживает вопрос, связанный с допустимостью и доказательственным значением результатов, полученных применением программных технико-криминалистических средств. Практическому

⁵²⁶ Россинская Е. Р., Неретина Н. С., Чубина Е. А. Современное состояние и перспективы развития машинного обучения и искусственного интеллекта для решения задач судебно-экспертной деятельности : аналитический обзор. М. : Консорциум «Инновационная юриспруденция». 2024. С. 85; Искусственный интеллект в юридической деятельности : учебник для вузов / под ред. С. Е. Чаннова. М. : Юрайт, 2025. С. 35.

⁵²⁷ Харисова З. И., Катянова А. А. О перспективах перехода органов внутренних дел на отечественное программное обеспечение в рамках импортозамещения // Организация Объединенных Наций и глобальные проблемы человечества в XXI веке : сборник материалов Международной научно-практической конференции. Уфа : Башкирский государственный университет, 2019. С. 251.

использованию любого криминалистического алгоритма или технико-криминалистического средства в обязательном порядке должна предшествовать оценка их допустимости, что обеспечивается широко распространенными и достаточно изученными в настоящее время методами тестирования и отладки программного обеспечения⁵²⁸. Кроме того, на этапе проектирования программного технико-криминалистического средства важно заложить в алгоритмы его работы логику уголовно-процессуального законодательства, актуальные методики и рекомендации в области криминалистики, теории оперативно-розыскной деятельности, теории управления и пр.

В научной литературе выделяют множество критериев допустимости и эффективности криминалистических алгоритмов, например, правомерность, нравственная безупречность и избирательность воздействия⁵²⁹, кроме того, имеются критерии оценки эффективности в отношении интеллектуальных алгоритмов решения задач при обработке информации в многокритериальных системах принятия решений⁵³⁰ и т. п.

Вопрос допустимости того или иного программного технико-криминалистического средства связан с объективной оценкой его содержания и принятием следователем решения о допустимости его применения в каждом конкретном случае расследования. Полное соответствие содержания того или иного алгоритма нормам действующего уголовного и уголовно-процессуального законодательства обеспечивает как правомерность, так и законность применения программного технико-криминалистического средства, разработанного на основе такого алгоритма и, соответственно, не приведет к нарушению законных прав и интересов граждан. Любое программное технико-криминалистическое средство должно обеспечивать нравственный подход в решении поставленных задач, т. е. заложенный в него алгоритм не должен содержать некорректных сведений, которые могли бы унижить честь или достоинство участников расследования, ошибочно предлагать решение, преумаляющее общественную опасность

⁵²⁸ Куликов С. С. Тестирование программного обеспечения. Минск : Четыре четверти, 2020. С. 20.

⁵²⁹ Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. Указ. соч. С. 187.

⁵³⁰ Чечнев В.Б. Анализ и классификация многокритериальных методов принятия решений. Онтология проектирования. 2024. Т. 14, № 4 (54). С. 607; Гречкин В. А. Интеллектуальные алгоритмы обработки информации в многокритериальных системах поддержки принятия решений // Вестник Ставропольского государственного университета. 2010. № 5. С. 37; Кохендерфер М., Рэй К., Уилер Т. Алгоритмы принятия решений. М. : ДМК Пресс, 2023. С. 521.

преступного деяния или оправдывающее действия преступника. Кроме того, алгоритмы должны применяться избирательно (при необходимости) и последовательно по усмотрению следователя.

При этом оценка целесообразности применения криминалистического алгоритма охватывается всеми указанными ранее критериями (правомерности, нравственности и избирательности), следователь в каждом случае должен сам определять являются ли здесь допустимыми известные ему криминалистические алгоритмы и программы⁵³¹.

К сожалению, всегда может присутствовать вероятность ошибки в выводах, сделанных той или иной информационной системой, в том числе интеллектуальной, как это возможно, например, в случае некомпетентности следователя. Поэтому на этапе зарождения подобных систем и их ввода в эксплуатацию все рекомендации интеллектуальных систем должны быть подвергнуты тщательной проверке субъектом расследования, что соответственно предполагает рассматривать такие решения лишь в качестве рекомендательных (особенно на этапе малого количества обучающих данных). Однако можно утверждать, что трудовые затраты и сложности ее реализации призваны обеспечить в будущем неоценимую помощь следователю в ходе расследования преступлений.

Выдвинутые в рамках рассмотрения правовых, методических, организационных и технических основ применения типовых алгоритмов расследования преступлений в сфере компьютерной информации предположения сонаправлены ряду выдвигаемых «изолированно» научным положениям ученых-криминалистов, экспертов и футурологов за последние несколько лет, например – прогнозу о существенных изменениях процесса предварительного расследования и частных криминалистических методик, которые будут упрощаться и все более становиться схожими с алгоритмами расследования⁵³², а также направлению алгоритмизации и цифровизации методов и методик судебно-экспертного исследования⁵³³.

Также стоит отметить сонаправленность выдвигаемого решения (и возможности формирования цифрового двойника преступления в целом) концепции криминалистической ситуалогии, которая сводится к упорядочению

⁵³¹ Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. Указ. соч. С. 192.

⁵³² Белкин Р. С. Курс криминалистики. Т.1. Указ. соч. С. 251.

⁵³³ Россинская Е. Р. Система теории цифровизации судебно-экспертной деятельности. Указ. соч. С. 24.

большого количества следственных ситуаций в однотипные классы (подклассы) для ограничения числа потенциально принимаемых решений следователем⁵³⁴. В аспекте ситуационного подхода деятельность следователя определяется как мысленное сопоставление конкретной следственной ситуации с типовой и в случае, если эти ситуации однотипны, предлагаемый алгоритм по разрешению типовой ситуации может быть использован для ситуации конкретной.

Кроме того, предлагаемый подход по реализации информационно-компьютерной модели преступного деяния соответствует направлению развития Индустрии 5.0⁵³⁵ в свете формирования цифровых двойников объектов, явлений или процессов, прогнозирования и принятия решений на основе искусственного интеллекта, создания коллаборативных роботов (коботов), способствующих взаимодействию человека с робототехникой на основе технологий компьютерного зрения, машинного обучения и интеграции больших языковых моделей, развития стратегии кибербезопасности «Zero trust»⁵³⁶ (от англ. «zero trust» – нулевое доверие), предполагающей недоверие к любой операции в информационном пространстве и пр., по этой причине подход в направлении противодействия современным преступлениям можно по аналогии именовать подходом «Криминалистика 5.0». Таким образом, характер инженерной разработки, направленной на создание программного обеспечения (Приложение 6) или интеллектуальной системы в рамках ситуационного моделирования, может определить возможность формирования алгоритмов, позволяющих на основе введенных в систему исходных данных выдвигать ограниченное число потенциально возможных принимаемых решений для следователя, что при соблюдении ряда условий (систематического накопления информации о ситуации, знания типовой ситуационной структуры, учета субъективных и объективных факторов, способных изменить ситуацию и т. п.) может быть важно, особенно для молодых специалистов, задействованных в расследовании рассматриваемых преступлений, ввиду отсутствия у них профессионального опыта, а также в условиях недостатка времени, предоставленного на расследование, информации о механизме преступления, а также лицах его совершивших.

⁵³⁴ Волчецкая Т. С. Криминалистическая ситуалогия. Указ. соч. С. 179.

⁵³⁵ Индустрия 5.0 : На пути к устойчивой, ориентированной на человека парадигме // Европейский союз : офиц. сайт. URL: <https://op.europa.eu/en/publication-detail//publication/468a892a-5097-11eb-b59f-01aa75ed71a1> (дата обращения: 27.05.2025).

⁵³⁶ Garbis J., Chapman J. Zero Trust security: an enterprise guide. Apress Berkeley, 2021. P. 28.

ГЛАВА 5. ИНТЕЛЛЕКТУАЛИЗАЦИЯ ПРОЦЕССА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ КАК ОСНОВА РАЗВИТИЯ ТЕОРИИ ИНФОРМАЦИОННО-КОМПЬЮТЕРНОГО ОБЕСПЕЧЕНИЯ КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

5.1. Концептуальные основы учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности

Система частных криминалистических теорий, являясь на сегодняшний день адаптивной и развивающейся, подвержена изменениям, которые объясняются возникновением потребности в новых средствах, приемах и методах борьбы с преступностью, а также необходимостью их обобщения и анализа. Трансформация одной из частных криминалистических теорий под воздействием изменений или уточнения представлений об элементах ее составляющих может привести к частичным изменениям содержания системы криминалистических теорий в целом. Это, соответственно, может повлечь за собой изменение связей между элементами всей системы, а также их уровней.

Тенденция развития любой науки в настоящее время тесно связана с процессом формализации, что касается и частных криминалистических теорий, например, в плане формализации описания объектов исследования (цифровых следов, технических средств, информационных систем и пр.) или профессиональных знаний в целях программирования расследования⁵³⁷.

Сфера компьютерной информации в наибольшей степени требует формализации и зависит от развития науки о данных (от англ. «data science» – раздел компьютерных наук, изучающий проблемы анализа, обработки и представления данных в цифровой форме) – междисциплинарной области на стыке аналитики, статистики, математики, программирования, машинного обучения, а также логики, теории алгоритмов, системного анализа и управления, теории принятия решений и пр.

Результат объединения знаний из смежных областей может привести к возникновению новых частных криминалистических теорий, учений и

⁵³⁷ Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. Указ. соч. С. 110.

концепций⁵³⁸. На сегодняшний день это подтверждается, например, существованием частной теории информационно-компьютерного обеспечения криминалистической деятельности⁵³⁹ и входящими в нее учениями (о способах совершения компьютерных преступлений, о цифровых следах, о криминалистическом исследовании технических средств и информационных систем, о цифровизации системы криминалистической регистрации и др.).

Гарантией реализации основной функции криминалистики, заключающейся в содействии практике борьбы с преступностью, выступает трансформация и модификация частных криминалистических теорий, обеспечивающая максимальное соответствие вновь появляющимся угрозам. По этой причине необходимо рассмотреть ряд актуальных на сегодняшний день факторов, в наибольшей степени влияющих на процесс расследования преступлений в сфере компьютерной информации. Среди такого рода факторов можно отметить: рост объема цифровых данных и, как следствие, увеличение массива потенциально возможных криминалистически значимых сведений, которые могут выступать цифровыми доказательствами, а также времени, затрачиваемого на их обнаружение, фиксацию, изъятие и исследование; необходимость принятия решений (тактических, технико-криминалистических или методических) в условиях неопределенности (крайнего дефицита или неполноты информации), в том числе по выбору средств достижения целей для каждой из сложившейся следственной ситуации, обеспечивающих максимально эффективное их задействование при раскрытии и расследовании преступлений.

Процессу организации раскрытия, расследования и предотвращения преступлений присуща разработка и принятие управленческих решений⁵⁴⁰. Однако данный процесс довольно часто сопровождается информационной неопределенностью в сложившейся следственной ситуации, при которой необходимо решить какое средство и на основе какого метода целесообразно применить, в соответствии с какой методикой или рекомендацией расследования, чтобы максимально эффективно, с минимальными временными и трудовыми

⁵³⁸ Макаренко И. А. Проблемы симбиоза научных исследований, образования и правоприменительной практики // Современные технологии и подходы в юридической науке и образовании : сборник материалов международного научно-практического форума. Калининград : Балтийский федеральный университет им. Иммануила Канта, 2021. С. 169.

⁵³⁹ Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. Указ. соч. С. 19.

⁵⁴⁰ Возгрин И. А. Криминалистическая методика расследования преступлений. Указ. соч. С. 112.

затратами устранить неопределенность. Под информационной неопределенностью в данном случае стоит понимать некую ситуацию, когда информации для решения поставленной задачи оказывается недостаточно. Соответственно, решение, принятое в условии определенности или достаточности исходных данных, отличается тем, что следователю известно, к какому результату приведет исполнение каждого из альтернативных решений, довольно часто такого рода решения бывают связаны с применением технико-криминалистических средств и работой с доказательствами.

Именно преступления в сфере компьютерной информации отмечаются высокой степенью информационной энтропии – мерой неопределенности системы (непредсказуемости). Такой их характер обусловлен значительной степенью неочевидности применяемых способов совершения преступных деяний, что, в основном, является следствием применения разнообразных средств анонимизации личности преступника, методов шифрования данных и сетевого трафика и т. п. Высокая степень информационной энтропии является фактором увеличения количества различных состояний (вариаций) следственных ситуаций, по этой причине процесс принятия решений следователем при расследовании преступлений в сфере компьютерной информации может усложняться.

Познавательную деятельность можно представить в виде ряда сменяющих друг друга процедур принятия решений, поэтому устранение или снижение информационной неопределенности может быть сведено к исполнению алгоритма действий. Именно формализация (наравне с алгоритмизацией) выступает важнейшим процессом при формировании криминалистических методик, а также служит необходимым условием создания наиболее действенных инструментов противодействия преступлениям в сфере компьютерной информации в виде программных технико-криминалистических средств, одновременно выступая показателем эффективности в поиске сходств и различий между желаемыми и фактически достигнутыми результатами. При этом чем меньше будет различий между ними – тем выше оценивается эффективность действий следователя⁵⁴¹.

Универсальная схема принятия решений в стадии расследования преступлений вполне может быть заимствована из «типовой» модели, выработанной теорией и наукой управления, с необходимыми корректировками и дополнениями, обусловленными спецификой сферы деятельности, в рамках

⁵⁴¹ Шаталов А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. Указ. соч. С. 124.

которой принимаются соответствующие решения⁵⁴², при этом такого рода унифицированная модель применима для процесса принятия любых решений – правовых, тактических, технико-криминалистических и методических, а значит, отличаясь более высоким уровнем обобщения, она способна стать теоретической базой для практического применения.

Формирование и систематизацию положений, принципов и категорий, представляющих собой идеализированную модель процедуры выработки оптимальных решений, обеспечивает криминалистическая теория принятия решений. Поэтому, не останавливаясь подробно на ее структуре и методах, нужно лишь отметить возможность учета вероятностного характера принятия криминалистического решения путем задействования алгоритмов искусственного интеллекта, а также важность принятия именно обоснованного решения, поскольку ошибки в выборе средств и методов, способов действий или линий поведения в условиях расследования могут привести к таким неблагоприятным последствиям как утрата доказательств, что особенно важно при работе с цифровыми данными.

Склонность человека к рассуждениям в условиях, когда исходные данные недостоверны, либо их недостаточно до момента развития науки о данных считалась слабостью «человеческого интеллекта», но это привело к пониманию значимости роли вероятностных рассуждений, что стало особенно важно для сложных систем различной природы. Для сложных следственных ситуаций одной из основных трудностей является именно информационная неопределенность исходных данных, которая часто усугубляется факторами конфликта и риска⁵⁴³.

Статистические данные по преступлениям в сфере компьютерной информации говорят о сравнительно большой доле нераскрытых преступных деяний. Проведенный анализ преступлений, уголовные дела по которым были приостановлены или сданы в архив из-за невозможности установления личности виновного, показал, что основным фактором, приводящим к такому раскладу, является именно информационная неопределенность исходных данных. По этой причине для оптимизации процесса принятия решений в сложных следственных ситуациях наиболее перспективным является подход, связанный с поиском дополнительных сведений, способствующих получению доказательств. Повышенная латентность цифровых данных и активное противодействие

⁵⁴² Криминалистика. Теоретический курс. Указ. соч. С. 187.

⁵⁴³ Драпкин Л. Я., Шуклин А. Е. Принятие оперативно-розыскных и следственных решений в ситуациях информационной неопределенности, конфликта и риска // Российский юридический журнал. 2006. № 3 (51). С. 89.

киберпреступников значительно затрудняют получение доказательств, в связи с чем на первый план выходят специальные технико-криминалистические средства, которые обеспечивают поиск криминалистически значимой компьютерной информации и от применения которых в значительной степени зависит эффективность следственных мероприятий.

Кроме того, для принятия наиболее эффективного решения при расследовании преступления в сфере компьютерной информации довольно часто следователь сталкивается с необходимостью обработки больших объемов информации в сжатые сроки. Для этого целесообразно учитывать многочисленные факторы, которые оказывают влияние на весь ход расследования и требуют выбора подходящего инструмента, как правило, используемого в виде специальных информационных систем, оказывающих поддержку принятия решений или предоставляющих рекомендации к действиям.

Решение данной проблемы заключается в применении систем поддержки принятия решений на основе искусственного интеллекта (методов нечеткой логики и предиктивной аналитики, под которой понимается моделирование, оценка имеющихся данных на основе модели, а также выдача прогноза). Под предиктивной аналитикой также понимается ряд дисциплин, связанных с принятием решений. Соответственно, модель предиктивной аналитики может выступать в качестве прогностической, описательной, либо модели принятия решений⁵⁴⁴. К методам предиктивной аналитики, например, относятся нейронные сети, нечеткая логика, методы ансамблевого обучения, позволяющие повысить качество результатов или усилить модель машинного обучения путем объединения нескольких различных моделей в ансамбль⁵⁴⁵ и пр.

Важной проблемой при построении любой модели предиктивной аналитики является подготовка набора данных для извлечения зависимостей. Соответственно, для построения качественной системы поддержки принятия решений необходимо иметь набор данных, содержащий информативные признаки для решения конкретной задачи. Кроме того, необходима предварительная их разметка либо использование методов предобработки.

⁵⁴⁴ Искусственный интеллект – предсказательная аналитика и системы : аналитический сборник Центра компетенций Национальной технологической инициативы МФТИ // Автономная некоммерческая организация «Цифровая экономика» : офиц. сайт. URL: https://cdo2day.ru/wp-content/uploads/2020/11/almanach_ai_5.pdf (дата обращения 07.05.2025).

⁵⁴⁵ Исследование и разработка моделей, методов, алгоритмов оценки качества наборов данных для задач предиктивной аналитики динамики показателей / Н. Г. Ярушкина, В. С. Мошкин, Г. Ю. Гуськов [и др]. Ульяновск : УлГТУ, 2024. С. 10.

Таким образом, преодоление неопределенности сводится к упрощению представления поставленной задачи, формированию и обработке набора данных, формализации и построению информационной модели. Один из наиболее распространенных подходов к упрощению задачи выбора состоит в получении дополнительной информации за счет описания рассматриваемых вариантов (альтернатив) на языке критериев. Недостаточность данных при принятии решений необходимо учитывать в рамках построенной модели в соответствии с установленными показателями эффективности (целевых функций, функций ценности). Как правило, для исследования неопределенностей используется математический аппарат, который опирается на теорию вероятностей и теорию нечетких множеств, разрабатываются специфические средства для формализации, представления и обработки вероятностной и нечеткой информации⁵⁴⁶. Признаки, описывающие варианты решения проблемы и неопределенные факторы, характеризующие возможные состояния рассматриваемых ситуаций, в свою очередь, зависят от многих параметров, часть из которых являются вычисляемыми и определяются в результате обработки данных. И вновь, обращаясь к решению проблемы вариативности выбора, стоит отметить, что одним из подходов многоэтапного выбора в условиях неопределенности, является, например, широко известный подход «дерево решений» (от англ. «decision tree» – дерево принятия решений), представляющий собой иерархический ветвящийся граф, имеющий корневую вершину (проблему, требующую решения), вершины-решения, вершины-случаи и являющийся одним из важнейших методов машинного обучения.

Наука как форма общественного сознания выполняет множество функций, одна из которых – познавательная, заключающаяся в формировании знаний, которые в конечном счете принимают форму гипотезы или теории, описывающей, объясняющей или систематизирующей добытые знания, способствуя прогнозированию дальнейшего познания.

В криминалистическом смысле прогноз необходимо рассматривать в качестве одного из оснований планирования аналогично следственной версии, либо следственной ситуации. Следственная ситуация как обстановка, в которой осуществляется расследование в данный момент, в значительной степени определяет содержание планирования. При этом прогноз выступает в качестве основания планирования через предположение и оценку будущего состояния

⁵⁴⁶ Петровский А. Б. Теория принятия решений. М. : Издательский центр «Академия», 2009. С. 135.

процессов и явлений в сфере расследования преступления, таким образом, он позволяет уточнить круг задач, возникающих перед следователем на каком-либо этапе расследования, их приоритетность, правильный выбор технико-криминалистических средств⁵⁴⁷ для успешного проведения планируемых следственных и иных действий.

Процесс получения, обработки и анализа необходимой для прогноза информации называется прогнозированием, который, как правило, обеспечивается моделью прогнозирования, например, статистической прогностической моделью, моделью машинного обучения или глубокого обучения. Однако во многих реальных задачах прогнозы, полученные с помощью указанных моделей, часто сопровождаются низкой точностью ввиду недостаточного объема исходных данных, неверного подхода к обучению системы на неполных данных, либо не содержат количественной оценки неопределенности, которая могла бы показать вероятность принятия эффективного решения.

Повысить достоверность и интерпретируемость прогностических моделей позволяет конформное прогнозирование, которое обеспечивает удобство и предиктивную аналитику вне зависимости от типа распределения данных и применяемой модели обучения с выдачей меры доверия или уверенности к прогнозу⁵⁴⁸. Прозрачность такого рода моделей и объяснимость принятия того или иного решения может обеспечить объяснимый искусственный интеллект, который решает проблему «черного ящика», свойственную сложным моделям⁵⁴⁹. Таким образом, конформное прогнозирование, являясь специальной техникой машинного обучения, позволяет «откалибровать» модель искусственного интеллекта в целях исключения принятия недостоверных решений.

Подводя итоги вышеуказанному необходимо отметить, что снизить степень влияния факторов, затрудняющих процесс расследования преступлений в сфере компьютерной информации, в настоящее время можно интеграцией в него технологий искусственного интеллекта.

Накопление теоретических знаний, а также взаимное влияние теории и практики является основой развития любой науки. Просматривая преемственность между условными «поколениями» криминалистических теорий, сформированных

⁵⁴⁷ Литвинов А. Н., Степанюк Р. Л. Прогнозирование и планирование в криминалистике. М. : ЮРКНИГА, 2004. С. 133.

⁵⁴⁸ Манохин В. Конформное прогнозирование в Python. М. : ДМК Пресс, 2024. С. 11.

⁵⁴⁹ Sarker I. H. AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Perth : Edith cowan university. 2024. P. 15.

на различных этапах развития криминалистики, можно выявить закономерность приспособления современных достижений науки для целей уголовного судопроизводства. Это подтверждает необходимость адаптации достижений криминалистики в целях соответствия потребностям практики борьбы с преступностью.

Так, для исследования технических средств и информационных систем разработан особый комплекс специальных знаний в виде теории информационно-компьютерного обеспечения криминалистической деятельности, сформированной в целях теоретического и прикладного обеспечения раскрытия и расследования преступлений, что особенно важно по преступлениям в сфере компьютерной информации и иным преступным деяниям, совершаемым с использованием информационных технологий.

Познание преступного деяния в криминалистике осуществляется посредством применения всей совокупности методов этой области научного знания⁵⁵⁰. Традиционно к методам криминалистики относят, например, такие методы как наблюдение, измерение, описание, сравнение, эксперимент, моделирование, а также математические и специальные методы исследования. Стоит отметить, что, начиная с 60-х годов, преимущественно, ввиду развития направления криминалистической экспертизы, широкое признание в исследованиях получили математические методы⁵⁵¹. Одновременно появлялись новые методы, которые относили к «специальным методам» криминалистики, некоторые методы были заимствованы из других наук (например, кибернетические, физические, химические, статистические и пр.).

Вполне обоснованным на сегодняшний день является включение в специальные методы криминалистики методов науки о данных (методов искусственного интеллекта и таких относящихся к нему классов, как машинное обучение, компьютерное зрение, визуализация данных, глубокое обучение, обработка естественного языка и пр.) как наиболее близких к сфере компьютерной информации.

По этой причине выдвигается гипотеза о необходимости развития (дополнения) одного из элементов общей теории криминалистики – учения о методах криминалистики (в плане пополнения специальных методов), а также

⁵⁵⁰ Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Указ. соч. С. 13.

⁵⁵¹ Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. Указ. соч. С. 122.

частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности. Это объясняется экспоненциальным ростом циркулирующих в настоящее время объемов цифровых данных, что делает применение технологий искусственного интеллекта для криминалистического анализа не только целесообразным, но и необходимым.

Предполагается, что интеграция методов науки о данных в криминалистику позволит в дальнейшем перейти от реактивной модели противодействия преступлениям (вмешательство постфактум) к проактивной (основанной на криминалистическом прогнозировании и предупреждении преступлений).

Предмет теории информационно-компьютерного обеспечения криминалистической деятельности составляют закономерности, связанные: с цифровыми следами, содержащими криминалистически значимую компьютерную информацию, в том числе отражениями данных следов в технических средствах и информационных системах; со способами и обстоятельствами совершения преступлений; с информационными технологиями, обеспечивающими возможность обнаружения, фиксации, изъятия и исследования криминалистически значимой компьютерной информации; с информационно-компьютерным криминалистическим обеспечением тактики и технологии производства следственных и судебных действий и обеспечения методики расследования преступлений, в том числе формирования их информационно-компьютерных моделей⁵⁵².

Объектами рассматриваемой теории являются, с одной стороны, сами технические средства и информационные системы как носители розыскной и доказательственной криминалистически значимой информации, а с другой – система действий и отношений в механизмах преступлений с использованием технических средств и информационных систем, а также информационные технологии, допускающие выявление, фиксацию, изъятие, сохранение, исследование и использование криминалистически значимой доказательственной и ориентирующей информации⁵⁵³.

Частная теория информационно-компьютерного обеспечения криминалистической деятельности входит в общую теорию криминалистики и, в

⁵⁵² Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 193-202. С. 197.

⁵⁵³ Россинская Е. Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3. С. 110.

свою очередь, состоит из восьми учений:

1. Концептуальные основы теории информационно-компьютерного обеспечения криминалистической деятельности, включая предмет теории, ее объекты, изучаемые закономерности;
2. Учение о способах компьютерных преступлений;
3. Учение о цифровых следах как источниках криминалистически значимой компьютерной информации;
4. Учение о криминалистическом исследовании компьютерных средств и систем;
5. Учения о цифровизации системы криминалистической регистрации;
6. Учение об информационно-компьютерных криминалистических моделях компьютерных преступлений;
7. Учение об информационно-компьютерном обеспечении криминалистической деятельности тактики следственных и судебных действий;
8. Учение об информационно-компьютерном обеспечении криминалистической деятельности методик расследования компьютерных преступлений⁵⁵⁴.

Несмотря на то, что в настоящее время имеется множество теоретических предложений и исследований, предусматривающих использование технологий на основе искусственного интеллекта в целях прогнозирования или расследования преступлений, необходимо отметить скромное количество непосредственно прикладных разработок. Сложившаяся ситуация схожа с развитием теории программирования расследования, которая начала свое формирование более 50 лет назад, но получила за последние десятки лет преимущественно теоретическую проработку, при том, что разработка программы расследования в техническом плане реализуема проще в сравнении с созданием и внедрением в процессы решения криминалистических задач и обеспечение криминалистической деятельности систем на основе искусственного интеллекта⁵⁵⁵.

Являясь фундаментальной, существующая теория информационно-компьютерного обеспечения криминалистической деятельности также требует постоянного развития для соответствия современным вызовам, поскольку

⁵⁵⁴ Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 198.

⁵⁵⁵ Головин А. Ю. Технологии искусственного интеллекта в криминалистике: задачи, которые необходимо решить // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 2. С. 29.

преступления в сфере компьютерной информации представляют собой динамичную и высокотехнологичную угрозу, эволюция которой опережает традиционные методы расследования. Выявленные теоретические основы и практические аспекты расследования указанных преступных деяний в рамках проведенного исследования позволяют констатировать о возможности развития и расширения содержания представленной выше теории путем интеграции современных аналитических и прогностических возможностей на основе технологии искусственного интеллекта, направленных на интеллектуализацию процесса расследования, анализ больших объемов цифровых данных, выявление скрытых связей между событиями и пр., что позволит повысить эффективность расследования рассматриваемого вида преступлений в целом.

Стоит отметить, что в настоящее время складывается ситуация, при которой алгоритмизация процесса расследования преступлений в сфере компьютерной информации вполне допустима⁵⁵⁶, равно как и интеллектуализация. Это объясняется схожим механизмом совершения большинства преступных деяний в рассматриваемой сфере, что подтверждается официальными статистическими данными. Однако, для отличающихся особой сложностью ситуаций, алгоритмизация потребует либо накопления данных, либо довольствования вероятностным решением.

Создавая конкретное интеллектуальное программное обеспечение в рамках проблемной области, прежде всего, следует очертить сферу его использования, которая задается особенностями самой проблематики⁵⁵⁷, при этом регистрация и учет преступлений выглядит как наиболее традиционная область компьютерно-ориентированных систем, а интеллектуализация предполагает выявление сходства различных рассматриваемых объектов и выдачу похожих или аналогичных обстоятельств, нахождение связей или ассоциаций между различными фактами, формирование предположений относительно вероятной корреляции расследуемого дела с некоторыми другими.

Имеющийся сегодня в распоряжении следствия значительный массив информации криминалистического значения не может быть формализован

⁵⁵⁶ Драпкин Л. Я., Долинин В. Н., Шуклин А. Е. Проблемы алгоритмизации в криминалистике и следственной деятельности // Уголовное право и криминалистика, 2018. № 6. С. 31.

⁵⁵⁷ Rossinskaya E. R., Belkin A. R. KBS for criminology and forensic expertise // Toepassingsgebieden methoden en technieken operationele toepassingen besluitvorming kennismanagement : Congresgebouw RAI. Amsterdam, 1993. P. 147.

полностью, но может и должен быть организован⁵⁵⁸. Так, в свете накопления данных для изучения взаимосвязей между элементами криминалистической характеристики рассматривалась возможность анализа информации, содержащейся в статистических карточках, представляемых следователями в информационные подразделения МВД России на различных этапах расследования, а также в материалах уголовных дел⁵⁵⁹. Помимо документов первичного учета и материалов уголовных дел для построения информационных моделей в литературе предлагалось использовать статистику о состоянии преступности, материалы об отказе в возбуждении уголовного дела и материалы оперативно-розыскной деятельности, заключения экспертов и специалистов, обобщения следственно-судебной практики, протоколы оперативных совещаний органов дознания и следствия, межведомственные информационные материалы с рекомендациями по практике расследования преступлений, а также отдельные данные типовых криминалистических характеристик, смежных с исследуемыми преступлениями, и международный опыт расследования преступных деяний⁵⁶⁰.

Вышеуказанный перечень элементов, составляющих наборы структурированных или сгруппированных по определенным признакам и необходимых для разработки программного обеспечения на основе искусственного интеллекта данных, безусловно, подлежит тщательной предварительной разметке, определяющей процесс присвоения идентификаторов, отражающих тип данных, или осуществления интерпретации данных для решения конкретных задач. Таким образом, корректно размеченные, репрезентативные и релевантные наборы данных являются основой для формирования моделей искусственного интеллекта в виде программного обеспечения, предназначенного для выполнения интеллектуальных задач на уровне, сопоставимом с результатами интеллектуального труда человека или превосходящем их, с целью выявления закономерностей, принятия решений или прогнозирования результатов.

Рассматривая концептуальные основы теории информационно-компьютерного обеспечения криминалистической деятельности и ряд

⁵⁵⁸ Ищенко П. П. Информационное обеспечение следственной деятельности. Указ. соч. С. 82.

⁵⁵⁹ Ким Д. В. Ситуационный подход как основа создания информационно-поисковых систем в расследовании преступлений // История государства и права. 2005. № 7. С. 25; Булгаков Д. Ю. Использование методов машинного обучения для прогнозирования раскрываемости преступлений на основе документов первичного учета // Моделирование, оптимизация и информационные технологии. 2021. № 2 (33). С. 3.

⁵⁶⁰ Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Указ. соч. С. 39.

сопутствующих учений, можно отметить возможность ее дополнения рядом закономерностей и формирования нового концепта в свете интеллектуализации криминалистического обеспечения и реализации алгоритмических решений в виде программных технико-криминалистических средств для обнаружения, фиксации, изъятия и исследования цифровых доказательств на основе технологий искусственного интеллекта.

Объект и предмет рассматриваемой теории сформулированы весьма удачно. Так, объекты уже включают в себя компьютерные средства и системы, которые как носители розыскной и доказательственной криминалистически значимой информации могут без всяких дополнений представлять собой различного рода интеллектуальные решения. С позиции рассмотрения объектов теории как системы действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также технологий обнаружения, фиксации, изъятия и исследования криминалистически значимой доказательственной и ориентирующей информации, можно отметить, что такого рода системы также могут быть подвергнуты процессу интеллектуализации.

Предмет соотносим с закономерностями возникновения, движения, собирания, исследования и использования компьютерной информации при раскрытии и расследовании преступлений и в общем своем понимании, аналогично, предполагает возможность интеллектуализации указанного процесса. Однако, можно расширить предмет теории информационно-компьютерного обеспечения криминалистической деятельности с учетом современных вызовов и технологических реалий, внесением ряда дополнений, обусловленных внедрением в практику расследования технологий искусственного интеллекта и интеллектуализацией криминалистической деятельности, в частности, закономерностями:

– обнаружения, фиксации, изъятия и исследования криминалистически значимой компьютерной информации с использованием алгоритмов искусственного интеллекта (интеллектуальных программных технико-криминалистических средств), которые отражают особенности автоматизированного выявления цифровых следов при помощи систем на основе искусственного интеллекта, а также нахождения связей между цифровыми следами и действиями субъектов рассматриваемых преступлений (в основе данного процесса лежит применение систем на основе машинного обучения и интеллектуального анализа данных для автоматической идентификации цифровых доказательств, потенциально содержащих криминалистически значимую

информацию, которые способны выполнять первичную фильтрацию значительных по объему данных, осуществлять их классификацию по типу, источнику или степени релевантности);

- генерации, модификации или уничтожения цифровых следов с использованием технологий искусственного интеллекта, которые описывают возможности создания искусственных цифровых следов или сфальсифицированного цифрового контента интеллектуальными системами, в частности, генеративными моделями, а также способы обнаружения сгенерированных, модифицированных или уничтоженных с помощью искусственного интеллекта цифровых данных с применением криминалистических методик;

- интеллектуального распознавания криминалистически значимых связей в больших массивах данных, которые выявляют соответствия между цифровыми следами и действиями субъектов рассматриваемых преступлений;

- правового и технического регулирования искусственного интеллекта в криминалистике и интеграции результатов интеллектуального анализа в систему доказательственной информации, которые предусматривают процедуру юридической или криминалистической верификации выявленных данных и определяют условия допустимости, достоверности и достаточности найденных цифровых доказательств, стандартизацию процессов интеллектуального анализа, их воспроизводимости, прозрачности алгоритмов рассуждений, исключая предвзятость, ложноположительные или ложноотрицательные результаты;

- реконструкции событий преступного деяния средствами интеллектуального моделирования – создания цифровых двойников преступного деяния, которые отражают возможности машинного моделирования способов совершения рассматриваемых преступлений, их цифрового воспроизведения, генерации и тестирования следственных версий на основе обученных моделей, способных реконструировать предполагаемый ход событий, воспроизводить предполагаемые действия преступника в условиях, приближенных к реальным, выявлять наиболее эффективные тактику и технологии производства следственных и судебных действий, формировать адаптивные методики расследования преступлений;

- взаимодействия интеллектуальных моделей с криминалистическими базами данных в виде учетов, которые отражают адаптацию искусственного интеллекта к разнородным криминалистически значимым данным, выявление скрытых взаимосвязей между ними, а также автоматическое формирование

криминалистических версий на основе накопленной информации;

- противодействия расследованию с использованием систем на основе искусственного интеллекта, которые описывают способы применения злоумышленниками интеллектуальных систем для сокрытия следов, автоматизированного шифрования или анонимизации сетевого трафика, введения следствия в заблуждение, а также механизмы выявления и нейтрализации таких технологий;

- функционирования интеллектуальных систем поддержки следователя в условиях информационной неопределенности в целях принятия тактически верного решения;

- обработки неполной и фрагментированной информации на основе имеющихся в базах данных интеллектуальной системы сведений с целью формирования следственных версий и методик расследования;

- интеллектуального прогнозирования возможности расследования преступного деяния и раннего обнаружения признаков подготовки преступления.

Как видно, представленные закономерности затрагивают все имеющиеся в указанной теории учения, по этой причине можно сделать вывод, что современный этап развития криминалистики требует дополнения теории информационно-компьютерного обеспечения криминалистической деятельности и интеграции в нее указанных закономерностей, объединив их в отдельное учение об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности.

Концептуальная основа предлагаемого учения развивает положения общей теории криминалистики в части применения интеллектуальных систем для выявления, моделирования, интерпретации и верификации цифровых следов преступной деятельности в современных условиях, а также прогнозирования возможности расследования преступного деяния, формирования рекомендаций по выбору наиболее эффективной методики расследования.

Предметом учения является система закономерностей обнаружения, фиксации, изъятия и исследования криминалистически значимой компьютерной информации (в том числе выявления генерации, модификации или уничтожения цифровых следов) с использованием технологий искусственного интеллекта при раскрытии и расследовании преступлений, а также совокупность особенностей разработки, функционирования и использования интеллектуальных систем в виде программных технико-криминалистических средств в качестве инструмента поддержки принятия решений в условиях информационной неопределенности или

фрагментарности данных, формирования цифровых двойников и реконструкции событий преступного деяния, а также выдачи оптимальных методик расследования преступлений.

Объект учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности составляют непосредственно сами интеллектуальные технические средства и системы и содержащаяся в них криминалистически значимая компьютерная информация, интеллектуальные программные технико-криминалистические средства, обеспечивающие обнаружение, фиксацию, изъятие и исследование криминалистически значимой компьютерной информации с использованием алгоритмов искусственного интеллекта, а также система действий и отношений, реализованных на основе интеллектуальных систем, обеспечивающих анализ криминалистически значимой компьютерной информации, поддержку принятия решений в условиях информационной неопределенности, моделирование цифровых двойников и событий преступного деяния, а также формирование оптимальных методик расследования преступлений и выдачу вероятности их раскрытия.

С учетом того, что развитие криминалистики осуществляется за счет изучения новых закономерностей, механизмов слеодообразования, современных технологий обнаружения, фиксации, изъятия и исследования криминалистически значимой информации⁵⁶¹ расширение системы теории информационно-компьютерного обеспечения криминалистической деятельности путем формирования нового учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности выглядит вполне обоснованно и подтверждается в настоящее время «сдвигом» преступности в высокотехнологичную область.

Можно также предположить, что предлагаемая концепция интеллектуализации процесса расследования преступлений обеспечит научно-техническую основу для реализации практико-ориентированных решений противодействия преступным деяниям не только в сфере компьютерной информации или по преступлениям против общественной безопасности и общественного порядка (глава 28 УК РФ в составе раздела IX УК РФ), но и ряда сопутствующих областей, например, по преступлениям против личности (раздел VII УК РФ), в сфере экономики (раздел VIII УК РФ) и пр.

⁵⁶¹ Россинская Е. Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридический вестник Самарского университета. 2019. № 4. С. 146.

Отдельное внимание стоит уделить перспективному направлению, объединяющему достижения квантовых вычислений и современных информационных (эммерджентных и сквозных) технологий, в том числе технологии искусственного интеллекта, для повышения эффективности расследования преступлений – квантовому криминалистическому обеспечению. Данный подход может существенно расширить возможности традиционных криминалистических методов и средств, в частности, обеспечить:

- ускоренный анализ цифровых данных с помощью квантовых вычислений благодаря широкому потенциалу экспоненциального ускорения обработки данных квантовыми компьютерами, что особенно важно при анализе сетевого трафика в режиме «онлайн»;
- дешифрование данных на основе алгоритма Шора⁵⁶², например, при расследовании преступлений, связанных с цифровыми фиатными активами и сложными средствами защиты информации;
- целостность цифровых доказательств задействованием квантовой криптографии (протоколов «QKD»⁵⁶³ (от англ. «quantum key distribution» – квантовое распределение ключей) и блокчейн-технологий, которые позволяют создать непрерывную и защищенную цепочку передачи цифровых доказательств, исключая попытки перехвата или изменения данных;
- аутентичность и неизменность данных на основе использования уникальных квантовых цифровых подписей;
- более точное прогнозирование и эффективную выдачу оптимального решения проблемной ситуации в условиях информационной неопределенности;
- выявление аномалий и корреляцию разрозненных цифровых данных благодаря интеграции квантовых алгоритмов в системы искусственного интеллекта.

Квантовое криминалистическое обеспечение расследования преступлений стоит рассматривать как перспективу развития интеллектуализации процесса расследования преступлений.

Именно сочетание квантовых вычислений и технологий искусственного интеллекта рассматривается как синергия научно-технологического прогресса, определяющая новую парадигму QAI (от англ. «quantum artificial intelligence» –

⁵⁶² Прикладные квантовые технологии для защиты информации / Андрущенко А. С., Борисова А. В., Жилиев А. Е. и др. М. : Медиа Группа Авангард, 2023. С. 21.

⁵⁶³ Kumar M., Mondal B. A brief review on quantum key distribution protocols // Multimedia tools and applications. 2025. № 343. P. 3.

квантовый искусственный интеллект)⁵⁶⁴ – объединения вычислительной мощности квантовых систем с возможностями распознавания закономерностей и обучения моделей на основе искусственного интеллекта в целях повышения эффективности анализа данных и обеспечения принятия решений в условиях информационной неопределенности.

Таким образом, квантовый искусственный интеллект представляет собой новый вектор развития методов криминалистики, интеграция которого в существующие методики расследования станет важным шагом в противодействии современным и будущим киберугрозам.

В заключение необходимо выделить перспективные направления интеллектуализации процесса расследования преступлений в различных областях:

- внедрение когнитивных технологий анализа больших данных, в том числе разнородных, а также методов извлечения сведений из информационных массивов для решения задач выявления и раскрытия преступлений;
- моделирование ситуаций с целью упреждающего получения данных о возможных зонах с повышенным риском преступных проявлений;
- создание и внедрение в практику систем поддержки принятия решений;
- создание унифицированных информационных ресурсов, предоставляющих доступ к единым и пространственно-распределенным базам данных и хранилищам информации.
- разработка централизованной информационной платформы сбора и обработки цифровых данных о различных сферах общественной жизни;
- разработка комплексных аппаратно-программных средств с возможностью поиска следов противоправной деятельности в цифровых средах;
- использование современных методов сбора, обработки и анализа цифровых данных, в том числе методов искусственного интеллекта и квантовых технологий в криминалистике и т. п.

⁵⁶⁴ Tarafdar R. Quantum AI: the future of machine learning and optimization // World journal of advanced research and reviews. 2025. V. 25. №. 2. P. 2744; Chauhan D. Ranka P., Pritika B. Applications of quantum artificial intelligence: a systematic review // Integration of AI, quantum computing, and semiconductor technology. 2025. P. 159; Azeez M., Ugiagbe U., Albert-Sogules I. Quantum AI for cybersecurity in financial supply chains: enhancing cryptography using random security generators // World journal of advanced research and reviews. 2024. V. 23. №. 1. P. 2444.

Внедрение технологических решений, разработанных на основе искусственного интеллекта, в различные отрасли экономики и сферы общественных отношений связано со сквозным характером применения систем, разработанных на основе искусственного интеллекта, и потребностью в формировании кластеров данных для их обучения, с необходимостью автоматизированной обработки больших массивов цифровых данных, высокой степенью влияния указанных разработок на результативность деятельности человека и относительной доступностью инструментов, позволяющих разрабатывать интеллектуальные модели.

Описанные предложения соответствуют перспективным направлениям научно-технического развития системы МВД России в области цифровой трансформации, плану мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий на 2025–2028 г.г., а также целям реализации Стратегии развития искусственного интеллекта в Российской Федерации, согласно которой должны быть созданы условия для обеспечения национальной безопасности и правопорядка в стране, роста благосостояния и качества жизни населения, а также эффективного взаимодействия государства, организаций и граждан в сфере развития искусственного интеллекта.

Дальнейшего внимания заслуживает вопрос, связанный с развитием технологий сбора и анализа данных, а также потребностью в формировании криминалистических кластеров данных для формирования моделей на основе искусственного интеллекта, что соответствует приоритетам, обозначенным в Стратегии развития информационного общества в Российской Федерации на 2017–2030 г.г.

5.2. Концепция нейросетевого криминалистического кластера данных как основа систематизации криминалистически значимой компьютерной информации

Несмотря на динамичное развитие общей теории криминалистики, например, путем ее дополнения частными криминалистическими теориями, релевантные на сегодняшний день обзоры, посвященные выявлению проблем в области расследования преступлений в сфере компьютерной информации⁵⁶⁵, позволяют сделать вывод о значимости собирания цифровых доказательств и необходимости автоматизации процесса их исследования, что обусловлено сложностями анализа больших массивов данных в электронном виде.

Рассматривая способ понимания действительности в виде совокупности наиболее существенных элементов теории или системы взглядов, объединенных в логическую систему на основе определенных принципов, категорий и законов⁵⁶⁶, можно изложить концепцию систематизации криминалистически значимой компьютерной информации в целях формирования кластера обучающих данных для интеллектуального программного технико-криминалистического средства.

На сегодняшний день информация, являясь одним из наиболее ценных продуктов для мирового сообщества, часто становится объектом преступного посягательства, при этом информационные технологии служат орудием такого рода правонарушений. В результате «оцифровки» значительного объема пользовательских данных различными интернет-сервисами и веб-приложениями (сведения о пользовательских устройствах и их индивидуальных настройках, лог-файлы авторизации, поведенческие, персональные данные и т. п.), сформировалась возможность использования генерируемой информации в качестве основы для формирования информационно-аналитического кластера распределенных данных с функцией нейросетевого анализа⁵⁶⁷.

⁵⁶⁵ Horsman G., Sunde N. Unboxing the digital forensic investigation process // *Science and justice*. № 62. 2022. P. 176; Dunsin D., Ghanem M., Ouazzane K. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response // *Digital Investigation*. № 48. 2024. P. 3; Casino F., Dasaklis T., Research trends, challenges, and emerging topics in digital forensics: A review of reviews // *IEEE Access*. № 10. V. 2022. P. 25483; Машков С. А. «Большие данные» и криминалистика: возможности и перспективы // *Сибирские уголовно-процессуальные и криминалистические чтения*. 2024. № 2. С. 81.

⁵⁶⁶ Петровская В. Н., Щепин В. И. Концепции современного естествознания. Указ. соч. С. 38.

⁵⁶⁷ Харисова З. И. Концепция глобального нейросетевого криминалистического кластера данных в области противодействия преступлениям в сфере компьютерной информации // *Вестник Уфимского юридического института МВД России*. 2025. № 3 (109). С. 116.

Предлагаемый нейросетевой криминалистический кластер на основе общедоступной информации при условии соблюдения установленных нормативными правовыми актами ограничений в отношении распространения такой информации, аналогично криминалистическим учетам в цифровом виде, определил бы возможность гибкой настройки и выдачи отчетов по интересующим следствие направлениям. Необходимость поддержания инфраструктуры предлагаемой системы заключается в плановом и своевременном обновлении сформированных каталогов и инструментов для поиска данных, а также обеспечения соблюдения требований по обработке общедоступных источников, а также грамотного переобучения системы после обновления базы данных.

При этом, главной проблемой по формированию нейросетевого криминалистического кластера является отсутствие единых стандартов в подходе к охраняемой информации, в частности – персональные данные граждан различных стран. По этой причине актуальной задачей на этапе зарождения такого учета являлось бы формирование рассматриваемой информационной системы в рамках реализации для одного государства (национального кластера) либо возможностью создания массива кластеров данных при условии их обезличивания (путем введения условных идентификаторов). Достоинствами формирования нейросетевого криминалистического кластера данных являются повышение эффективности поиска необходимой для раскрытия или расследования информации за счет алгоритмизации этого процесса, удобство обработки значительного количества данных с использованием ключевых слов и фильтров в едином сегменте сети, хранения и использования цифровых доказательств, расширение механизмов оперативного доступа к данным, а также снижение трудозатрат и ресурсов по их поиску.

Эффективность раскрытия и расследования преступлений в большинстве случаев зависит от качества и количества криминалистически значимой информации, источниками которой могут быть как материальные и идеальные следы, так и слеодообразующие объекты⁵⁶⁸. К такого рода информации относят находящиеся в причинно-следственной связи с преступлением данные или сведения, которые, например, могут характеризовать способ и средства его совершения, объект, субъект или предмет преступного посягательства и пр.

⁵⁶⁸ Аверьянова Т. В. Криминалистика. Указ. соч. С. 382.

Потребности правоохранительных органов в настоящее время ставят перед криминалистикой задачи, связанные с разработкой новых наукоемких информационных систем идентификации личности, средств накопления, передачи и использования криминалистически значимой информации, методов фиксации, предварительного и судебно-экспертного исследования технических средств⁵⁶⁹.

Процесс накопления, обработки, поиска и хранения криминалистически значимой информации, объединенной общими характеристиками, позволяет формировать информационно-поисковые системы, которые способствуют решению диагностических, классификационных и идентификационных задач. Системы объектов в виде баз данных или хранилищ информации представляют собой криминалистическую регистрацию, система средств которой складывается из подсистем (криминалистических учетов), отличающихся друг от друга учитываемыми данными, способами или формами их систематизации.

Назначение криминалистического учета сводится к тому, чтобы по заранее зафиксированным и определенным образом систематизированным регистрационным признакам, способам совершения преступления, объектам посягательств и т. п. устанавливать личность преступника⁵⁷⁰.

С появлением нового вида регистрируемых объектов может, соответственно, возникнуть новый вид учета⁵⁷¹. В рамках рассмотрения преступлений в сфере компьютерной информации стоит отметить одну из успешно функционирующих на сегодняшний день подсистем программно-технического комплекса интегрированного банка данных федерального уровня Главного информационно-аналитического центра МВД России «Дистанционное мошенничество»⁵⁷², которая предназначена для систематизации и анализа сведений данных, образующихся в ходе предварительного расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий дистанционным способом, а также в процессе проверки сообщений (заявлений) о вышеуказанных преступлениях.

⁵⁶⁹ Федоров Г. В. Инновационные направления развития криминалистики. Указ. соч. С. 214.

⁵⁷⁰ Выявление причин преступности и предупреждение преступлений. Общие положения / под. ред. П. Ф. Гришанина. Указ. соч. С. 116.

⁵⁷¹ Курс криминалистики. Указ. соч. Т. 1. С. 451.

⁵⁷² Абросимова Ю. М. Совершенствование информационно-аналитического обеспечения в системе МВД России при помощи формирования, ведения и использования подсистемы «Дистанционное мошенничество» ПТК ИБД-Ф // Вестник Барнаульского юридического института МВД России. 2022. № 2 (43). С. 71.

Подсистема «Дистанционное мошенничество» позволяет аккумулировать информацию о способах совершения преступлений, идентификационных данных о мобильных средствах связи (IMEI), номерах банковских счетов и карт, сетевых адресах, электронных ящиках и кошельках, используемых при совершении преступного деяния, идентификаторах абонентов (IMSI), фабуле дела, а также лицах и документах, фигурирующих в нем, сумме причиненного ущерба, реквизитах организаций, зафиксированных в материалах проверки сообщения о происшествиях (преступлениях), серийности преступных деяний и пр.

Таким образом, одной из важнейших задач, решаемой интегрированным банком данных федерального уровня (ИБД-Ф), является подготовка сводной аналитической и статистической информации в целях формирования и ведения централизованных учетов. В настоящее время насчитываются десятки различных учетов, которые в зависимости от особенностей учитываемых объектов и характеризующих их признаков подразделяются на оперативно-справочные, криминалистические и справочно-вспомогательные учеты. Криминалистическая регистрация является систематизированным научно обоснованным учетом и основой информационного обеспечения правоохранительных органов сведениями об объектах и лицах в сфере уголовного судопроизводства и оперативно-розыскной деятельности.

На сегодняшний день информационное обеспечение осуществляется преимущественно на основе различных технических средств ввода, обработки и хранения информации и представлено автоматизированными информационно-поисковыми системами и банками данных, системами их управления, экспертными, фактографическими, справочными системами⁵⁷³ и т. п.

Возможности криминалистических учетов в системе информационного обеспечения следственной деятельности обусловлены тем, что это наиболее организованная и технически оснащенная ее часть⁵⁷⁴. С учетом того, что криминалистическая регистрация определяется перечнем учетных объектов, набор которых диктуется существующим уровнем технического развития, одним из вариантов решения проблем, связанных с поиском, анализом и исследованием цифровых следов, является введение новой системы регистрации цифровых доказательств с возможностью их систематизации и оперативного поиска.

⁵⁷³ Ищенко П. П. Информационное обеспечение следственной деятельности. Указ. соч. С. 16.

⁵⁷⁴ Ищенко П. П. Криминалистические учеты: свойства объектов и развитие системы // Вестник криминалистики. 2008. № 2 (26). С. 87.

Формами криминалистических учетов, входящих в указанную систему криминалистической регистрации цифровых доказательств, могут являться документированная информация, структурированные базы данных со сведениями о технических средствах и их сетевой активности, программное обеспечение, в том числе вредоносное, веб-ресурсы, аудио- и видеозаписи, а также их смешанные варианты.

В связи с этим предлагается ввести новый криминалистический учет, который выступит кластером обучающих данных для информационной системы, используемой в целях систематизации криминалистически значимой компьютерной информации, построения алгоритмов расследования⁵⁷⁵ и моделирования преступлений⁵⁷⁶ в сфере компьютерной информации. Криминалистические учеты могут систематизироваться по функциональному назначению, объектам, способу, масштабу ведения и другим основаниям.

Основными источниками информационного обеспечения следственной деятельности в настоящее время являются криминалистические регистрационные системы правоохранительных ведомств, ведомственные учеты правоохранительных органов, не затрагивающие преступную деятельность, различные информационные системы государственных органов власти и управления, учреждений, организаций и предприятий различных форм собственности, информационные ресурсы научно-методического и справочного содержания⁵⁷⁷, а также сведения, размещенные в киберсреде (геопространственные данные об объектах исследования, профилях в социальных сетях и пр.), метасреде (сведения о цифровых аватарах, пользовательской активности и т. п.) и в распределенных реестрах (данные, собранные в сетях «Тор», «I2P», сведения о криптовалютных операциях, площадках незаконного оказания услуг и пр.).

⁵⁷⁵ Волчецкая Т. С. Современные направления развития криминалистики как науки и как учебной дисциплины // Вестник Башкирского университета. 2015. Т. 20. С. 351; Драпкин Л. Я., Долинин В. Н., Шуклин А. Е. Проблемы алгоритмизации в криминалистике и следственной деятельности. Указ. соч. С. 31; Бахтеев Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности. Указ. соч. С. 35.

⁵⁷⁶ Каминский, М. К. Криминалистическая модель «компьютерных преступлений» // Вестник Удмуртского университета. 1996. № 1. С. 70.

⁵⁷⁷ Ищенко П. П. Информационное обеспечение следственной деятельности. Указ. соч. С. 28.

Исходными документами, формирующими интегрированный банк данных⁵⁷⁸, являются информационно-поисковые карты, идентификационные карты, опознавательные карты, учетные алфавитные карты и обычные карты (например, постановление по федеральному розыску и пр.)⁵⁷⁹.

Перечисленные ресурсы довольно широко используются следователями, но, зачастую, бессистемно, эпизодически, либо не в полном объеме. Для повышения эффективности их использования необходима систематизация имеющихся данных, обеспечивающая организацию информационных потоков и удобный к ним доступ. Помимо системы, объединяющей источники информационного обеспечения, целесообразно выделение категорий средств, которые позволят обработать и проанализировать сформированные данные, к которым можно отнести, например, средства связи и доступа к информации, управления данными и фильтрации информации, анализа и визуализации данных, программные технико-криминалистические средства, автоматизированные рабочие места сотрудников правоохранительных органов и пр. Рост числа учитываемых свойств, средств и способов совершения преступлений в сфере компьютерной информации, а также цифровых следов приведет к возникновению новых видов учета (в том числе коллекционных⁵⁸⁰), формированию экспертных фондов⁵⁸¹ и расширению круга учитываемых признаков. Увеличение объема регистрируемых данных и доступных информационных ресурсов, а также создание новых и совершенствование уже существующих криминалистических учетов является перспективным направлением развития информационного обеспечения следственной деятельности⁵⁸².

Средством преодоления «нестыкуемости» различных существующих информационных систем, используемых при расследовании преступлений, может являться унификация системы криминалистических учетов, а также внедрение и совершенствование средств информационного обеспечения в виде программных технико-криминалистических средств, которые не являются источниками

⁵⁷⁸ Volchetskaya T. S., Pankina I. Y., Makarova O. A. Problems of using modern proof technologies in jury trial // Vth Khmyrovsky criminalistic readings : conference proceedings. 2022. P. 72.

⁵⁷⁹ Якушев Д. И. Специальные информационные технологии в правоохранительной деятельности : учебно-методическое пособие. СПб. : СПбУ МВД России. 2024. С. 27.

⁵⁸⁰ Полещук О. В. Формирование и использование криминалистических коллекций в раскрытии и расследовании преступлений : монография. М. : Юрлитинформ, 2011. С. 11.

⁵⁸¹ Мирский Д. Я. Создание информационных фондов в области судебной экспертизы: методические рекомендации. М. : ВНИИ судебных экспертиз, 1984. С. 6.

⁵⁸² Белкин Р. С. Курс криминалистики. Указ. соч. С. 385.

криминалистически значимой информации, но обеспечивают процесс получения, обработки, хранения, поиска и предоставления по запросу необходимых данных. Таким образом, для более эффективного использования экспертно-криминалистических учетов в раскрытии и расследовании преступлений целесообразно интегрировать различные виды учетов в единую систему, что позволит установить корреляционные связи между объектами разных видов учетов⁵⁸³. В такого рода системе должен быть предусмотрен функционал для определения связей между следами, оставленными преступником в информационной системе или техническом средстве или изъятыми в рамках одного преступного деяния, с другим комплексом следов, изъятым с иного объекта. Соответственно, на начальном этапе расследования с использованием интегрированных учетов появится возможность решения задачи построения модели личности предполагаемого преступника⁵⁸⁴, а отчасти и модели преступного деяния.

Отдельного внимания в рамках данной концепции заслуживает вопрос обеспечения безопасности работы с персональными данными, которые могут входить в структуру больших данных и обладать самостоятельным правовым режимом. Если персональные данные, включенные в массив криминалистически значимой информации, подвергнуты процессу анонимизации, при котором невозможна их последующая идентификация даже с использованием различных технологий обеспечения информационной безопасности, такие сведения перестают подпадать под определение персональных данных в правовом смысле. При этом такого рода процесс будет представлять собой анонимизацию и отличаться от обезличивания, поскольку данные не смогут быть деанонимизированы при наличии дополнительных сведений. В иных случаях, когда сведения предполагаются «идентифицируемыми», их обработка должна требовать получения согласия субъекта персональных данных.

Повысить эффективность расследования преступлений в сфере компьютерной информации за счет систематизации, классификации и автоматизированного анализа цифровых следов позволит интегрированная система учета цифровых доказательств, структурными элементами при реализации которой

⁵⁸³ Аминев Ф. Г. Актуальные проблемы формирования и использования экспертно-криминалистических учетов в расследовании и раскрытии преступлений : монография. Уфа : РИО БашГУ, 2004. С. 155.

⁵⁸⁴ Жбанков В. А. К вопросу о понятии и содержании поисковой деятельности по установлению личности неизвестного преступника // Проблемы криминалистической теории и практики : сборник научных трудов. Москва : Юридический институт МВД России, 1995. С. 122.

могут выступить подсистемы сбора и агрегации данных, их классификации и структурирования, анализа и оценки, хранения и обмена данными, а также генерации отчетов и визуализации⁵⁸⁵ (Рисунок 4).



Рисунок 4 – Структура системы криминалистической регистрации цифровых доказательств по преступлениям в сфере компьютерной информации

Так, подсистема сбора и агрегации данных обеспечит оперативный сбор разнородных цифровых доказательств из множества источников, например, с локальных носителей данных, серверов, облачных хранилищ, технических средств, а также элементов IoT, сетевых маршрутизаторов, журналов криптовалютных транзакций, адресов электронных кошельков, межсетевых экранов, прокси-серверов, систем обнаружения вторжений и пр.

Подсистема классификации и структурирования доказательств в зависимости от заданных критериев и способов стандартизации данных обеспечит их систематизацию и разделение по типу, например, на текстовые файлы, бинарные данные, лог-файлы, метаданные, графические данные, аудио- или видеозаписи, а также классификацию по временным меткам и корреляцию событий (создание временных шкал, выявление закономерностей взаимодействия между событиями (например, совпадение времени доступа к информационной системе и осуществление несанкционированного доступа к компьютерной информации)).

Подсистема анализа и оценки доказательств позволит осуществить аналитическую обработку собранных данных, выявить скрытые взаимосвязи между событиями на основе методов машинного обучения, кластеризации, предсказания сценария развития преступления, оценки достоверности цифровых доказательств и их весомости.

⁵⁸⁵ Ищенко Е. П. У истоков цифровой криминалистики // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 3 (55). С. 24.

Подсистема хранения и обмена данными обеспечит их централизованную сохранность в виде базы данных, обеспеченной функциями индексирования, шифрования и контроля доступа, интеграцию с национальными и международными реестрами криминалистически значимых данных с возможностью обмена информацией для оперативного реагирования, а также аудит и протоколирование для фиксации изменений и доступа к данным.

Подсистема генерации отчетов и визуализации послужит гибким инструментом для построения отчетов в наглядной форме (дашбордов (от англ. «dashboard» – панель управления), диаграмм, временных линий, графов связей между событиями, а также статистических сводок с возможностью формирования выводов на основе пользовательских запросов и анализа шаблонов на базе обученных ранее данных).

В систему криминалистического учета по преступлениям в сфере компьютерной информации целесообразно включить:

1. Подсистему учета зарегистрированных преступлений для сбора и систематизации информации о каждом зарегистрированном преступном деянии, включая дату, время, место, способ совершения преступления, используемые средства, предмет преступного посягательства, размер ущерба. Источниками формирования указанной подсистемы могут являться, например, заявления потерпевших, сообщения о преступлениях, поступившие из иных источников (например, от провайдеров интернет-услуг, компаний, специализирующихся на обеспечении информационной безопасности и защиты информации), материалы уголовных дел прошлых лет. Объектами подсистемы могут выступить специально разработанные карты учета, содержащие структурированные данные об основных обстоятельствах преступления.

2. Подсистему учета лиц, совершивших преступления, для систематизации информации о подозреваемых или обвиняемых лицах, включая анкетные данные, сведения о судимостях, используемые учетные данные, IP-адреса и MAC-идентификаторы принадлежащих им устройств, адреса электронной почты, аккаунты в социальных сетях и мессенджерах, профессиональные навыки и умения. Источниками формирования указанной подсистемы могут являться материалы уголовных дел, оперативно-розыскная информация, а также данные, полученные в результате проведения следственных действий, информация, предоставленная иностранными правоохранительными органами и пр.

3. Подсистему учета средств совершения преступлений для сбора информации о задействованных технических средствах и программном обеспечении, включая их характеристики, происхождение, способы задействования. Источниками формирования указанной подсистемы могут являться материалы уголовных дел, заключения экспертов, информация, полученная в результате анализа вредоносного программного обеспечения, данные, предоставленные компаниями, специализирующимися на обеспечении информационной безопасности и защиты информации.

4. Подсистему учета цифровых следов преступлений и мест их расположения для систематизации информации о цифровых следах, оставляемых различными средствами совершения преступлений (например, лог-файлы, дампы памяти, особенности прохождения сетевого трафика), а также о местах их наиболее вероятного расположения (например, журналы серверов, файлы операционной системы, баз данных и пр.). Источниками формирования указанной подсистемы могут являться материалы уголовных дел, заключения экспертов, научные исследования в области противодействия преступлениям в сфере компьютерной информации, базы данных сигнатур вредоносного программного обеспечения и пр. Объектами подсистемы могут выступить специально разработанные карты учета, содержащие структурированные справочники цифровых следов, содержащие их описания, характеристики и типичные места расположения, а также связи с конкретными способами совершения преступлений.

5. Подсистему учета криминалистически значимой информации об обстановке совершения преступлений для выявления и систематизации факторов, способствовавших совершению преступления. Источниками формирования указанной подсистемы могут являться материалы уголовных дел, данные, полученные в результате анализа открытых источников (OSINT-разведка), информация, предоставленная потерпевшими и пр.

Криминалистический учет по преступлениям в сфере компьютерной информации может осуществляться по следующим основаниям:

- по способу совершения преступления и использованным средствам (MAC-идентификаторы, IP-адреса, серийные номера, IMEI-коды, лицензии программ и пр.);
- по способу сокрытия следов преступления и используемым при этом техническим средствам и программному обеспечению;
- по месту и времени задействования технических средств при совершении преступления;

- по лог-файлам и журналам событий в информационной системе и программном обеспечении;
- по сетевому трафику, сетевым артефактам;
- по сигнатурам распространяемого вредоносного кода и паттернам аномального поведения (коллекциям вредоносного программного обеспечения);
- по учетным записям и идентификаторам в сети «Интернет»;
- по цифровым аватарам в метасреде;
- по идентификаторам в сетях «Tor» и «I2P»;
- по хэш-суммам используемых при совершении преступления файлов (программного обеспечения);
- по поддельным электронным документам, цифровым подписям и сертификатам;
- по используемым при совершении преступления веб-ресурсам;
- по биометрическим данным;
- по метаданным мультимедиаконтента;
- по скомпрометированным данным;
- по синтетически сгенерированному контенту (дипфейк-контент);
- по идентификаторам криптовалютных транзакций и прочим финансовым операциям.

Таким образом, формирование нового криминалистического учета по преступлениям в сфере компьютерной информации является важным шагом на пути повышения эффективности их расследования.

Указанная система должна учитывать специфику цифровой среды, обеспечивать сбор, систематизацию и анализ информации о различных аспектах преступных деяний, а также соответствовать требованиям законодательства в области защиты персональных данных и обеспечения информационной безопасности.

Дифференциация учетов производится по их целевому назначению и особенностям учитываемых объектов, способам выявления и фиксации признаков, характеризующих объекты учета, особенностям организации учетов.

По уровню централизации предлагаемый криминалистический учет может формироваться как: региональный (ведется на уровне региона информационными центрами МВД России, региональными органами внутренних дел, экспертно-криминалистическими управлениями или центрами, подразделениями уголовного розыска); централизованный (ведется центральными аппаратами МВД России,

Главным информационно-аналитическим центром МВД России и Экспертно-криминалистическим центром МВД России) и централизованно-местный (ведется с целью регистрации однотипных объектов на местном или централизованном уровнях).

Предложенная система учета цифровых доказательств сможет послужить в дальнейшем основой для формирования модульной и масштабируемой платформы поддержки принятия решений (Рисунок 5), позволяющей собирать, классифицировать и анализировать цифровые доказательства в режиме реального времени, использовать современные методы анализа на основе искусственного интеллекта для выявления закономерностей и оценки вероятности развития событий, обеспечить безопасное хранение и обмен данными с возможностью интеграции с существующими национальными и международными системами, а также реализовать комплексное программное технико-криминалистическое средство с возможностью формирования типовых следственных версий и планов расследования преступлений в сфере компьютерной информации.



Рисунок 5 – Элементно-структурная схема соотношения цифровой модели преступления в сфере компьютерной информации с нейросетевым криминалистическим кластером данных (объектно-онтологическая схема)

Оптимизация процесса поиска, анализа и интерпретации цифровых доказательств возможна с применением алгоритмов искусственного интеллекта не только в отношении реализации программных технико-криминалистических средств, но и в совокупности с формируемым цифровой моделью преступления кластером цифровых доказательств в виде криминалистических учетов и системой поддержки принятия решений.

Предлагаемый подход к анализу данных, нахождению закономерностей, идентификации связей и корреляций между переменными и построению моделей с использованием инструментов визуализации по своей сути представляет собой технику EDA-анализа⁵⁸⁶ (от англ. «exploratory data analysis» – разведочный анализ данных) в виде комплекса методик, позволяющих исследовать, нормализовать и стандартизовать данные, определять их качество, структуру и характеристики, а также выявлять аномалии среди них⁵⁸⁷. Таким образом, в эпоху цифровизации и растущего объема данных необходимо применение EDA-техник в криминалистике, которые обладают существенным потенциалом, являясь перспективой в области совершенствования всех имеющихся экспертных систем и криминалистических учетов.

Подводя итог вышеуказанному, можно отметить, что криминалистика приобретает новые исследовательские и практико-ориентированные возможности благодаря применению современного стека индустрий Web 4.0 и Web 5.0, которые представлены технологиями искусственного интеллекта, распределенного реестра, сверхвысокой передачи данных, а также EDA-анализа, что, в свою очередь, может обеспечить формирование не только дополнительного источника информационного обеспечения следственной деятельности, но и полноценного набора данных для цифровой криминалистической модели преступления в сфере компьютерной информации (модели цифрового двойника преступления).

⁵⁸⁶ Тьюки Дж. Анализ результатов наблюдений. Разведочный анализ. М. : Мир, 1981. С. 18.

⁵⁸⁷ Маунт Д. Погружение в аналитику данных. СПб. : БХВ-Петербург, 2023. С. 19.

5.3. Цифровая криминалистическая модель преступления в сфере компьютерной информации (модель цифрового двойника преступного деяния) на основе нейросетевого криминалистического кластера данных

Вопросы совершенствования методик расследования преступлений в сфере компьютерной информации, в том числе интеграции различных информационных технологий в процесс расследования за последние годы рассматривались довольно часто и подробно. Однако рассматриваемые преступления отличаются значительным своим многообразием и трансформацией с течением времени, что объясняет сложность в определении эффективных мер расследования. Стоит также отметить недостаток имеющихся на сегодняшний день сведений по систематизации методик их расследования как в отечественной, так и в зарубежной литературе. Имеющиеся в настоящее время работы, посвященные криминалистическому обеспечению расследования преступлений в сфере компьютерной информации, носят в большинстве случаев неупорядоченный и фрагментарный характер. Часто при выявлении особенностей преступных деяний изучается лишь отдельно взятое преступление, как следствие, формируется узконаправленная методика расследования именно рассмотренного криминального акта.

Вопросы интеграции информационных технологий в процесс расследования, как правило, также носят рекомендательный или обзорный характер и, как правило, не затрагивают промежуточные процессы систематизации и анализа разнородных данных по той или иной группе преступных деяний. По этой причине необходимо рассмотреть возможность структурирования имеющихся сведений по рассматриваемой теме, систематизации особенностей учета указанных преступных деяний и унификации процесса их расследования.

Разработку дифференцированных методических рекомендаций с учетом специфики расследования преступлений определенного вида и сложившихся криминальных ситуаций обеспечивает ситуационный подход к преступной деятельности⁵⁸⁸. Интеграция знания, касающегося проблем принятия решений, криминалистической характеристики преступления и криминалистической характеристики расследования, со знаниями таких научных дисциплин, как кибернетика, информатика, психология и теория управления, обеспечивает

⁵⁸⁸ Волчецкая Т. С. Теоретические проблемы использования метода моделирования в криминалистической науке. Указ. соч. С. 17.

построение типовых моделей криминальной и следственной ситуаций⁵⁸⁹, а в совокупности с текущим фондом знаний в области информационных технологий, теории принятия решений и науки о данных позволяет построить цифровую криминалистическую модель преступления в сфере компьютерной информации – модель цифрового двойника преступного деяния. В связи с этим ставится задача рассмотрения указанной модели в целях формирования адаптированных методик расследования в условиях постоянной трансформации и эволюции киберпреступлений.

Под моделью в криминалистике понимается искусственно созданная система, которая способна воспроизвести или заменить исследуемое преступное деяние или отдельную следственную ситуацию и прочие сопутствующие обстоятельства с целью получения об оригинале (объекте моделирования, исходном событии) дополнительной информации, необходимой для расследования или успешного решения иной поставленной задачи. Создание цифрового двойника преступного деяния предполагает формирование модели, обладающей необходимыми для исследования сходствами с оригиналом преступления (исходным криминальным событием или явлением), что позволяет обеспечить последующее исследование этой модели в качестве средства получения криминалистически значимой информации.

Метод моделирования во всех сферах научного познания является важнейшим из доступных методов исследования и может быть применен в случаях, требующих исследования событий или явлений в исходном виде, процессов, имевших место в прошлом, объектов исчезнувших, отсутствующих частично, либо существование которых является лишь предположительным или вероятностно-прогнозируемым. Указанный подход позволяет исследовать такое явление как преступление, которое, являясь событием прошлого, недоступно для восприятия и исследования в исходном виде.

Процесс моделирования позволяет обеспечить решение следующих криминалистических задач: снижение информационной неопределенности (за счет получения дополнительных криминалистически значимых сведений); планирования; управления ходом расследования и прогнозирования раскрытия преступного деяния; формирование оптимальной методики расследования преступления; принятия оптимального и эффективного решения по управлению ситуацией.

⁵⁸⁹ Волчецкая Т. С. Криминалистическая ситуалогия. Указ. соч. С. 23.

В ряде случаев использование модели вместо натурального объекта представляется более целесообразным, так как позволяет значительно упростить исследование, требует меньших усилий и материальных затрат, ускоряет процесс исследования⁵⁹⁰.

Особую практическую значимость такой подход приобретает в связи с возможностью получения следователем ориентирующих сведений в условиях высокой степени информационной неопределенности.

Рассматривая в качестве объектов криминалистики две взаимообусловленные системы «преступления» и «расследования», необходимо отметить, что модель расследуемого события (преступления) отражает содержание элементов криминалистической характеристики преступного деяния, в то время как модель «расследования» может отражать организацию, планирование или методику расследования. Стоит также отметить, что любая информационная модель преступления до момента вынесения по уголовному делу судебного решения или приговора носит вероятностный характер, что выступает отличительной особенностью при рассмотрении соотношения типовой модели преступлений определенного вида и типовой криминалистической характеристики, требующей высокой степени достоверности, выявления закономерностей между ее элементами, вычисления корреляционных зависимостей⁵⁹¹. Соответственно, типовая криминалистическая характеристика является результатом исследования, проводимого на типовой модели преступления определенного вида.

Подавляющее большинство определений криминалистической характеристики представлены лишь в виде системы данных, способствующих раскрытию и расследованию преступлений, однако системно-структурный анализ набора составляющих криминалистическую характеристику признаков, как правило, не проводится⁵⁹². Поэтому в литературе все чаще отмечается, что качественно новым этапом должно являться создание типовой информационной модели преступления, которая на основе выявленных статистических зависимостей между ее элементами позволяет получать новый источник

⁵⁹⁰ Хлынцов М. Н. Криминалистическая информация и моделирование при расследовании преступлений. Саратов : Изд-во Саратов. ун-та, 1982. С. 4.

⁵⁹¹ Волчецкая Т. С. Криминалистическая ситуалогия. Указ. соч. С. 137.

⁵⁹² Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. Указ. соч. С. 135.

актуальной криминалистически значимой информации⁵⁹³.

Структурно-содержательный анализ элементов криминалистической характеристики преступлений в сфере компьютерной информации, структурирование и систематизация данных о преступных деяниях и упорядочение существующих их вариаций (система кодирования) с учетом рассмотренных закономерностей учения об интеллектуализации процесса расследования и принятия решений в условиях неопределенности позволяют перейти к формированию информационной модели преступления, которая может выступить основой создания интеллектуального программного технико-криминалистического средства с возможностью оперативной адаптации к новым вызовам цифрового пространства. Информационная система, построенная на основе статистической обработки репрезентативной выборки уголовных дел определенной категории, отражающая закономерные связи между элементами события преступления и используемая для построения типовых версий, а также формирования методики расследования данной категории преступлений представляет собой типовую информационную модель⁵⁹⁴, определяющую возможность перехода к процессу моделирования.

Правильный подход к выявлению и систематизации криминалистически значимых признаков преступлений при формировании модели преступления обеспечивает создание методик их расследования. Кроме того, типовая криминалистическая модель преступной деятельности определенного вида может выступать основой программы расследования, структурными элементами которой является комплекс типовых ситуаций, вытекающих из типовых следственных версий, а также взаимосвязанных с ними промежуточными задачами расследования и алгоритмами их решения⁵⁹⁵. Особенно велико значение типовых вероятностных моделей при расследовании дел в условиях высокой степени информационной неопределенности.

⁵⁹³ Ищенко Е. П., Колдин В. Я. Типовая информационная модель преступления как основа методики расследования. Указ. соч. С. 136; Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография. М. : Проспект, 2021. С. 21; Калужный А. Н. Виды корреляционных взаимосвязей данных криминалистической характеристики преступлений и их значение для процесса расследования // Научный вестник Орловского юридического института МВД России им. В. В. Лукьянова. 2025. № 1 (102). С. 222.

⁵⁹⁴ Колдин В. Я., Ищенко Е. П., Крестовников О. А. Типовая информационная модель или криминалистическая характеристика преступления // Академический юридический журнал. 2006. № 4. С. 13.

⁵⁹⁵ Колдин В. Я. Типовые модели и алгоритмы криминалистического исследования. Указ. соч. С. 95.

Наиболее перспективным методом моделирования в настоящее время является компьютерное моделирование, под которым понимается решение задач анализа или синтеза сложных систем на основе использования ее компьютерной модели, позволяющей учитывать большое количество переменных, предсказывать развитие нелинейных процессов, возникновение синергетических эффектов и дает возможность не только получить прогноз, но и определить, какие управляющие воздействия приведут к наиболее благоприятному развитию событий⁵⁹⁶.

Развитие информационных технологий и рост вычислительных мощностей компьютеров обусловило появление нового вида компьютерного моделирования – имитационного, которое предполагает представление модели в виде алгоритма, выполнение которого имитирует последовательность смены состояний в системе и таким образом представляет собой поведение моделируемого объекта или явления. Имитационная модель является универсальным средством исследования сложных систем в виде логико-алгоритмического описания поведения отдельных их элементов и их взаимодействий как последовательности событий, возникающих в моделируемой системе⁵⁹⁷. Такое восприятие моделирования хорошо согласуется с понятием цифровой криминалистической модели преступления, представляющей собой формализацию и представление информации о его криминалистически значимых признаках и их закономерных связях между собой в виде чисел и различных математических категорий⁵⁹⁸.

Формирование модели, как правило, имеет цель замены оригинала при исследованиях, которые, например, могут подвергнуть исходное его состояние нежелательным или недопустимым изменениям. Но непосредственная замена оригинала моделью возможна только в случае, если они в достаточной степени похожи. Соответствие сформированной модели оригиналу (моделируемому объекту) или процессу выражается адекватностью (от лат. «adaequatus» – приравненный). Проверку адекватности проводят на всех этапах построения модели начиная с самого первого этапа — концептуального анализа. Если описание системы будет составлено не адекватно реальной системе, то и модель, как бы

⁵⁹⁶ Вехов В. Б., Ковалев С. А. Компьютерное моделирование при расследовании преступлений в сфере компьютерной информации. Волгоград : ВА МВД России, 2014. С. 6.

⁵⁹⁷ Боев В. Д. Имитационное моделирование систем. М. : Юрайт, 2025. С. 30.

⁵⁹⁸ Бессонов А. А. Криминалистическая характеристика преступлений в цифровую эпоху // Развитие научных идей профессора Р. С. Белкина в условиях современных вызовов (к 100-летию со дня рождения) : сборник научных статей по материалам Международной научно-практической конференции. Т. 1 Ч. 1. М. : Академия управления Министерства внутренних дел Российской Федерации, 2022. С. 56; Бессонов А. А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности. Указ. соч. С. 60.

точно она ни отображала описание системы, не будет адекватной оригиналу.

Компьютерное моделирование объединяет достижения математического моделирования, системного программирования, информационных технологий и обладает способностью анализа данных и их интерпретации, использования формализованной и неформализованной информации (формул, логических правил, вербальных описаний и т. п.), заполняя пространство между математическим моделированием с его аналитическими формами описания и искусственным интеллектом с его формами и правилами представления знаний⁵⁹⁹.

Анализ данных применяется, как правило, в целях выполнения некой описательной, диагностической, предсказательной или предписывающей функции и является довольно востребованным процессом ввиду бурного роста объемов, разнообразия и скорости изменения данных и роста спроса на принятие решений на основе данных⁶⁰⁰.

Соответственно, среди методов анализа данных выделяют⁶⁰¹:

- описательный анализ для получения представления о том, что произошло или происходит в наборе данных;
- диагностический анализ (для понимания того, почему произошло то или иное явление), который характеризуется способностью детализации и обнаружения закономерностей в данных;
- предиктивный анализ, который используется для составления прогнозов на основе закономерностей в данных и обеспечивается машинным обучением в совокупности с предиктивным моделированием на базе причинно-следственных связей;
- предписывающую аналитику, которая обеспечивает как предсказание по исследуемому случаю, так и предложение оптимального решения проблемы за счет использования графовых нейронных сетей и рекомендательных механизмов машинного обучения.

Таким образом, совокупность методов анализа данных может обеспечить процесс моделирования систем, интерпретацию моделируемых событий, а также прогностические и рекомендательные функции для закладывания в интеллектуальное программное обеспечение.

С технологиями моделирования и анализа больших данных на основе

⁵⁹⁹ Боев В. Д. Имитационное моделирование систем. М. : Юрайт, 2025. С. 40.

⁶⁰⁰ Асито Ф. Предсказательная аналитика с KNIME. М. : ДМК Пресс, 2025. С. 15.

⁶⁰¹ Ватьян А. С., Гусарова Н. Ф., Добренко Н. В. Data science: проблемы и решения. СПб. : Университет ИТМО, 2025. С. 8.

искусственного интеллекта довольно тесно связана возможность формирования цифровых двойников. Цифровые двойники, играют одну из главных ролей в трансформации индустрии информационных технологий и являются одним из ключевых компонентов Индустрии 5.0⁶⁰².

Под цифровым двойником в общем смысле подразумевается виртуальный клон некоторого физического объекта (системы, явления) или процесса, фактически использующего знания в режиме реального времени для воспроизведения своего текущего состояния. Соответственно, цифровой двойник преступления представляет собой виртуальную модель, отражающую состояние и динамику реального преступного деяния в сфере компьютерной информации, позволяющую исследовать различные сценарии его совершения, выявлять закономерности между элементами его криминалистической характеристики, формировать алгоритм расследования преступления, выдавать вероятность его раскрытия. Так, например, широкое распространение получают цифровые двойники киберугроз⁶⁰³, которые позволяют специалистам в области обеспечения информационной безопасности и защиты информации выявлять уязвимости и принимать превентивные меры до того, как они будут использованы в реальной жизни, моделируя потенциальные кибератаки. В научной литературе уже рассматриваются возможности формирования цифровых двойников личности⁶⁰⁴, профиля человека⁶⁰⁵, систем сбора доказательств⁶⁰⁶, а также преступников на основе профилирования личности⁶⁰⁷ и пр.

⁶⁰² Dhanaraj R., Murugesan S., Balusamy B. Digital twin technologies for healthcare 4.0. London : The institution of engineering and technology, 2022. P. 25.

⁶⁰³ Sarker I. H. AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Perth : Edith cowan university, 2024. P. 28.

⁶⁰⁴ Иванов В. В., Зуев Д. И. Цифровой двойник и цифровая личность: понятие, соотношение, значение в процессе совершения киберпреступлений и в праве в целом // Правовое государство: теория и практика. 2022. № 4. С. 14.

⁶⁰⁵ Зайцев О. А., Пастухов П. С. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. № 56. С. 288.

⁶⁰⁶ К вопросу о создании цифровой криминалистической модели для сбора электронных доказательств при расследовании киберпреступлений / У. А. Мусаева, Т. Б. Нгуен, Т. Х. Нгуен и др. // Всероссийский криминологический журнал. 2024. Т. 18. № 4. С. 398.

⁶⁰⁷ Model of a domain-specific profiling system based on Explainable AI technologies / Z. I. Kharisova, V. V. Antonov, L. E. Rodionova, G. G. Kulikov // IOP Conference Series: Materials Science and Engineering. 2021. V. 1069. №. 1. P. 12001; Смушкин А. Б. О возможности вероятностного моделирования поведения лица с помощью цифрового двойника преступника // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели. М. : МГЮА, 2025. С. 144.; Халиков А. Н. Расследование преступлений в аспекте применения психологических знаний // Мир криминалистики. 2023. № 2. С. 96.

На основе изложенного можно сделать вывод, что вероятностное цифровое моделирование является весьма перспективным направлением в области интеллектуализации процесса расследования и повышения результативности расследования именно преступлений в сфере компьютерной информации, как наиболее опосредованных с цифровой информацией преступных деяний.

Функционирование цифрового двойника преступного деяния подразумевает непрерывный процесс аккумуляции данных о совершенном преступлении, начиная с момента возбуждения уголовного дела, до завершения стадии предварительного следствия или дознания, а также обмен данными между физическим объектом (процессом) и его виртуальной копией. Таким образом формируется иммерсивная метасреда воспроизведения преступного деяния (в восприятии метавселенных), что может способствовать дальнейшему «сближению» методов противодействия киберпреступности и метапреступности.

На начальном этапе формирования цифрового двойника осуществляется декомпозиция элементов, составляющих криминалистическую характеристику преступных деяний определенного вида, после чего проводится структурирование данных с использованием формализованных моделей, обеспечивающих интероперабельность и возможность интеграции с информационной системой. Для построения прогностической модели применяются методы статистического анализа данных, позволяющие выявлять корреляционные зависимости между элементами криминалистической характеристики и предсказывать возможное развитие следственных ситуаций. С целью повышения точности прогнозирования могут использоваться методы машинного обучения, включая алгоритмы классификации, кластеризации, регрессии и пр. Обучение моделей осуществляется на ретроспективных данных о совершенных преступлениях рассматриваемого вида, после чего формируются правила дедуктивного вывода, позволяющие на основе имеющихся данных о конкретном инциденте выдвигать гипотезы о применяемых средствах совершения преступления, личности преступника и других значимых обстоятельствах. На конечном этапе формируется модель, формализованно имитирующая объект-оригинал и обеспечивающая возможность моделирования различных сценариев развития преступной деятельности, интеграцию с криминалистическими кластерами данных и программными технико-криминалистическими средствами, а также визуализацию результатов моделирования. В обязательном порядке должна осуществляться верификация и валидация модели на предмет адекватности, тестирование на контрольных примерах с внесением корректировок, направленных на повышение ее точности.

Обмен данными осуществляется посредством передачи их в информационную систему, в которой формируется виртуальная модель объекта-оригинала, после чего допустимо осуществлять анализ данных на основе искусственного интеллекта с выдачей вероятностного результата.

Цифровой двойник преступного деяния в контексте правоприменительной деятельности может обеспечить:

- анализ цифровых следов, выявленных в ходе расследования;
- выдвижение и проверку следственных версий, направленных на установление обстоятельств, подлежащих доказыванию (на основе анализа данных, полученных в результате моделирования);
- выдачу рекомендаций, содержащих алгоритмы действий по расследованию конкретного преступного деяния, а также вероятность его раскрытия на основе результатов моделирования;
- разработку превентивных мер, направленных на предотвращение преступлений;
- использование модели для проведения тактических учений, направленных на выработку навыков выявления, раскрытия и расследования моделируемого вида преступлений.

Таким образом, цифровой двойник преступления в сфере компьютерной информации представляет собой перспективное направление развития криминалистической науки и практики. При правильном применении и грамотной интерпретации формируемых цифровым двойником данных такого рода инструмент может значительно повысить эффективность борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий в целом.

Программирование в виде средства доведения методических знаний до следователя, должно способствовать тому, чтобы в тех случаях, когда есть готовые оптимальные решения, следователь не занимался изобретением уже изобретенного, а брал и использовал готовое решение⁶⁰⁸. Аналогично решения на основе искусственного интеллекта могут представлять собой системы, выступающие источником знаний и рекомендаций для следователя, но не преумаляющие значимость его фигуры.

⁶⁰⁸ Соя-Серко Л. А. Программирование и творчество в деятельности следователя // Проблемы предварительного следствия в уголовном судопроизводстве. М. : Всесоюзный ин-т по изучению причин и разработке мер предупреждения преступности, 1980. С. 33.

Стоит отметить, что искусственный интеллект в настоящее время активно используется в области обнаружения киберугроз, как показывает всесторонний обзор, проведенный Институтами кибертехнологий и киберисследований Великобритании и Катара⁶⁰⁹, основными используемыми в этих целях методами являются машинное обучение, нейронные сети и генетические алгоритмы, а наиболее существенной проблемой признано отсутствие качественных и доступных наборов данных для обучения моделей искусственного интеллекта. Аналогичная тенденция складывается и в области расследования преступлений в сфере компьютерной информации, где основной проблемой является сложность формирования наборов обучающих данных, анализ значительных по объему массивов криминалистически значимой компьютерной информации, ее неструктурированность и отсутствие централизованного сбора.

Криминалистическая характеристика преступлений, одновременно как частная криминалистическая теория (в качестве инструментария для расстановки приоритетов и взаимосвязей между элементами), и как совокупность статистически обоснованных аналитических данных может выступить фундаментом для разработки систем искусственного интеллекта⁶¹⁰. Элементы криминалистической характеристики, закладываемые в качестве базы данных для интеллектуальных систем, должны иметь разный вес, поэтому крайне важным является расстановка отдельных параметров (установление критериев значимости) с точки зрения их воздействия на ход расследования.

При криминалистическом исследовании признакам и свойствам, присущим объекту исследования, дается качественная и количественная характеристика, выражение которой обычно достигается путем создания формализованной системы описания таких признаков и процедур их исследования⁶¹¹. Набор специальных алгоритмов, способный самообучаться на основе данных, от размера (объема) которого зависит точность выявления закономерностей и выдаваемого результата, называется машинным обучением. Среди многообразных парадигм и подходов машинного обучения выделяются модели и их реализации в виде программного обеспечения, которые в упрощенном виде имитируют работу биологической нейронной сети человека и именуются искусственными

⁶⁰⁹ Al-Khater W. A. et al. Comprehensive review of cybercrime detection techniques // IEEE access. 2020. V. 8. P. 137294.

⁶¹⁰ Бахтеев Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности. Указ. соч. С. 36.

⁶¹¹ Полевой Н. С Криминалистическая кибернетика. Указ. соч. С. 53.

нейронными сетями (нейросетями). Обучение таких сетей заключается в поиске набора весовых коэффициентов, при котором входной сигнал после прохода по нейросети преобразуется в нужного вида выходной. Для этих целей формируется обучающая выборка в виде набора входных и соответствующих им выходных (правильных) сигналов, т. е. происходит обучение на примерах с идеальными данными. Преимущество нейронных сетей в сравнении с моделями машинного обучения состоит в их способности выявлять нелинейные зависимости в данных без явного указания структуры модели или распределения переменных в наборе⁶¹². Наборы данных в исходном состоянии могут содержать большое количество признаков, в составе которых только часть могут быть действительно значимыми (т. е. будут иметь связь с целевой переменной), тогда как остальные выступают избыточными и лишь ухудшают качество выстраиваемой модели. Удаление избыточных данных позволяет сократить время настройки модели, улучшить ее точность и облегчить интерпретируемость⁶¹³.

Для выявления зависимостей в структуре преступной деятельности необходим анализ и обобщение большого массива дел определенной категории, что объясняется вероятностным характером при исследовании признаков преступлений как массовых случайных событий⁶¹⁴.

Необходимо отметить, что стабильный рост количества преступлений, совершаемых в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий, а также рост доли такого рода преступлений в общей структуре преступности, большая часть которых являются латентными, объясняют актуальность рассмотрения цифровой модели именно данного вида преступных деяний, при совершении которых часто используются одни и те же способы, методы и средства⁶¹⁵. Эмпирическую базу для проводимого моделирования составили сведения о 284 преступлениях в сфере компьютерной информации, совершенных за период с 2020 по 2025 г.г. Таким образом, в качестве основных данных для построения модели использован массив сведений из материалов уголовных дел (Приложение 7).

⁶¹² Асито Ф. Предсказательная аналитика с KNIME. Указ. соч. С. 289.

⁶¹³ Ватьян А. С., Гусарова Н. Ф., Добренко Н. В. Data science: проблемы и решения. СПб.: Университет ИТМО, 2025. С. 156.

⁶¹⁴ Колдин В. Я. Типовые модели и алгоритмы криминалистического исследования. Указ. соч. С. 36.

⁶¹⁵ Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. Указ. соч. С. 135.

При формировании модели использовано 30 переменных (признаков): вид преступления; способ совершения преступления; среда совершения преступления; средство совершения преступления; цифровые следы преступления; расположение цифровых следов преступления; способ сокрытия следов; серийность преступления; место совершения преступления; дата совершения преступления; время совершения преступления; идентификатор преступника; возраст преступника; пол преступника; образование преступника; род занятий преступника; судимость преступника; идентификатор потерпевшего; возраст потерпевшего; пол потерпевшего; образование потерпевшего; род занятий потерпевшего; предмет посягательства; ущерб потерпевшего; техника совершения преступления; подтехника совершения преступления; способы выявления; меры реагирования; факт раскрытия; алгоритм расследования.

Содержание переменных исходя из собранного эмпирического материала было представлено категориальными, бинарными и числовыми данными в виде отдельных признаков или их совокупности следующим набором:

- вид преступления «Crime_ID_Cx»;
- способ совершения преступления «Method_Mxxx»;
- среда совершения преступления «Scope»;
- средство совершения преступления «Means»;
- цифровые следы преступления «Traces»;
- расположение цифровых следов преступления «Trace_location»;
- способ сокрытия следов «Trace_hidden»;
- серийность преступления «Seriality»;
- место совершения преступления «Place»;
- дата совершения преступления «Date»;
- время совершения преступления «Time»;
- личность преступника [«Criminal_name», «Criminal_age», «Criminal_gender», «Criminal_edu», «Criminal_job», «Criminal_court»];
- личность потерпевшего [«Victim_name», «Victim_age», «Victim_gender», «Victim_edu», «Victim_job», «Victim_vulnerability», «Victim_damage»];
- техника совершения преступления «Txxxx»;
- подтехника совершения преступления «Sxxxx»;
- меры выявления «Dxxxx»;
- меры реагирования «Rxxxx»;
- раскрытие преступления «Revealed»;

– алгоритм расследования «Algorithm».

Присвоение весов элементам криминалистической характеристики рассматриваемых преступлений основывалось на приоритетности и значимости каждого составного элемента с точки зрения криминалистической ценности для раскрытия и расследования преступления. С этой целью были выделены значимые переменные, такие как «Method», «Scope», «Means», «Traces», «Trace_Location», «Trace_Hidden», «Seriality».

Отбор значимых признаков в наборе данных не только упрощает модель за счет снижения вычислительных затрат, но также повышает ее точность за счет высокой степени корреляции отдельных переменных с преступным событием⁶¹⁶.

Модель была обучена на наборе данных из 284 строк, которая по введенным пользователем данным предоставляет возможность прогнозирования вероятности его раскрытия и выдачи наиболее подходящего алгоритма расследования на основе сопоставления введенных данных и имеющейся в базе данных смоделированной системы сведений.

Большинство методов машинного обучения в настоящее время с целью построения точных и надежных моделей требуют большого количества данных, которые позволяют на их основе выявлять закономерности и зависимости между признаками, используемыми для выдачи прогноза или результатов на новых данных, таким образом, разнообразие и репрезентативность обеспечивают учет сложных зависимостей между переменными.

В реальных условиях сбор больших объемов данных может быть сложной задачей. Например, в рассматриваемой области сбор данных ограничен рядом юридических норм – сложностью обработки персональных данных, обезличиванием или анонимизацией данных, обеспечением сохранности сведений, необходимостью их структурирования, предобработки и пр. Это создает барьеры для применения традиционных методов машинного обучения, так как они становятся неэффективными при нехватке данных. Кроме того, обработка больших наборов данных требует значительных вычислительных ресурсов.

Проблема нехватки данных стимулировала разработку методов, способных работать с ограниченными объемами данных. Эти подходы, известные как обучение с малым количеством данных (от англ. «few-shot learning» – обучение по нескольким примерам), позволяют моделям извлекать максимум информации из

⁶¹⁶ Sarker I. H. AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Op. cit. P. 66.

небольших наборов данных и решать задачи, где традиционные методы менее эффективны⁶¹⁷. Такие методы основываются на принципах переноса знаний (использование информации, приобретенной во время предварительного обучения на одном наборе данных, для повышения ее эффективности при решении новых задач, на других наборах данных) и метаобучения (обучение модели решению не только конкретных задач, но и приобретению новой способности к самообучению, используя накопленный опыт). В отличие от традиционных методов, которые требуют тысяч примеров, обучение с малым количеством данных может успешно работать с небольшими объемами. Соответственно, обучение с малым количеством данных противопоставляется традиционным методам с основным упором не на количество, а на качество данных. Достаточность объема данных подтверждается полученными метриками точности, а также рядом подобных наборов, формируемых в целях моделирования современных киберугроз, уязвимостей и эксплойтов передового технологического ландшафта текущего времени⁶¹⁸.

Набор входных и соответствующих им выходных (правильных) сигналов, по которым происходит оценка качества работы сети после обучения на обучающей выборке выступает тестовой выборкой, т. е. на ее основе происходит контрольная работа на примерах с реальными данными. Набор данных, построенный на основе проведенного структурно-содержательного анализа элементов криминалистической характеристики преступлений в сфере компьютерной информации и содержащий 284 записи о преступлениях по 30 признакам, был разделен в соотношении 80 % данных, используемых для обучения модели и 20 % – для тестирования, что является стандартной практикой в машинном обучении для оценки модели. Предобработка предполагала проверку данных на предмет их качества, полноты и достоверности, а также кодирование признаков в зависимости от их типа (категориальные, бинарные и числовые), выявление, исключение или восполнение (например, методом экспертных оценок) пропущенных значений.

⁶¹⁷ Девис Дж. Обучение с малым количеством данных. М. : Литрес, 2024. С. 8.

⁶¹⁸ Обзор набора данных «Forensic Toolkit Dataset» // Официальный сайт платформы коллективной разработки моделей, наборов данных и приложений в сфере машинного обучения компании Hugging Face Inc. URL: https://huggingface.co/datasets/darkknight25/forensic_toolkit_dataset (дата обращения: 08.08.2025); Обзор набора данных «Kali linux toolkit dataset» // Официальный сайт платформы коллективной разработки моделей, наборов данных и приложений в сфере машинного обучения компании Hugging Face Inc. URL: https://huggingface.co/datasets/darkknight25/kali_linux_toolkit_dataset (дата обращения: 08.08.2025); Обзор набора данных «Modern cyber threat simulation dataset» // Официальный сайт платформы коллективной разработки моделей, наборов данных и приложений в сфере машинного обучения компании Hugging Face Inc. URL: https://huggingface.co/datasets/darkknight25/modern_cyber_threat_simulation_dataset (дата обращения: 08.08.2025).

Пропущенные значения в наборе данных могут являться, например, следствием допущения ошибок при сборе информации, отсутствия сведений о тех или иных признаках, что довольно часто встречается для случаев, когда личность преступника была не установлена, или когда при совершении преступления использовались средства анонимизации. Кроме того, выявление пропусков в наборах данных и изучение их структуры, несмотря на отсутствие информационной составляющей, могут служить основанием для выделения новых взаимосвязей между переменными и наблюдениями.

Проверка на качество модели показала, что модель хорошо обобщает данные и не переобучена. По результатам оценки эффективности модели на тестовом наборе данных получена точность прогнозирования вероятности раскрытия преступного деяния 96, 1 %.

Классификация и регрессия являются контролируемыми подходами обучения, часто используемыми в машинном обучении⁶¹⁹. В литературе по машинному обучению и анализу данных предложено множество алгоритмов классификации, но метод «дерево решений» является одним из самых эффективных и широко используемых инструментов такого рода. Метод k-ближайших соседей и опорных векторов, байесовский анализ, адаптивный бустинг, логистическая регрессия и т. д. также являются популярными методами в этой области. Ансамблевое обучение – еще один подход, который объединяет прогнозы из нескольких моделей для повышения эффективности прогнозирования. Например, метод случайного леса использует несколько деревьев решений для обнаружения аномалий. Для обработки данных применялся ряд методов математической статистики и алгоритмы искусственного интеллекта. В результате проведенного моделирования были выявлены типичные признаки преступлений, совершаемых в сфере компьютерной информации, а также закономерные связи между ними, использованные для обучения модели. На основе сформированной модели было разработано интеллектуальное программное технико-криминалистическое средство⁶²⁰, позволяющее на основе введенных пользователем данных о совершенном преступлении формировать наиболее соответствующий ему алгоритм расследования и определять вероятность

⁶¹⁹ Sarker I. H. AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Ind. ess. P. 50.

⁶²⁰ Свидетельство о государственной регистрации программы для ЭВМ № 2025680704 Российская Федерация. Cybercrime DT Model (AI) [Цифровой двойник киберпреступления] – цифровая криминалистическая модель преступления в сфере компьютерной информации : № 2025669600 : заявл. 31.07.2025 : опубл. 07.08.2025.

раскрытия смоделированного преступления с интерпретацией принимаемых моделью решений. Сформированное программное обеспечение представляет собой цифровую криминалистическую модель преступного деяния с учетом корреляционных связей по разнородным признакам. Идеального метода, одинаково показывающего себя на любом наборе данных и для решений абсолютно любых задач, не существует, ввиду того, что преступная деятельность является сложной, динамичной системой и требует для получения объективных и достоверных результатов любого ее исследования применения комплекса методов и, как правило, построения нескольких моделей⁶²¹. Эффективность выдаваемых интеллектуальной моделью результатов зависит также от объема вводимых данных и, как для любой экспертной системы справедливо, – чем больше вводных данных, тем точнее результат решения поставленной задачи.

На основе проведенного сравнительного анализа ряда моделей машинного обучения («LinearRegression» «LogisticRegression», «Random Forest», «GradientBoosting (XGBoost)», а также «GNN») для задачи предсказания вероятности раскрытия преступления наилучшие метрики показала модель на основе случайного леса «RandomForest (Regressor)», что подтверждается данными об ансамблевых методах машинного обучения обычно превосходящих простые линейные модели на сложных, многомерных данных (метрики качества: ROC-AUC (от англ. «receiver operating characteristic – area under curve» – метрика оценки качества бинарных классификаторов⁶²²) для моделей, предсказывающих принадлежность объекта к классу – 0,994; F1-метрика (F1-score или F-мера) оценки эффективности модели классификации, которая объединяет точность (precision) и полноту (recall) данных⁶²³ – 0,90; доля правильных ответов «Accuracy» – 0,965). Рассчитанные метрики подтверждают, что модель «RandomForest» хорошо справилась с поставленной задачей. Также для поиска наиболее подходящего алгоритма расследования использовалась модель «K-Nearest Neighbors», которая показала точность 93,4 %.

Таким образом, итогом проведенного исследования явилось интеллектуальное программное технико-криминалистическое средство –

⁶²¹ Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Указ. соч. С. 20.

⁶²² Carrington A. M., Manuel D. G., Fieguth P. W. Deep ROC analysis and AUC as balanced average accuracy, for improved classifier selection, audit and explanation // IEEE transactions on pattern analysis and machine intelligence. 2022. V. 45. №. 1. P. 330.

⁶²³ Leevy J., Hancock J., Zuech R. Detecting cybersecurity attacks across different network features and learners // Journal of big data. 2021. V. 8. №. 1. P. 2.

«Cybercrime DT Model (AI) [Цифровой двойник киберпреступления]», в основу работы которого заложены указанные модели машинного обучения. При осуществлении криминалистического изучения преступной деятельности часто бывает необходимо установить зависимость воздействия какого-либо признака на изменение параметров другого, что можно осуществить методом регрессионного анализа, который заключается в прогнозировании с некоторой вероятностью неизвестных значений одних переменных по известным значениям других (если переменные, характеризующие признаки, связаны между собой определенным соотношением, как правило, корреляцией с коэффициентом более 0,5⁶²⁴. По своей сути регрессионный анализ выступает инструментом моделирования и исследования свойств изучаемых данных⁶²⁵ и по этой причине является основополагающим методом построения цифровых двойников различных объектов, процессов и явлений.

Ансамблевая модель «Random Forest Regressor» является одним из наиболее обоснованных с научной точки зрения методов для задач регрессии и классификации⁶²⁶, особенно когда признаки разнородны и могут быть категориальными, бинарными и числовыми. Модель является устойчивой к явлению переобучения и хорошо работает с пропущенными значениями, позволяя объективно оценивать значимость признаков. Точность прогнозирования вероятности раскрытия преступного деяния и выдачи наиболее соответствующего сложившейся следственной ситуации алгоритма расследования оказалась выше при использовании такого рода ансамбля обученных моделей. Построенная модель позволяет с высокой степенью точности (более 96 %), используя формализованные и структурированные сведения, выдавать прогноз вероятности раскрытия преступления по введенным пользователем данным.

Способность понять, почему модель приняла то или иное решение, называется интерпретируемостью, которая показывает адекватность модели и обеспечивается, как правило, относительно сложными видами машинного обучения. Так, в этих целях в модели «Random Forest» предсказания могут объясняться с помощью специальных методов, таких как «SHAP»

⁶²⁴ Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Указ. соч. С. 491.

⁶²⁵ Стрижов В. В. Методы индуктивного порождения регрессионных моделей. М. : Вычислительный центр им. А. А. Дородницына Российской акад. наук, 2008. С. 3.

⁶²⁶ Nuradiah R., Sudiarjo A., Yunautama D. A Comparative analysis of logistic regression and random forest algorithm for cyberattacks classification // 2024 18th International conference on telecommunication systems, services, and applications (TSSA) materials. 2024. № 2. P. 202.

(от англ. «shapley additive explanations» – объяснение аддитивных уравнений Шепли)⁶²⁷ для интерпретации вклада каждого признака в предсказание конкретного наблюдения, а также «LIME» (от англ. «Local interpretable model-agnostic explanations» – локальные интерпретируемые объяснения, не зависящие от модели) для объяснения предсказаний для отдельных экземпляров данных. Таким образом, указанные методы позволяют проверить модель на адекватность, т. е. можно убедиться, что модель не опирается на случайные признаки и формирует прозрачные и понятные для человека выводы. Они позволяют объяснить, почему модель приняла то или иное решение, что способствует повышению доверия к анализу и обеспечению его качества.

По итогам создания модели удалось определить признаки, в наибольшей степени влияющие на возможность раскрытия преступлений. Важность признаков была выявлена и на основе категориального вклада, интерпретация которого позволяет сделать вывод, что способы сокрытия следов (переменная «Trace_hidden»), предполагающие использование различных анонимизирующих средств и технологий, например, таких как «VPN», маскирующее программное обеспечение «Tor», SIP-телефония, оказывают наибольшее влияние на вероятность раскрытия преступления (снижая ее), что в целом согласуется с данными практики расследования. Более того, именно признак способа сокрытия следов внес в процентном соотношении наибольший вклад в прогноз вероятности раскрытия (как негативный фактор), сравнительно меньший вклад – серийность (как положительный фактор), тогда как лишь наличие цифровых следов совершения преступного деяния и ряд сопутствующих признаков внесли сравнительно небольшой вклад. При этом отмечается важность типа цифровых следов в виде уникальных идентификаторов, таких как MAC-адрес, IMEI-код и пр., наличие которых повышает вероятность раскрытия.

Примечателен признак метода совершения преступления, сложность которого закономерно снижает вероятность раскрытия, например, в случаях применения ботнет сетей и сети даркнет. Значимый вклад, как и предполагалось, вносит показатель серийности преступного деяния «Seriality», особенно в связке с признаками даты совершения преступления «Date» и времени совершения преступного деяния «Time».

⁶²⁷ Wang H., Liang Q., Hancock J. Feature selection strategies: a comparative analysis of SHAP-value and importance-based methods // Journal of big data. 2024. V. 11. № 1. P. 2.

Таким образом, значимость признаков в модели вполне интерпретируема и согласуется с экспертными и научными представлениями о преступлениях в сфере компьютерной информации.

Традиционно одной из главных составляющих любой методики выступает криминалистическая характеристика вида преступления, хотя с этой дефиницией в криминалистической литературе связаны неутраченные дискуссии⁶²⁸, обусловленные необходимостью установления корреляционных или вероятностных связей между элементами. Определенную значимость в этот вопрос могут внести тепловые карты (карты корреляционных связей). Упростить восприятие больших массивов цифровых сведений со сложной структурой с отображением связей между ними позволяет визуализация данных. Так, например, графическое представление в виде тепловых (цветовых) карт (от англ. «heatmaps» – тепловая карта) отображают степень связи между двумя переменными в виде цветового кода⁶²⁹.

Для выявления корреляционных зависимостей между переменными (элементами криминалистической характеристики преступления) сформированного набора данных были построены корреляционные матрицы в виде таблицы и тепловой карты (Рисунок 6), где по строкам и столбцам расположены переменные, а на их пересечении – коэффициенты корреляции Пирсона⁶³⁰, принимающие значения от «-1» до «1» и определяющие силу и направление связи между переменными. Значения близкие к «1» (насыщенность синего цвета) определяют положительную связь (прямая зависимость одной переменной от значимости другой). Значения близкие к «-1» (насыщенность красного цвета) – силу отрицательной связи (чем больше одна переменная, тем меньше другая).

Отсутствие связи между переменными выражалось значением близким к 0 (ячейки белого или невыраженного цвета).

⁶²⁸ Россинская Е. Р., Семикаленова А. И. Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа»). Указ. соч. С. 69.

⁶²⁹ Sadegh-Zadeh S., Tajdini M. An unsupervised machine learning approach for cyber threat detection using geographic profiling and domain name system data // Decision analytics journal. 2025. P. 100581.

⁶³⁰ Modi P. Using a structured composition of correlation coefficient functions to optimize machine learning-driven cyberattack detection models // 2025 IEEE conference on artificial intelligence (CAI) materials. 2025. № 2. P. 1004.

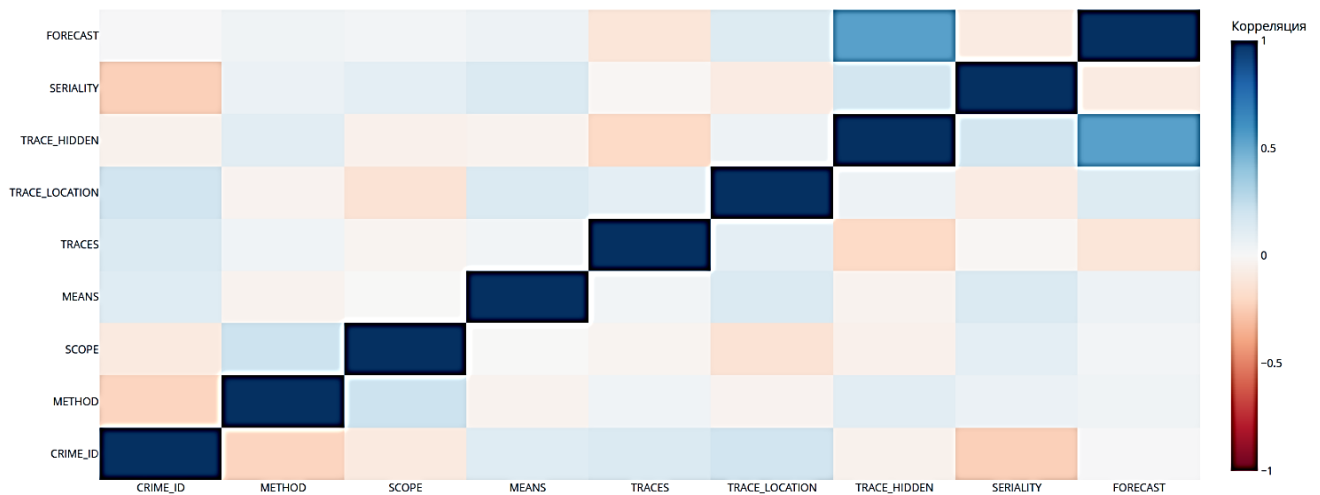


Рисунок 6 – Карта корреляционных связей значимых признаков элементов криминалистической характеристики преступлений в сфере компьютерной информации (встроенный метод отбора «Random Forest Feature Importance»)

Так, например, сильные и умеренные корреляции были обнаружены между переменными:

- вид преступления «Crime_ID» и средство совершения преступного деяния «Means» (в интерпретации показывает, что конкретные типы преступлений чаще совершаются определенными техническими средствами);
- дата совершения преступления «Date» и серийность «Seriality» (подтверждается тем, что серийные преступления происходят в определенные периоды);
- вид преступления «Crime_ID» и следы преступного деяния «Traces» (определенные типы преступлений связаны с рядом типичных цифровых следов);
- метод сокрытия цифровых следов «Trace_hidden» и цифровые следы преступления «Traces» (метод сокрытия цифровых следов находится в прямой зависимости от типа цифровых следов);
- вид преступления «Crime_ID» и место расположения цифровых следов «Trace_location» (определенные типы преступлений связаны с типичными местами обнаружения цифровых следов);
- способ совершения преступления «Method» и метод сокрытия цифровых следов «Trace_hidden» (определенные методы совершения преступлений чаще связаны с применением определенных методов сокрытия следов);
- вид преступления «Crime_ID» и способ совершения преступления «Method» (показана сильная отрицательная связь, что объясняется использованием

разных методов для совершения различных типов преступлений);

- способ совершения преступления «Method» и средство совершения преступного деяния «Means» (связь между методом совершения преступления и используемыми средствами);

- способ совершения преступления «Method» и место расположения цифровых следов «Trace_location» (способ совершения преступления влияет на место обнаружения цифровых следов);

- способ совершения преступления «Method» и серийность преступного деяния «Seriality» (связь между методом совершения преступления и его серийностью);

- серийность преступного деяния «Seriality» и место расположения цифровых следов «Trace_location» (серийность преступного деяния определяется определенными серийно повторяющимися цифровыми следами и их расположением).

Стоит также отметить, что такие признаки как серийность преступного деяния «Seriality», цифровые следы преступления «Traces» и способы их сокрытия «Trace_hidden» в большей мере влияют на вероятность раскрытия преступлений в сфере компьютерной информации. Таким образом, корреляционная матрица может использоваться для отбора значимых признаков и выявления скрытых закономерностей между данными.

Традиционные модели машинного обучения, как правило, анализируют каждое наблюдение изолированно. Однако, можно учесть связи между схожими преступлениями и выявить группы похожих случаев, выдавая графическое представление связей между преступными деяниями, анализ центральности и значимости наблюдений (узлов) использованием графовых GNN-сетей⁶³¹ (от англ. «graph neural network» – графовые нейронные сети).

На графе отдельные наблюдения отображаются в виде вершин (узлов), в рассматриваемом случае преступления из выборки данных (Рисунок 7). Каждый узел подписывается идентификатором (Crime_ID). Наблюдения с отметками «раскрыто» отмечены красным цветом, нераскрытые случаи – синим.

⁶³¹ Liu G., Lu K., Pi S. Graph neural networks embedded with domain knowledge for cyber threat intelligence entity and relationship mining // PeerJ computer science. 2025. V. 11. P. 23; Gao C., Zheng Y., Li N., A survey of graph neural networks for recommender systems: challenges, methods, and directions // ACM transactions on recommender systems. 2023. V. 1. №. 1. P. 2.

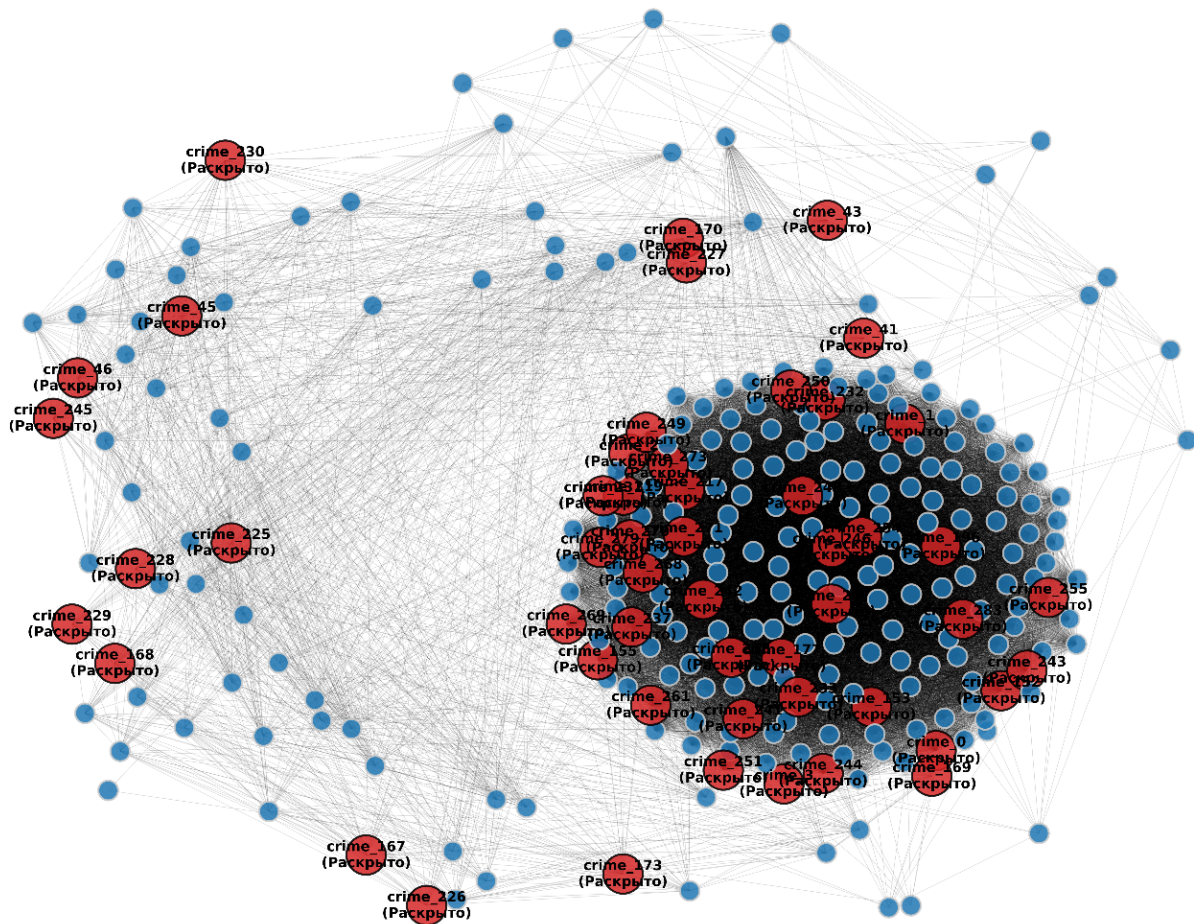


Рисунок 7 – Форма представления графа на случайной выборке, показывающая сходство в совершении преступных деяний, связанных с неправомерным доступом к компьютерной информации (ст. 272 УК РФ)

Ребра графа (связи) показывают схожесть между преступными деяниями и проведены между теми преступлениями, которые похожи по ряду признаков (вид преступления, метод и способ совершения, серийность и др.). Близко расположенные узлы определяют преступления, которые имеют много общих признаков (например, совершены с использованием одних и тех же технических средств или имеются данные о схожих техниках их совершения). Удаленно расположенные узлы – преступления, которые мало похожи на остальные и являются уникальными по своим характеристикам в наборе данных, или не имеют общих признаков с другими (например, способ совершения преступления был редким, необычным и идентифицировался уникальными следами).

Группы узлов, которые тесно связаны между собой, могут указывать на серию похожих преступлений или типовые сценарии и объединены в кластеры.

С учетом построенного графа можно выявить какие признаки объединяют раскрытые преступления в том или ином отдельном кластере, показать, что

изолированные (периферийные) преступления труднее раскрывать или необходимо их расследовать с задействованием уникальной методики.

Таким образом, периферийное расположение – результат алгоритма визуализации, который «раздвигает» непохожие узлы на периферию, а похожие «стягивает» к центру или в кластеры.

Так, в левой части графа на Рисунке 12 отчетливо видны кластеры, в которых сосредоточено сразу несколько раскрытых преступлений (например, в случае с переменной «Crime_ID» под номерами 225, 228, 229, 168). Это свидетельствует о наличии устойчивых паттернов, при которых раскрытие одного эпизода способствует раскрытию других, либо о том, что определенные типы преступлений легче поддаются расследованию благодаря общим признакам.

Аналитическая интерпретация графа раскрываемости преступлений позволяет также интерпретировать подходы к расследованию преступлений. Причины формирования кластеров раскрытых преступлений могут определяться: наличием общих или похожих цифровых доказательств, которые способствовали успешному расследованию сразу нескольких преступных деяний; использованием схожих методик расследования; серийным характером преступлений, когда раскрытие одного эпизода приводит к раскрытию связанных с ним дел. Таким образом, графовая модель позволяет не только визуализировать структуру преступлений, но и выявлять закономерности, связанные с их расследованием. Выявление подобных кластеров может быть использовано для разработки рекомендаций по оптимизации расследования аналогичных преступлений в будущем.

Таким образом, графовая визуализация преступлений это не только способ увидеть кластеры и связи между отдельными криминальными актами, но и инструмент для:

- выявления групп серийных преступлений или схожих уязвимостей;
- узлов с высокой центральностью (с наличием связей), которые могут быть индикаторами типовых сценариев, чаще всего приводящих к раскрытию или, наоборот, к нераскрытию преступления;
- используя графовые признаки (центральность, принадлежность к кластерам), можно строить модели, которые будут предсказывать вероятность раскрытия новых аналогичных преступлений;
- граф помогает понять, какие группы преступлений требуют особого внимания, где можно применить типовые методики расследования, а где нужны уникальные подходы;

– визуализация графа может использоваться для обучения следователей, чтобы они видели, какие признаки и связи наиболее важны для расследования.

В заключение можно добавить, что для определения вероятности раскрытия преступлений и поиска аналогий между преступными деяниями могут использоваться различные модели машинного обучения и искусственные нейросети. Однако только сети «GNN» позволяют учитывать индивидуальные признаки каждого преступления и взаимосвязи между ними, что особенно важно для преступлений, где серийность (повторяемость) или шаблонность играют ключевую роль, а также обеспечивать интерпретируемый анализ, позволяя выявлять скрытые закономерности и оптимизировать стратегию расследования.

Проведенное исследование позволило сделать вывод о возможности интеллектуализации процесса расследования преступлений, использования рекомендательных систем в виде системы поддержки принятия решений в условиях информационной неопределенности и применения методов науки о данных в криминалистике. Установлено, что такие признаки как метод, среда и средство совершения преступления, цифровые следы преступления, их расположение, способ их сокрытия и серийность преступления являются наиболее значимыми для выдачи вероятности раскрытия.

Цифровая криминалистическая модель преступления в сфере компьютерной информации позволяет на основании формализованных исходных данных (нейросетевого кластера данных) выдавать вероятность раскрытия преступного деяния, основанную на выявлении закономерностей в массиве сведений, выявлять признаки, в наибольшей степени влияющие на возможность расследования преступлений, выявлять оптимальный и максимально соответствующий введенным данным алгоритм расследования. Все полученные с помощью алгоритмов искусственного интеллекта результаты при их тщательном исследовании вполне интерпретируемы и подтверждаются практикой расследования. Планируется продолжить совершенствование модели путем увеличения нейросетевого кластера данных, а равно и точности прогнозирования и выдачи результатов по вводимым данным, а также повышения качества признаков, которые могут повлиять на точность прогноза модели.

Полученные данные подтверждают применимость методов науки о данных в расследовании преступных деяний и обеспечивают право на интеграцию учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности в практику расследования, при этом имеющийся на сегодняшний день арсенал алгоритмов

искусственного интеллекта может обеспечить объяснимость и прозрачность выдаваемых моделью результатов.

Таким образом, методологическую основу использования алгоритмов искусственного интеллекта в расследовании рассматриваемых преступлений составляют частная теория криминалистической характеристики преступлений, а также теория информационно-компьютерного обеспечения криминалистической деятельности в совокупности с учением об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности.

Технологии искусственного интеллекта являются наиболее перспективным вектором развития прикладных исследований в сфере расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий в целом, несмотря на сложность разработки и апробации такого рода решений.

Применение методов математической статистики и искусственного интеллекта в исследовании позволило построить цифровую криминалистическую модель преступления в сфере компьютерной информации на основе 30 признаков, определяющих содержательный состав элементов криминалистической характеристики преступлений в сфере компьютерной информации, выявить закономерные связи между ними и сформировать программное технико-криминалистическое средство с возможностью выдачи вероятности раскрытия преступного деяния по введенным пользователем данным, а также наиболее подходящего сложившейся ситуации алгоритма расследования.

Закономерности изученных преступлений на основе фильтрационных и встроенных в модели методов отбора «Random Forest Feature Importance» позволили выявить набор значимых для расследования преступного деяния признаков, которые были преобразованы в доказательственные переменные.

Сформированная модель была протестирована на точность выдачи соответствующего алгоритма расследования исходя из введенных пользователем данных. Стоит также отметить, что в целях исключения методологических ошибок, связанных с вынесением судебных решений или приговоров, основанных на неполных либо некачественных результатах расследования⁶³², целесообразно использование подобных моделей лишь на уровне вспомогательного средства, которое не должно полностью заменять ход рассуждений следователя, но может в

⁶³² Колдин В. Я., Ищенко Е. П., Крестовников О. А. Типовая информационная модель или криминалистическая характеристика преступления. Указ. соч. С. 6.

какой-то степени помочь с принятием того или иного решения, выступая интеллектуальным агентом⁶³³ в качестве программного обеспечения, аккумулирующего данные и выполняющего задачи с их использованием.

Несмотря на распространенное мнение о проблемах достижения точности, выдаваемой системами на основе искусственного интеллекта для описания социальных явлений⁶³⁴, можно отметить, что развитие науки о данных и внедрение новых интеллектуальных алгоритмов, в том числе объяснимого искусственного интеллекта, обеспечивающего прозрачность предсказаний, объяснимость принимаемых решений, а также выявление взаимосвязей в больших объемах цифровых данных, дает основание полагать о целесообразности дальнейшего развития учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности, исследования возможностей моделирования с помощью технологий искусственного интеллекта преступных деяний иных видов, что, безусловно, определяет большие перспективы получения новых и необходимых знаний в области их расследования.

Стоит также отметить, что отличительной особенностью цифрового двойника преступлений в сфере компьютерной информации, исходя из его определения, является то, что эксплуатация его сопряжена с использованием знаний в режиме реального времени для отражения состояния и динамики конкретного преступного деяния. Соответственно, при возникновении нового способа совершения преступления, в значительной степени отличающегося от способов, имеющих в наборе данных и служащих кластером обучающих данных для модели машинного обучения, вероятность выдачи корректного решения поставленной задачи снижается. В этих целях необходимо применение подхода, который будет учитывать трансформацию способов и средств совершения преступлений и оперативно вносить новые сведения в новые кластеры данных для обучения программных технико-криминалистических средств.

Для всех интеллектуальных технико-криминалистических средств, цифровых двойников преступных деяний (подразумевающих динамичность системы и изменчивость состояний), в основу которых закладывается некий статичный набор данных, будет необходима периодическая актуализация их баз

⁶³³ Lanhamai M. AI-Agents in action. Shelter island : Manning publications, 2025. P. 2.

⁶³⁴ Конькова Т. А. Агентное моделирование процесса голосования // Искусственные общества. 2018. Т. 13, № 4. С. 1; Гуров О. Н. Искусственные интеллектуальные системы и решение социальных задач: проблема доверия // Искусственные общества. 2021. № 1. С. 2.

данных, обеспечивающая соответствие текущему уровню развития преступности. Обеспечить функционал своевременной актуализации данных призвана система кодирования преступных деяний, основанная на ведении реестров техник и подтехник, используемых киберпреступниками, например, в соответствии с постоянно пополняемым банком данных угроз безопасности информации «Mitre Att&ck». Увеличение объема данных, их грамотная предобработка, а также подбор оптимальной модели машинного обучения позволит формировать максимально точные прогнозы и выдавать наиболее точные рекомендации по расследованию преступлений.

Таким образом выдвинутая гипотеза о возможности формирования цифрового двойника преступления в сфере компьютерной информации в виде его цифровой копии, позволяющей оптимизировать эффективность расследования, подтвердилась и позволила обозначить значимость криминалистической характеристики как основы формирования кластера данных для моделирования цифровых криминалистических моделей и установления корреляционных и иных связей между элементами (признаками) преступного деяния, что в перспективе может использоваться сотрудниками правоохранительных органов по конкретным следственным ситуациям при минимальных затратах труда, времени и средств.

ЗАКЛЮЧЕНИЕ

Рассмотрение теоретических основ и прикладных аспектов расследования преступлений в сфере компьютерной информации позволило сформулировать следующие выводы:

1. Сложившаяся ситуация, связанная со сложностью раскрытия указанных преступлений, опосредованных с цифровой формой информации, выступает катализатором внедрения ряда современных информационных технологий в практику расследования. Для создания эффективного механизма противодействия рассматриваемым преступным деяниям в основу формируемых технологических решений можно заложить систему характерных криминалистических признаков указанных криминальных актов, в совокупности представляющих собой их криминалистическую характеристику.

Преступления в сфере компьютерной информации как объект криминалистического исследования во многом характеризуются средой совершения преступного деяния (киберпространством, метaprостранством, распределенным реестром или квантовой вычислительной средой), которая выступает носителем криминалистически значимой информации. Соответственно, метaprеступления, а также иные вариации преступных деяний, определяемые средой их совершения, являются эволюционным видом преступлений в сфере компьютерной информации, требующими адаптации существующих методик расследования и разработки принципиально новых подходов с учетом специфики новой среды. В свою очередь, возможности, порождаемые новыми информационными технологиями и технологическими средами, могут использоваться правоохранительными органами в целях повышения эффективности процесса расследования, формирования виртуальных копий преступных деяний и пр., так, например, возможно создание цифровых криминалистических моделей (информационных моделей, информационно-компьютерных моделей), содержащих сведения о взаимосвязанных криминалистически значимых признаках преступлений, построенных на основе анализа и обобщения практики их раскрытия и предназначенных для формирования частных методик расследования. При этом, например, метавселенную можно использовать в качестве платформы для моделирования преступлений и мест их совершения, технологию распределенных реестров – для хранения больших массивов криминалистически значимой компьютерной информации, квантовые компьютеры – в качестве высокотехнологичных средств

криминалистического обеспечения.

2. Текущее состояние преступности в сфере компьютерной информации несмотря на постоянную трансформацию ее структуры отличается рядом специфичных признаков (элементов), определяющих их криминалистическую характеристику. Подробный анализ уголовных дел рассматриваемой категории обеспечил выявление соответствующего нынешнему уровню набора характерных признаков преступлений, благодаря чему их криминалистическую характеристику предложено изложить в следующем виде: способ совершения преступления с описанием типичных следов преступления, способов их сокрытия, вероятных мест их нахождения и распространенности (серийности) преступного деяния; обстановка (место (среда), время совершения) преступления; личность преступника; личность потерпевшего и предмет посягательства.

3. Использование системно-исторического подхода при исследовании генезиса преступлений, совершаемых в сфере компьютерной информации, позволило рассмотреть не только этапы его развития, но и современное состояние, а также возможные направления его трансформации с целью выявления наиболее перспективных прогностических методов предотвращения противоправных деяний, принятия предупреждающих мер, направленных на сокращение как существующих, так и потенциально возможных преступлений.

Дуализм интеграции информационных технологий подразумевает и цифровизацию применяемых в криминалистике технико-криминалистических средств в целях расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и технических средств в цифровой среде, определяя так называемый четвертый этап развития криминалистики («Криминалистика 4.0»). При этом формирующееся в наши дни направление развития Индустрии 5.0 в свете формирования цифровых двойников объектов, явлений или процессов, прогнозирования и принятия решений на основе искусственного интеллекта, технологий компьютерного зрения, машинного обучения и интеграции больших языковых моделей вполне позволяет определить принципиально новый подход направления расследования «высокотехнологичных» преступлений и именовать его подходом «Криминалистика 5.0».

Перспективным направлением в системе юридических технологий является разработка и совершенствование криминалистического обеспечения расследования преступлений, в частности, технико-криминалистических средств и информационных систем, которые могли бы учитывать не только текущие угрозы,

но и новые, перспективные в плане появления, формы. Одной из основных задач, решаемых подобными инструментами, является обнаружение, фиксация, изъятие и исследование цифровых доказательств, а также автоматизация процесса расследования и обеспечение целостности собранной информации, что позволяет определить ключевым для ее реализации стек индустрий Web 4.0 и Web 5.0, представленными технологиями искусственного интеллекта, распределенного реестра, сверхвысокой передачи данных 5G, Интернета вещей, а также виртуальной и дополненной реальности.

4. Разрыв между возможностями преступников и инструментами, доступными правоохранительным органам, подчеркивал необходимость адаптации правовых механизмов к динамической природе преступлений в сфере компьютерной информации, а сложность идентификации цифровых следов и собирания доказательственной базы требовал совершенствования ряда криминалистических методов и средств расследования. В этих целях была сформирована упрощенная модель, отражающая последовательность этапов расследования преступных деяний рассматриваемого вида, в которой способ совершения преступления, как исходный вектор, влияет на тип оставляемых цифровых следов, цифровые следы, в свою очередь, обнаруживаются использованием технико-криминалистических средств, которые определяют методику расследования преступлений в сфере компьютерной информации, алгоритм действий для поиска и собирания доказательств и их дальнейшей юридической интерпретации.

В работе приведена классификация технико-криминалистических средств, включающих в себя широкий круг аппаратных, программно-аппаратных и программных средств. Общая классификация технико-криминалистических средств проведена по криминалистическим и правовым основаниям, по сфере применения, доказательственному значению, правовой регламентации и функциональной направленности. Систематизация применимости различных технико-криминалистических средств на основе имеющихся представлений о свойствах цифровых доказательств позволила сделать вывод, что имеющиеся на сегодняшний день средства можно классифицировать по характеру воздействия на информацию, уровню автоматизации расследования, источнику получаемой информации, цели применения и функциональному назначению.

Практическая значимость приведенной классификации определяется возможностью систематизации знаний об имеющихся на сегодняшний день технико-криминалистических средствах, применяемых при расследовании

преступлений в сфере компьютерной информации, что облегчает их поиск и выбор для решения конкретных задач, формулирования принципов применения, определения критериев их подбора под конкретный вид преступного деяния, стимулирования разработки инструментов, направленных на расследование вновь возникающих преступлений, а также стандартизации использования указанных средств в процессе сбора цифровых доказательств и обеспечения их допустимости в суде.

5. В работе показано, что в качестве орудий и средств совершения преступлений в сфере компьютерной информации выступают различные технические средства и специализированное программное обеспечение, использование которых может быть обнаружено по специфическим для каждого применяемого «инструмента» цифровым следам. Индивидуальность и электронная форма указанных следов определяют возможность их исследования исключительно с применением цифровых инструментов, что обусловлено неприменимостью традиционных методов собирания доказательств к среде цифровых данных. Криминалистическое обеспечение расследования преступлений рассматриваемого вида стратегически целесообразно планировать с возможностью автоматизации рутинных задач, что возможно с задействованием технологий искусственного интеллекта, анализа больших данных, хранения доказательств в распределенных системах, моделирования преступных деяний и пр. т. е. на базе индустрий Web 4.0 и Web 5.0.

Поскольку предполагаемым вектором развития киберпреступности является использование различных генеративных алгоритмов машинного обучения, соответственно, было показано, что для расследования рассматриваемых в работе преступлений необходимы программные средства, способные самостоятельно, на основе гибких алгоритмов искусственного интеллекта, без участия человека, например, идентифицировать аномалии в сетевом трафике, анализировать вредоносный код и, соответственно, адаптироваться к новым видам атак. Таким образом, выявлено, что только программные технико-криминалистические средства смогут эффективно бороться с атаками, управляемыми искусственным интеллектом, в будущем, что подчеркивает насущность их рассмотрения в настоящее время.

6. В работе показано, что эффективность расследования преступлений в сфере компьютерной информации в большинстве случаев зависит от качества обнаружения, фиксации, изъятия и исследования цифровых доказательств путем использования технико-криминалистических средств, при этом, к основным

проблемам относятся фрагментарность и изменчивость цифровой информации, возможность шифрования и анонимизации данных, разнообразие среды исследования и невозможность стандартизации процесса выявления доказательств. Показано решение выявленных проблем, которое заключается в автоматизации указанных процессов путем использования программных технико-криминалистических средств, поскольку автоматическую классификацию и детектирование киберугроз, в том числе среди больших массивов сведений, в совокупности с геометрически растущим объемом цифровых данных, возможно охватить исключительно используя программное обеспечение, в частности, построенного на базе технологий искусственного интеллекта и машинного обучения.

В рамках исследования сформирована совокупность принципов, позволяющих повысить эффективность расследования рассматриваемых преступлений, обеспечить юридическую и техническую состоятельность цифровых доказательств (принцип хронологической документации (обеспечивающий фиксацию всех этапов работы с цифровыми доказательствами, предотвращение утраты сведений путем организации центров обработки данных на основе распределенных баз и облачных массивов), принцип независимых дисковых данных (с возможностью расчета контрольных сумм и контроля версий хранилищ) и принцип реализации защиты цифровых данных от посягательств (на основе использования алгоритмов шифрования и внедрения блокчейн-технологий с временными метками)). Показана возможность автоматизированного процесса собирания и исследования цифровых доказательств задействованием специализированного программного обеспечения, разработанного на базе искусственного интеллекта и машинного обучения и самоинтерпретируемых моделей (ХАИ-систем), способных объяснять принимаемые решения адаптированным для человека языком, что особенно важно для исключения проблем предвзятости алгоритмов.

Предложено закрепление за следователем права, но не обязанности привлечения специалиста при изъятии электронных носителей информации, исходя из собственных компетенций. Если в ходе следственных действий не проводится исследование информации, содержащейся на носителе информации, как, например, в случае его осмотра или копирования информации, то решение вопроса об участии специалиста вполне может осуществляться следователем (дознавателем) самостоятельно в порядке ст. 168 УПК РФ. Обращение с простыми электронными носителями информации, например, USB-накопителями, является

на сегодняшний день бытовым навыком, по этой причине представляется целесообразным дополнение ч. 2 ст. 164.1 УПК РФ – «Энергозависимые электронные носители информации подлежат изъятию с участием специалиста. В иных случаях специалист привлекается по усмотрению следователя при отсутствии у последнего компетенций, исключающих риск повреждения, модификации или уничтожения данных. Изъятие или копирование информации сопровождается видеозаписью, за исключением ситуаций изъятия энергонезависимых носителей без исследования их содержимого».

В работе представлены основные направления совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации, которые заключаются в: подробной регламентации и алгоритмизации процесса собирания, хранения и использования цифровых доказательств, введении национальных стандартов по фиксации и анализу цифровых доказательств, а также развитию систем сертификации специалистов, задействованных в расследовании преступлений в сфере компьютерной информации; расширении перечня программных технико-криминалистических средств для автоматизированного поиска, фиксации и исследования цифровых доказательств на базе технологий искусственного интеллекта и анализа больших данных; развитии облачных платформ для безопасного и неизменного хранения цифровых доказательств с применением блокчейн-технологий и распределенных реестров; создании единого кластера данных с возможностью оперативного доступа к цифровым доказательствам, поиска и обработки криминалистически значимой информации с использованием ключевых слов и фильтров в едином сегменте сети.

7. Анализ материалов судебно-следственной практики при изучении особенностей возбуждения уголовных дел о преступлениях в сфере компьютерной информации показал, что процедура получения объяснений на стадии проверки сообщения о преступлении имеет особую важность. Допустимо при этом применять положения, регламентирующие порядок проведения следственных действий, в том числе допросов граждан. Систематичность при планировании следственных действий может быть достигнута использованием заранее сформированного исходя из сложившейся практики расследования алгоритма действий. Именно получение объяснений может выступить отправной точкой алгоритмизации процесса расследования преступлений в сфере компьютерной информации и процесса поддержки принятия решений по уголовному делу должностным лицом. В связи с этим в ходе исследования была рассмотрена

последовательность шагов в виде алгоритма и их типичных вариаций, складывающихся на этапе возбуждения уголовного дела, отмечена сложность расследования преступлений, которая зачастую объясняется бесперспективной практикой стохастического принятия решений на основе лишь личного опыта, либо интуиции следователя, без задействования современных научных методов познания.

8. Обнаружение, изъятие, копирование и исследование цифровой информации, имеющей значение для уголовного дела, требует интеграции юридических и технических знаний, при этом, информация, содержащаяся на электронном носителе, может иметь различную форму и вид, включая ориентирующие сведения, способствующие планированию и проведению следственных действий. Анализ уголовных дел и материалов следственной практики позволил выявить организационно-тактические особенности производства отдельных следственных действий по преступлениям в сфере компьютерной информации, а также наиболее часто встречающиеся при этом ошибочные действия. На основе анализа взаимосвязей между алгоритмами расследования и следственными ситуациями сделано предположение, что типовая следственная ситуация обуславливает соответствующий ей типовой алгоритм расследования с выделением на каждом из этапов соответствующих ключевых признаков.

9. Выявленные в ходе проведенного исследования признаки, определяющие минимально необходимые элементы, входящие в материал проверки сообщения (заявления) о преступлении, а также в материалы первоначального и последующего этапов расследования могут быть заложены в основу предлагаемой информационно-компьютерной модели преступного деяния (цифрового двойника преступления), совершенного в сфере компьютерной информации. Вышеуказанные признаки выступили набором данных для определения наиболее подходящего и эффективного алгоритма его расследования, а также вероятности раскрытия смоделированного преступления.

Структуру частной криминалистической методики расследования преступлений в сфере компьютерной информации составили обстоятельства, подлежащие установлению при расследовании (установление признаков определенного состава преступления, обстоятельств, подлежащих доказыванию, и иных обстоятельств, выяснение которых требуется при расследовании преступлений данного вида), криминалистическая характеристика преступлений (как научная абстракция, содержащая в себе общие черты, свойственные

криминалистическим характеристикам рассматриваемой группы преступлений), а также криминалистическая характеристика расследования преступлений (в виде алгоритмической системы обобщенных сведений, раскрывающих основные закономерные черты механизма расследования преступлений по различным следственным ситуациям). Предлагаемый элементный состав позволил построить информационно-компьютерную модель (цифровой двойник) преступного деяния с выдачей по нему наиболее эффективного алгоритма расследования, а также вероятности раскрытия смоделированного преступления.

Криминалистические характеристики преступлений в сфере компьютерной информации могут выступить источником формирования исходной информации о событии преступления, а элементы, входящие в криминалистическую характеристику преступлений, способствовать определению связей и зависимостей хода расследования преступлений от особенностей преступных деяний. Следственная ситуация выступает в роли исходного условия для формирования алгоритма расследования, в таком случае переход от анализа ситуации к формализации алгоритма и его практической реализации является сущностью применения криминалистической методики на практике. Трансформация описательной формы изложения классических рекомендаций к нежестким алгоритмам (недетерминированным, вариативным, самообучающимся алгоритмам машинного обучения) является существенным этапом развития частных методик расследования преступлений, особенно тех, признаки которых можно отразить в цифровой форме. По этой причине, преступления в сфере компьютерной информации – это один из наиболее подходящих под критерий «оцифрованности» видов преступных деяний, позволяющих сформировать цифровой двойник преступного деяния.

Сделан вывод о том, что предложенный подход к формированию методик расследования преступлений возможно распространить и на другие родовые группы преступных деяний при условии аккумулирования сведений о типичных следственных ситуациях, совокупности элементов криминалистической характеристики преступления (типичных их признаках), а также имеющихся доказательствах, формализация сведений о которых позволит использовать их в качестве обучающих данных для реализации информационно-компьютерной модели преступного деяния и выявления наиболее эффективных алгоритмов его расследования.

10. Сформирована система унификации процесса расследования благодаря присвоению криминальным актам уникальных кодов, однозначно идентифицирующих как распространенные в настоящее время, так и вновь появляющиеся средства и способы совершения преступных деяний во всем их многообразии.

С целью преодоления фрагментарности учета многообразия способов и средств совершения преступлений в сфере компьютерной информации, а также сложности обработки больших объемов цифровых данных, выдвижения адаптивной и унифицированной методики их расследования рассматриваемые преступления были структурированы и классифицированы (для присвоения уникальных кодов), что нашло свое отражение в программном технико-криминалистическом средстве «КиберКодекс [CyberCodex] с кодификатором преступлений в сфере компьютерной информации»⁶³⁵. Предложена система кодирования преступных деяний, позволяющая заложить основу стандартизированного учета преступлений в сфере компьютерной информации, упрощающая процесс идентификации их составов. Теоретико-правовыми основами классификации и последующего кодирования преступлений в сфере компьютерной информации выступили три уровня: уровень норм, представленных статьями главы 28 УК РФ «Преступления в сфере компьютерной информации»; уровень, представленный способами совершения противоправного деяния, в виде квалифицирующего признака, определяемого в соответствии с перечнем преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации (перечень 25), утвержденным указанием Генеральной прокуратуры Российской Федерации №503/11 и МВД России № 1 от 28 июля 2025 г.; уровень, отражающий тактику, приемы и методы (способы), используемые преступниками, а также возможности противодействия им, сформированный на базе матрицы «Mitre Att&ck».

Результаты проведенного сопоставления категорий преступлений в сфере компьютерной информации техникам матрицы «Mitre Att&ck» позволили сформировать новую систему криминалистического кодирования преступлений, использование которой может выступить основой формирования методик их расследования в условиях эволюции способов совершения преступных деяний.

⁶³⁵ CyberCodex [КиберКодекс] – Программное технико-криминалистическое средство «Киберпреступность» с кодификатором преступлений в сфере компьютерной информации : № 2025680136 : заявл. 31.07.2025 : опубл. 22.08.2025.

Обеспечивая предсказуемость правоприменения, она создает основу для адаптации уголовного законодательства к постоянно меняющимся технологическим реалиям. В основе кодирования лежат признанные на международном уровне принципы, заложенные в матрице «Mitre Att&ck», которая на постоянной основе обновляется путем внесения новых потенциально возможных способов и средств совершения преступлений. Таким образом, было обосновано появление механизма учета новых видов преступлений в сфере компьютерной информации.

11. В работе показано, что характерной особенностью рассматриваемого вида преступлений является то, что начальная стадия их досудебного расследования, особенно в условиях неочевидности преступного события, характеризуется выраженным дефицитом исходной информации, необходимой для выдвижения и проверки следственных версий, раскрытия содержания события и идентификации лица, причастного к его совершению. Для восполнения указанного дефицита данных могут использоваться массивы сведений, содержащиеся в информационной модели (криминалистической характеристике) преступления, аналогичного расследуемому.

Корректное установление исходной следственной ситуации дает возможность при использовании типовой криминалистической характеристики преступлений устранить неопределенность в информационной базе расследования. В соответствии с типичными следственными ситуациями для разрешения проблемных ситуаций выдвигаются типовые версии, в соответствии с которыми планируется дальнейшее расследование. С точки зрения материального выражения информационно-компьютерной модели преступления план расследования может воплощаться в виде алгоритма действий в графическом виде, представляющего собой логическую модель предпринимаемых действий. Планирование расследования ориентировано на построение логической схемы расследования, при этом реализацией этого плана с учетом сложившихся условий является организация расследования.

В свете построения информационной модели преступления с позиции криминалистической ситуалогии и теории принятия решений алгоритм построения плана расследования сводится к рассмотрению конкретной сложившейся ситуации, подбору типовой информационной модели преступления, максимально схожей с условиями сложившейся ситуации, выбору в наибольшей степени соответствующей обстоятельствам конкретного дела типовой методики его расследования, а также типовой следственной ситуации и версий, на базе которых выдвигается рабочая версия и составляется план расследования. По аналогии,

планирование расследования в машиночитаемой форме представляет собой планирование алгоритма работы программы, для отображения которого используются средства, определяемые типом исполняемого алгоритма.

Из всей совокупности элементов криминалистической характеристики преступного деяния основной упор при алгоритмизации необходимо делать на способ совершения преступления в соответствии с матрицей угроз безопасности информации, например, «Mitre Att&ck», которая на постоянной основе обновляется путем внесения новых потенциально возможных уязвимостей, т. е. благодаря постоянной актуализации указанной базы данных появляется механизм учета вновь появляющихся видов преступлений.

Общим для всех преступлений определенной группы может выступить алгоритм расследования в соответствии с делением на категории преступлений в родовой группе, способы совершения этих преступлений (техники и подтехники), способы обнаружения следов преступления и меры противодействия расследованию. При этом целесообразно также учесть, что способы совершения преступления в сфере компьютерной информации, условно можно классифицировать по объекту воздействия, по доступу к объекту воздействия, уровню автоматизации и мотиву воздействия и т. д., что в совокупности определит четыре отдельных направления ветвления алгоритма расследования преступления с соответствующими им способами (техниками и подтехниками) совершения преступлений или их совокупности. Процесс алгоритмизации необходимо выстраивать с учетом вида и особенностей конкретного преступления, классификации способов совершения рассматриваемого преступления (по объекту воздействия, по доступу к объекту воздействия, уровню автоматизации и мотиву действий) и соответствующих методик его расследования.

Отправной точкой алгоритмизации процесса расследования преступлений в сфере компьютерной информации и процесса поддержки принятия решений по уголовному делу должностным лицом может стать процесс получения объяснений. Предполагается допустимым получение объяснений по факту совершения преступления и возможности их представления удаленно (в альтернативной форме) посредством сети «Интернет» по специально разработанной форме, отражающей типичные следственные ситуации, и реализованной на основе искусственного интеллекта. Такой подход позволит не только снизить временные затраты на процесс подачи заявления о преступном деянии, но и автоматизировать процесс обработки криминалистически значимой информации. Однако для снятия противоречий и разрешения дискуссионных вопросов, связанных с получением

объяснений, необходимо четко определить порядок получения объяснений. Указанным устанавливается цель перевода хотя бы части вербальных действий в невербальные, а именно в невербально-цифровые с возможностью их дальнейшей обработки в цифровом виде. Таким образом, характер инженерной разработки, направленной на создание программного обеспечения или интеллектуальной информационной системы в рамках ситуационного моделирования, может определить возможность формирования алгоритмов, позволяющих на основе введенных в систему исходных данных выдвигать ограниченное число потенциально возможных принимаемых решений для следователя, что при соблюдении ряда условий (систематического накопления информации о ситуации, знания типовой ситуационной структуры, учета субъективных и объективных факторов, способных изменить ситуацию и т. п.) может быть важно, особенно для молодых специалистов, задействованных в расследовании рассматриваемых преступлений, ввиду отсутствия у них профессионального опыта, а также в условиях недостатка времени, предоставленного на расследование, информации о механизме преступления, а также лицах его совершивших.

12. Степень влияния факторов, затрудняющих процесс расследования преступлений в сфере компьютерной информации, в настоящее время можно снизить интеграцией в него технологий искусственного интеллекта. По этой причине вполне обоснованно включение в специальные методы криминалистики методов науки о данных, как наиболее близких к сфере компьютерной информации.

Выявленные теоретические основы и практические аспекты расследования указанных преступных деяний в рамках проведенного исследования позволили констатировать о возможности развития и расширения содержания теории информационно-компьютерного обеспечения криминалистической деятельности путем интеграции современных аналитических и прогностических возможностей на основе технологии искусственного интеллекта, направленных на интеллектуализацию процесса расследования, анализ больших объемов цифровых данных, выявление скрытых связей между событиями и пр., что позволит повысить эффективность расследования рассматриваемых преступлений.

Предмет теории информационно-компьютерного обеспечения криминалистической деятельности предлагается расширить с учетом современных вызовов и технологических реалий внесением ряда закономерностей (дополнений), обусловленных внедрением в практику расследования технологий искусственного интеллекта. Описанные закономерности затрагивают все имеющиеся в указанной

теории учения, по этой причине сделан вывод, что современный этап развития криминалистики требует дополнения вышеуказанной теории и интеграции в нее указанных закономерностей, объединив их в отдельное учение об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности.

Концептуальная основа предлагаемого учения развивает положения общей теории криминалистики в части применения интеллектуальных систем для выявления, моделирования, интерпретации и верификации цифровых следов преступной деятельности в современных условиях, а также прогнозирования возможности расследования преступного деяния, формирования рекомендаций по выбору наиболее эффективной методики расследования.

Предметом учения является система закономерностей обнаружения, фиксации, изъятия и исследования криминалистически значимой компьютерной информации (в том числе выявления генерации, модификации или уничтожения цифровых следов) с использованием технологий искусственного интеллекта при раскрытии и расследовании преступлений, а также совокупность особенностей разработки, функционирования и использования интеллектуальных систем в виде программных технико-криминалистических средств в качестве инструмента поддержки принятия решений в условиях информационной неопределенности или фрагментарности данных, формирования цифровых двойников и реконструкции событий преступного деяния, а также выдачи оптимальных методик расследования преступлений.

Объект учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности составляют непосредственно сами интеллектуальные технические средства и системы и содержащаяся в них криминалистически значимая компьютерная информация, интеллектуальные программные технико-криминалистические средства, обеспечивающие обнаружение, фиксацию, изъятие и исследование криминалистически значимой компьютерной информации с использованием алгоритмов искусственного интеллекта, а также система действий и отношений, реализованных на основе интеллектуальных систем, обеспечивающих анализ криминалистически значимой компьютерной информации, поддержку принятия решений в условиях информационной неопределенности, моделирование цифровых двойников и событий преступного деяния, а также формирование оптимальных методик расследования преступлений и выдачу вероятности их раскрытия.

Предлагаемая концепция интеллектуализации процесса расследования преступлений обеспечит научно-техническую основу для реализации практико-ориентированных решений противодействия преступным деяниям не только в сфере компьютерной информации или по преступлениям против общественной безопасности и общественного порядка (глава 28 в составе раздела IX «Преступления против общественной безопасности и общественного порядка» Уголовного кодекса Российской Федерации), но и ряда сопутствующих областей, например, по преступлениям против личности и преступлениям в сфере экономики (разделы VII и VIII Уголовного кодекса Российской Федерации соответственно) и пр.

13. Изложена концепция систематизации криминалистически значимой компьютерной информации в целях формирования кластера обучающих данных для интеллектуального программного технико-криминалистического средства, определена возможность гибкой настройки и выдачи отчетов по интересующим следствие направлениям.

Описана структура интегрированной системы учета цифровых доказательств по преступлениям в сфере компьютерной информации, элементами при реализации которой могут выступить подсистемы сбора и агрегации данных, их классификации и структурирования, анализа и оценки, хранения и обмена данными, а также генерации отчетов и визуализации. Описаны ее подсистемы и функциональное назначение каждого из структурных элементов, а также основания ведения криминалистического учета. Предложенная система учета цифровых доказательств сможет послужить в дальнейшем основой для формирования модульной и масштабируемой платформы поддержки принятия решений, позволяющей собирать, классифицировать и анализировать цифровые доказательства в режиме реального времени, использовать современные методы анализа на основе искусственного интеллекта для выявления закономерностей и оценки вероятности развития событий, обеспечить безопасное хранение и обмен данными с возможностью интеграции с существующими национальными и международными системами, а также реализовать комплексное программное технико-криминалистическое средство с возможностью формирования типовых следственных версий и планов расследования преступлений в сфере компьютерной информации.

14. Цифровой двойник преступления представляет собой виртуальную модель, отражающую состояние и динамику реального преступления в сфере компьютерной информации, позволяющую исследовать различные сценарии его

совершения, выявлять закономерности между элементами его криминалистической характеристики, формировать алгоритм расследования преступного деяния, выдавать вероятность его раскрытия.

В качестве исходных данных для построения модели использован массив сведений из материалов уголовных дел. Эмпирическую базу исследования составили сведения о 284 преступлениях в сфере компьютерной информации, совершенных за период с 2020 по 2025 г.г. При формировании модели использовано 30 переменных (признаков): вид преступления; способ совершения преступления; среда совершения преступления; средство совершения преступления; цифровые следы преступления; расположение цифровых следов преступления; способ сокрытия следов; серийность преступления; место совершения преступления; дата совершения преступления; время совершения преступления; идентификатор преступника; возраст преступника; пол преступника; образование преступника; род занятий преступника; судимость преступника; идентификатор потерпевшего; возраст потерпевшего; пол потерпевшего; образование потерпевшего; род занятий потерпевшего; предмет посягательства; ущерб потерпевшего; техника совершения преступления; подтехника совершения преступления; способы выявления; меры реагирования; раскрыто; алгоритм расследования.

На основе сформированной модели было разработано интеллектуальное программное технико-криминалистическое средство «Cybercrime DT Model (AI) – [Цифровой двойник киберпреступления]»⁶³⁶, позволяющее на основе введенных пользователем данных о совершенном преступлении формировать наиболее соответствующий ему алгоритм расследования и определять вероятность раскрытия смоделированного преступления с интерпретацией принимаемых моделью решений. По итогам создания модели удалось определить признаки, в наибольшей степени влияющие на возможность расследования преступлений, среди которых способы сокрытия следов, предполагающие использование различных анонимизирующих средств и технологий, например, таких как «VPN», маскирующее программное обеспечение, «Tor», SIP-телефония и т. п., оказывают наибольшее влияние на вероятность раскрытия (снижая ее), что в целом согласуется с данными практики расследования. Более того, именно признак

⁶³⁶ Свидетельство о государственной регистрации программы для ЭВМ № 2025680704 Российская Федерация. Cybercrime DT Model (AI) [Цифровой двойник киберпреступления] – цифровая криминалистическая модель преступления в сфере компьютерной информации : № 2025669600 : заявл. 31.07.2025 : опублик. 07.08.2025.

способа сокрытия следов внес в процентном соотношении наибольший вклад в прогноз вероятности раскрытия (как негативный фактор). Значимый вклад в прогноз вероятности раскрытия внес признак серийности (как положительный фактор), тогда как лишь наличие цифровых следов совершения преступного деяния и ряд сопутствующих признаков внесли сравнительно небольшой вклад. При этом отмечается важность типа цифровых следов в виде уникальных идентификаторов, таких как MAC-адрес, IMEI-код и пр., наличие которых повышает вероятность раскрытия.

Установлено, что значимым признаком является способ совершения преступления, сложность которого закономерно снижает вероятность раскрытия, например, в случаях применения ботнет сетей и сети даркнет. Таким образом, значимость признаков в модели вполне интерпретируема и согласуется с экспертными и научными представлениями о преступлениях в сфере компьютерной информации. При этом наиболее значимыми для расследования являются непосредственно цифровые следы и способы их сокрытия.

Были выявлены корреляционные зависимости между переменными (элементами криминалистической характеристики преступления) сформированного набора данных, путем построения корреляционных матриц, которые наглядно показали сильные и умеренные корреляции между переменными. Таким образом, было показано, что корреляционная матрица может использоваться для отбора значимых признаков и выявления скрытых закономерностей между данными.

Графическое представление связей между преступными деяниями обеспечило использование графовых сетей, так, были выявлены признаки объединяющие раскрытые преступления в том или ином отдельном кластере, показано, что определенные виды преступлений (преимущественно «высокотехнологичные») труднее раскрывать или необходимо их расследовать с задействованием уникальной методики. Аналитическая интерпретация графа позволяет также интерпретировать подходы к расследованию преступлений. Причины формирования кластеров раскрытых преступлений могут определяться наличием общих или похожих цифровых доказательств, которые способствовали успешному расследованию сразу нескольких преступных деяний, использованием схожих методик расследования, серийным характером преступлений, когда раскрытие одного эпизода приводит к раскрытию связанных с ним дел. Таким образом, графовая модель позволила не только визуализировать структуру преступлений, но и выявить закономерности, связанные с их раскрытием.

Выявление подобных кластеров может быть использовано для разработки рекомендаций по оптимизации расследования аналогичных преступлений в будущем.

Полученные данные подтверждают применимость методов науки о данных в расследовании преступных деяний и обеспечивают право на интеграцию учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности в практику расследования, при этом имеющийся на сегодняшний день арсенал алгоритмов искусственного интеллекта может обеспечить объяснимость и прозрачность выдаваемых моделью результатов.

Целесообразно дальнейшее развитие учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности, а также исследования возможностей моделирования с помощью технологий искусственного интеллекта преступных деяний иных видов, что, безусловно, определяет большие перспективы получения новых и необходимых знаний в области их расследования.

Автор выражает надежду, что предлагаемые в работе предложения и рекомендации найдут свое отражение в практике расследования преступлений в сфере компьютерной информации в обозримом будущем и позволят повысить результативность следственных действий, что в конечном итоге положительно отразится на эффективности расследования преступлений рассматриваемого вида.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) [с учетом поправок, внесенных Федеральными конституционными законами от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ, от 06.10.2022] // Собрание законодательства Российской Федерации. – 2020. – № 11. – Ст.1416.

2. Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ [в ред. от 17 ноября 2025 г.] // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law (дата обращения: 17.11.2025). – Текст : электронный.

3. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18 декабря 2001 г. № 174-ФЗ [в ред. от 27 октября 2025 г.] // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_34481 (дата обращения: 17.11.2025). – Текст : электронный.

4. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 г. № 187-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_220885 (дата обращения: 07.04.2025). – Текст : электронный.

5. О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 30 ноября 2024 г. № 421-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_491931/#dst100011 (дата обращения: 28.03.2025). – Текст : электронный.

6. О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 31 июля 2025 г. № 282-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_34481/a8ce863fe783cf2bec75f4f1de3e5ffb7b4cc043/ (дата обращения: 26.08.2025).

7. О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» : Федеральный закон от 07 апреля 2025 г. № 58-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_502581 (дата обращения: 07.04.2025). – Текст : электронный.

8. О персональных данных : Федеральный закон № 152-ФЗ от 27 июля 2006 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_61801 (дата обращения: 08.10.2025).

– Текст : электронный.

9. О полиции : Федеральный закон от 07 февраля 2011 г. № 342-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_110165 (дата обращения: 22.10.2025). – Текст : электронный.

10. О связи : Федеральный закон № 126-ФЗ от 07 июля 2003 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_43224 (дата обращения: 16.11.2025). – Текст : электронный.

11. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 01 апреля 2025 г. № 41-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_502182 (дата обращения: 01.06.2025). – Текст : электронный.

12. О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 24 июня 2025 г. № 156-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_508287 (дата обращения: 25.06.2025). – Текст : электронный.

13. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_61798 (дата обращения: 22.10.2025). – Текст : электронный.

14. Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_7519 (дата обращения: 01.04.2025). – Текст : электронный.

15. Об электронной подписи : Федеральный закон от 06 апреля 2011 г. № 63-ФЗ : в ред. от 28 декабря 2024 г. // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_112701 (дата обращения: 22.10.2025). – Текст : электронный.

16. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента Российской Федерации от 07 мая 2024 г. № 309 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_475991 (дата обращения:

22.10.2025). – Текст : электронный.

17. О развитии искусственного интеллекта в Российской Федерации : Указ Президента Российской Федерации от 10 октября 2019 г. № 490 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_335184 (дата обращения: 22.10.2025). – Текст : электронный.

18. О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02 июля 2021 г. № 400 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_389271 (дата обращения: 22.10.2025). – Текст : электронный.

19. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 09 мая 2017 г. № 203 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_216363 (дата обращения: 22.10.2025). – Текст : электронный.

20. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации : офиц. сайт. URL: <http://pravo.gov.ru> (дата обращения: 22.10.2025). – Текст : электронный.

21. О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме : постановление Правительства Российской Федерации от 22 декабря 2012 г. № 1382 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_139820/fbd07791b302296474e4be2c2ee28baf46599852 (дата обращения: 31.07.2025). – Текст : электронный.

22. О реализации пилотного проекта по оперативному взаимодействию уполномоченных государственных органов и организаций и информационному обмену между ними при противодействии правонарушениям, совершаемым с использованием информационных технологий : распоряжение Правительства РФ от 28 мая 2025 г. № 1350-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_506509 (дата обращения: 30.05.2025). – Текст : электронный.

23. Об утверждении правил установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи

общего пользования : постановление Правительства РФ от 30 августа 2025 г. № 1333 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_513489/ (дата обращения: 01.09.2025). – Текст : электронный.

24. Положение о единой системе межведомственного электронного взаимодействия : постановление Правительства Российской Федерации от 08 сентября 2010 г. № 697 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_104665/59a1ee33e6096f0bf3fd23d27e eb41a502ed129e (дата обращения: 30.10.2025). – Текст : электронный.

25. Об установлении Правил предоставления владельцем агрегатора сведений с использованием единой системы межведомственного электронного взаимодействия по запросу уполномоченного государственного органа, осуществляющего оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации : постановление Правительства Российской Федерации от 30 августа 2025 г. № 1328 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: <https://www.consultant.ru/law/hotdocs/90673.html> (дата обращения: 27.05.2025). – Текст : электронный.

26. Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_495619 (дата обращения: 11.01.2025). – Текст : электронный.

27. Об утверждении Концепции технологического развития на период до 2030 года (вместе с «Концепцией технологического развития на период до 2030 года») : распоряжение Правительства Российской Федерации от 20 мая 2023 г. № 1315-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_447895 (дата обращения: 22.10.2025). – Текст : электронный.

28. Об утверждении плана мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства Российской Федерации от 14 августа 2025 г. № 2207-р // Правительство Российской Федерации : офиц. сайт. URL: <http://government.ru/docs/55975> (дата обращения: 14.08.2025). – Текст : электронный.

29. Об утверждении плана мероприятий по реализации Стратегии развития отрасли связи Российской Федерации на период до 2035 года : распоряжение

Правительства Российской Федерации от 24 мая 2025 г. № 1312-р // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_506116/f62ee45faefd8e2a11d6d88941ac66824f848bc2 (дата обращения: 27.05.2025). – Текст : электронный.

30. О едином учете преступлений : приказ Генеральной прокуратуры Российской Федерации № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_57951/2ff7a8c72de3994f30496a0ccb1ddafdadfd518 (дата обращения: 08.02.2025). – Текст : электронный.

31. Об организации научной и научно-технической деятельности в системе МВД России : приказ МВД России от 28 апреля 2023 г. № 260 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=exp&n=824308#lw8jkuu8yvnolnffl> (дата обращения: 22.02.2025). – Текст : электронный.

32. Об утверждении концепции научного обеспечения деятельности органов внутренних дел Российской Федерации на период до 2030 года : приказ МВД России от 13 ноября 2020 г. № 767 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_7519 (дата обращения: 17.03.2025). – Текст : электронный.

33. Об утверждении профессионального стандарта «Следователь-криминалист» : приказ Министерства труда и социальной защиты Российской Федерации от 23 марта 2015 г. № 183н // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_178094 (дата обращения: 08.02.2025). – Текст : электронный.

34. Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 06 декабря 2017 г. № 227 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_290538/2ff7a8c72de3994f30496a0ccb1ddafdadfd518 (дата обращения: 22.01.2025). – Текст : электронный.

35. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 г. № 17 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_147084 (дата обращения: 08.02.2025). – Текст : электронный.

36. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание

Генеральной прокуратуры Российской Федерации от 28 июля 2025 г. № 503/11, МВД России № 1 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_517620/251f7ac207ca304c6331640eb36b162351c24684 (дата обращения: 26.08.2025). – Текст : электронный.

37. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 // КонсультантПлюс – справочно-правовая система : офиц. сайт. URL: https://www.consultant.ru/document/cons_doc_law_434573 (дата обращения: 08.02.2025). – Текст : электронный.

38. Конвенция Организации Объединенных Наций против киберпреступности: укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям от 27 ноября 2024 г. (A/79/460) // Министерство иностранных дел Российской Федерации : офиц. сайт. URL: https://www.mid.ru/foreign_policy/news/1989289 (дата обращения: 22.10.2025). – Текст : электронный.

39. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. (ETS № 185) // Совет Европы: офиц. сайт. URL: <https://www.europarl.europa.eu/meetdocs/20142019/documents/libe/dv/7convbudapest/7convbudapesten.pdf> (дата обращения: 22.10.2025). – Текст : электронный.

40. ГОСТ Р 59709–2022 Защита информации. Управление компьютерными инцидентами. Термины и определения; дата введения: 01 февраля 2023 г. – М. : Российский институт стандартизации, 2022. – 20 с.

41. ГОСТ Р 56545–2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей; дата введения: 01 апреля 2016 г. – М. : Стандартинформ, 2015. – 12 с.

42. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем; дата введения: 19 августа 2015 г. – М. : Стандартинформ, 2015. – 12 с.

43. ГОСТ Р 71223–2024. Вычислительная техника. Термины и определения; дата введения: 01 июня 2025 г. М. : Российский институт стандартизации, 2025. – 16 с.

44. ГОСТ Р 34.11–2012 Информационная технология. Криптографическая защита информации. Функция хэширования; дата введения: 01 января 2013 г. – М. : Стандартинформ, 2013. – 21 с.

45. ГОСТ Р ИСО/МЭК 27037–2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме; дата введения: 09 сентября 2014 г. – М. : Стандартинформ, 2015. – 47 с.

46. ГОСТ Р 70942–2023. Устройства цифровых вычислительных машин запоминающие. Термины и определения; дата введения: 12 октября 2023 г. – М. : Российский институт стандартизации, 2023. – 16 с.

47. ГОСТ Р 57429–2017. Национальный стандарт Российской Федерации. Судебная компьютерно-техническая экспертиза. Термины и определения; дата введения: 28 марта 2017 г. – М. : Стандартинформ, 2018. – 12 с.

48. ГОСТ Р 71201–2024. Персональные электронно-вычислительные машины. Типы, основные параметры, общие технические требования; дата введения: 01 июня 2024 г. – М. : Российский институт стандартизации, 2024. – 8 с.

49. Международный стандарт ISO / IEC TS 27110:2021 Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие указания по разработке основ кибербезопасности (Information technology, cybersecurity and privacy protection. Cybersecurity framework development guidelines); дата введения: 01 февраля 2021 г. – Switzerland : ISO/IEC, 2021. – 32 с.

50. Международный стандарт ISO / IEC 27014:2020 Информационная безопасность, кибербезопасность и защита конфиденциальности (Information security, cybersecurity and privacy protection); дата введения: 01 января 2020 г. – Switzerland : ISO/IEC, 2020. – 16 с.

51. Международный стандарт ISO / IEC 27032:2023 Кибербезопасность. Руководство по обеспечению безопасности в сети Интернет (Cybersecurity. Guidelines internet security); дата введения: 28 июня 2023 г. – Switzerland : ISO/IEC, 2023. – 36 с.

Материалы судебной и иной правоприменительной практики

52. Материалы уголовного дела № 12401250033000526, возбужденного 04 июня 2024 г. УМВД России по Иркутской области (МВД России Иркутское ОП № 5).

53. Материалы уголовного дела № 12401920053000057, возбужденного 16 января 2024 г. МВД по Республике Татарстан (УМВД России по городу Казани).

54. Материалы уголовного дела № 12301010018000015, возбужденного 09 января 2023 г. ГУ МВД России по Алтайскому краю (МО МВД России по г. Каменский).

55. Материалы уголовного дела № 12301500049001096, возбужденного 03 мая 2023 г. ГУ МВД России по Новосибирской области (УМВД России по г. Новосибирску).

56. Материалы уголовного дела № 12301800002000570, возбужденного 12 июня 2023 г. СО ОМВД России по Белорецкому району Республики Башкортостан.

57. Материалы уголовного дела № 12201010040001465, возбужденного 20 июля 2022 г. ГУ МВД России по Алтайскому краю (УМВД России по г. Барнаулу).

58. Материалы уголовного дела № 12301420029000604, возбужденного 07 сентября 2023 г. УМВД России по г. Липецку.

59. Материалы уголовного дела № 12301800002001025, возбужденного 26 октября 2023 г. СО ОМВД России по Белорецкому району Республики Башкортостан.

60. Материалы уголовного дела № 12201010041001894, возбужденного 28 сентября 2022 г. ГУ МВД России по Алтайскому краю (УМВД России по г. Барнаулу).

61. Материалы уголовного дела № 12201711493000919, возбужденного 05 октября 2022 г. УМВД России по Ямало-Ненецкому (АО ОМВД России по г. Новому Уренгою).

62. Материалы уголовного дела № 11901320001060334, возбужденного 31 июля 2019 г. ГУ МВД России по Кемеровской области (УМВД России по г. Кемерово ОП «Заводский»).

63. Материалы уголовного дела № 11701070014020098, возбужденного 10 марта 2017 г. ГУ МВД России по Ставропольскому краю (ОМВД России Благодарненский).

64. Материалы уголовного дела № 11701070014020077, возбужденного 07 марта 2017 г. ГУ МВД России по Ставропольскому краю (ОМВД России Благодарненский).

65. Приговор по уголовному делу № 1-154-0006/2025 // Артемовский районный суд Свердловской области : офиц. сайт. URL: https://artemovsky--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=r&delo_id=1540006 (дата обращения: 08.02.2025).

66. Приговор по уголовному делу № 1-239/2025 // Ленинский районный суд г. Владимира : офиц. сайт. URL: https://leninsky--wld.sudrf.ru/modules.php?name=sud_delo&name_op=r_juid&vnkod=33RS0001&srv_num=1&delo_id=1540006&case_type=0&judicial_uid=77RS0023-02-2025-010692-87 (дата обращения: 20.10.2025).

67. Приговор по уголовному делу № 1-46/2025 // Семилукский районный суд г. Воронежа : офиц. сайт. URL: https://semiluksky--vrn.sudrf.ru/modules.php?name=sud_

delo&srv_num=1&name_op=case&case_id=19061884&case_uid=be7f959c-cdc2-4dbb-9c38-b7215a05b923&delo_id=1540006 (дата обращения: 14.05.2025).

68. Приговор по уголовному делу № 1-86/2025 // Тоншаевский районный суд Нижегородской области : офиц. сайт. URL: https://tonshaevsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=46728556&case_uid=a1bcda d7-e8c2-4fa0-be37-9515948dce42&delo_id=1540006 (дата обращения: 30.10.2025).

69. Приговор по уголовному делу № 3/1-0338/2025 // Официальный портал судов общей юрисдикции города Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/rs/tverskoj/services/cases/criminal-materials/details/5187dbb0-b6fb-11f0-8e85-6d57f7d43af6> (дата обращения: 01.11.2025).

70. Приговор по уголовному делу № 10-17703/2025 // Официальный портал судов общей юрисдикции города Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/mgs/services/cases/appeal-criminal/details/03273280-782c-11f0-bc99-8d8541b34621> (дата обращения: 01.09.2025).

71. Приговор по уголовному делу № 1-188/2025 // Приволжский районный суд г. Казани Республики Татарстан : офиц. сайт. URL: https://privolzhsky--tat.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=365473880&case_uid=5978fa7b-f7ce-4e95-8479-7a42883090fe&delo_id=1540006 (дата обращения: 08.02.2025).

72. Приговор по уголовному делу № 1-480/2024 // Вахитовский районный суд г. Казани : офиц. сайт. URL: https://vahitovsky--tat.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=370408556&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

73. Приговор по уголовному делу № 1-8/2024 // Ленинский районный суд г. Саранска Республики Мордовия : офиц. сайт. URL: https://leninsky--mor.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=131817209&case_uid=d1943dd0-9e60-434d-ae7c-ad5096407646&delo_id=1540006 (дата обращения: 08.02.2025).

74. Приговор по уголовному делу № 1-103/2024 // Октябрьский городской суд Республики Башкортостан : офиц. сайт. URL: http://oktabrsky--bkr.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=147445045&case_uid=aec2f93c-2992-4d83-99a9-dc95e9804546&delo_id=1540006 (дата обращения: 08.02.2025).

75. Приговор по уголовному делу № 1-243/2024 // Оренбургский районный суд Оренбургской области : офиц. сайт. URL: https://orenburgsky--orb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=265996474&case_uid=b8b16dc1-0cd8-4f1e-b828-2e411e9f587d&delo_id=1540006 (дата обращения: 08.02.2025).

76. Приговор по уголовному делу № 01-0285/2024 // Официальный портал судов общей юрисдикции г. Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/rs/lyublinskij/services/cases/criminal/details/29d72bc0-fb9c-11ec-956b-a9e3851a82ca> (дата обращения: 08.02.2025).

77. Приговор по уголовному делу № 1-288/2024 // Промышленный районный суд г. Ставрополя : офиц. сайт. URL: https://promyshleny--stv.sudrf.ru/modules.php?name=sud_delo&srv_%20num=1&name_op=doc&number=425524525&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

78. Приговор по уголовному делу № 1-250/2024 // Советский районный суд г. Томска : офиц. сайт. URL: https://sovetsky--tms.sudrf.ru/modules.php?name=sud_delo&srv_num=1&nameop=doc&number=11138974&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

79. Приговор по уголовному делу № 1-977/2023 // Стерлитамакский городской суд Республики Башкортостан : офиц. сайт. URL: http://sterlitamaksky--bkr.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=134549564&case_uid=21cf7e70-e48d-462a-a09e-e84f634e8980&delo_id=1540006 (дата обращения: 08.02.2025).

80. Приговор по уголовному делу № 1-608/2023 // Советский районный суд г. Томска : офиц. сайт. URL: http://sovetsky--tms.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=11134764&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

81. Приговор по уголовному делу № 1-171/2023 // Вахитовский районный суд г. Казани : офиц. сайт. URL: https://vahitovsky--tat.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=236195779&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

82. Приговор по уголовному делу № 1-637/2023 // Гагаринский районный суд г. Севастополя : офиц. сайт. URL: https://gagarinskiy--sev.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=51710604&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

83. Приговор по уголовному делу № 1-15/2023 // Тимашевский районный суд Краснодарского края : офиц. сайт. URL: http://timashevsky--krd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=363864441&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

84. Приговор по уголовному делу № 1-45/2022 // Ковровский городской суд Владимирской области : офиц. сайт. URL: http://kovrovsky--wld.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=120430332&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

85. Приговор по уголовному делу № 1-131/2022 // Первоуральский городской суд Свердловской области : офиц. сайт. URL: http://pervouralsky--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=409327185&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

86. Приговор по уголовному делу № 1-142/2022 Саяногорский городской суд Республики Хакасия : офиц. сайт. URL: http://saianogorsky--hak.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=53520798&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

87. Приговор по уголовному делу № 1-237/2022 Харабалинский районный суд Астраханской области : офиц. сайт. URL: http://harabalinsky--ast.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=182264936&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

88. Приговор по уголовному делу № 1-250/2022 // Центральный районный суд г. Симферополя Республики Крым : офиц. сайт. URL: http://centr-simph--krm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=99109845&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

89. Приговор по уголовному делу № 1-233-36/2020 // Ленинский районный суд г. Мурманска : офиц. сайт. URL: http://lensud--krs.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=156511389&case_uid=01f90cd7-fe7b-4b82-9d03-01b4818dfb03&delo_id=1540006 (дата обращения: 08.02.2025).

90. Приговор по уголовному делу № 1-149/2019 // Саровский городской суд Нижегородской области : офиц. сайт. URL: https://sarovsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=104015501&case_uid=a2519d1d-d5f3-45c8-a536-2386e9b88b75&delo_id=1540006 (дата обращения: 08.02.2025).

91. Приговор по уголовному делу № 1-167/2019 // Саровский городской суд Нижегородской области : офиц. сайт. URL: https://sarovsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=104015975&case_uid=d45ac732-0fab-45e1-b969-34e877aad8dd&delo_id=1540006 (дата обращения: 08.02.2025).

92. Приговор по уголовному делу № 1-105/2016 // Кировградский городской суд Свердловской области : офиц. сайт. URL: http://kirovgradsky--cvd.sudrf.ru/modules.php?name=sud_delo&srvnum=1&name_op=doc&number=17566285&delo_id=1540006&new=0&text_number=1 (дата обращения: 08.02.2025).

93. Приговор по уголовному делу № 10-15427 // Официальный портал судов общей юрисдикции г. Москвы : офиц. сайт. URL: <https://mos-gorsud.ru/mgs/cases/docs/content/4ce5f02c-a4ae-45ae-a0a1-8a539cb978c5> (дата обращения: 08.02.2025).

Учебники, монографии, учебные пособия

94. Аверченков, В. И. Защита персональных данных в организации : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. – М. : Флинта, 2021. – 124 с.
95. Аверьянова, Т. В. Криминалистика : учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. – М. : Норма : Инфра-М, 2023. – 928 с.
96. Агафонов, В. В. Особенности формирования доказательств с использованием информации о соединениях между абонентами и (или) абонентскими устройствами: криминалистические и процессуальные аспекты : монография / В. В. Агафонов, С. А. Вазюлин, В. Ф. Васюков. – М. : Юрлитинформ, 2015. – 184 с.
97. Агibalов, В. Ю. Виртуальные следы в криминалистике и уголовном процессе: монография / Агibalов В.Ю. – М. : Юрлитинформ, 2012. – 152 с.
98. Аминев, Ф. Г. Актуальные проблемы формирования и использования экспертно-криминалистических учетов в расследовании и раскрытии преступлений : монография / Ф. Г. Аминев. Уфа : РИО БашГУ, 2004. – 182 с.
99. Анирад, К., Сиддха, Г., Мехер, К. Искусственный интеллект и компьютерное зрение: реальные проекты на Python, Keras и TensorFlow / К. Анирад, Г. Сиддха, К. Мехер. – СПб. : Питер, 2023. – 624 с.
100. Антонян, Е. А., Обзор правоприменительной практики по противодействию киберпреступлений / Е. А. Антонян, Е. Р. Россинская, Е. Н. Клещина. – М. : Консорциум «Инновационная юриспруденция», 2024. – 88 с.
101. Асито, Ф. Предсказательная аналитика с Ktime / Ф. Асито. – М. : ДМК Пресс, 2025. – 360 с.
102. Бабкин, Э. А. Принципы и алгоритмы искусственного интеллекта : монография / Э. А. Бабкин, О. Р. Козырев, И. В. Куркина. – Н. Новгород : Нижегородский государственный технический университет, 2006. – 132 с.
103. Баев, О. Я. Избранные работы / О. Я. Баев. – Воронеж : Воронежский государственный университет, 2011. – Т. 2. – 432 с.
104. Баев, О. Я. Основы методики уголовного преследования и профессиональной защиты от него: (на примере уголовно-процессуального исследования должностных и служебных преступлений) : научно-практическое пособие. – М. : Эксмо, 2009. – 396 с.
105. Белкин, Р. С. История отечественной криминалистики / Р. С. Белкин. – М. : Норма, 1999. – 496 с.
106. Белкин, Р. С. Криминалистика: проблемы, тенденции, перспективы

/ Р. С. Белкин. Общая и частные теории. – М. : Юрид. лит., 1987. – 270 с.

107. Белкин, Р. С. Курс криминалистики / Р. С. Белкин. – М. : Юнити, 2001. – Т. 1. – 394 с.

108. Белкин, Р. С. Курс криминалистики / Р. С. Белкин. – М. : Юнити, 2001. – Т. 3. – 837 с.

109. Белкин, Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. – М.: Норма: Норма-Инфра-М, 2001. – 240 с

110. Белкин, Р. С. Собираение, исследование и оценка доказательств. Сущность и методы / Р. С. Белкин. – М. : Наука, 1966. – 296 с.

111. Белкин, А. Р. Теория доказывания в уголовном судопроизводстве / Р. С. Белкин. – М. : Норма, 2007. – 528 с.

112. Бердникова, О. П. Особенности расследования мошенничества в сфере компьютерной информации: учебное пособие / О. П. Бердникова, Р. А. Дерюгин. – Екатеринбург : Уральский юридический институт МВД России, 2021. – 83 с.

113. Бессонов, А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография / А. А. Бессонов. – М. : Проспект, 2021. – 816 с.

114. Бессонов, А. А. Основы криминалистического учения об исследовании и использовании криминалистической характеристики преступлений : монография / А. А. Бессонов. – М. : Юрлитинформ, 2016. – 256 с.

115. Боев, В. Д. Имитационное моделирование систем / В. Д. Боев. – М. : Юрайт, 2025. – 253 с.

116. Бойцов, А. К., Практическое моделирование на UML : монография / А. К. Бойцов, С. С. Колмогорова. – СПб. : Реноме, 2023. – 684 с.

117. Боровская, Е. В., Давыдова, Н. А. Основы искусственного интеллекта : учебное пособие / Е. В. Боровская, Н. А. Давыдова. М. : Лаборатория знаний, 2020. – 130 с.

118. Вандер, М. Б. Схемы криминалистических алгоритмов. СПб. : СПбЮИ, 1998. – 32 с.

119. Ватьян, А. С., Гусарова, Н Ф., Добренко, Н В. Data science: проблемы и решения / А. С. Ватьян, Н Ф. Гусарова, Н В. Добренко. – СПб. : Университет ИТМО, 2025. – 219 с.

120. Вехов, В. Б. Компьютерное моделирование при расследовании преступлений в сфере компьютерной информации : учеб. пособие / В. Б. Вехов, С. А. Ковалев. – Волгоград : ВА МВД России, 2014. – 77 с.

121. Вехов, В. Б. Компьютерные преступления. Способы совершения. Методики расследования. – М. : Право и закон, 1996. – 136 с.
122. Видонов, Л. Г. Криминалистические характеристики убийств и системы типовых версий о лицах, совершивших убийство без очевидцев – методические рекомендации к использованию систем типовых версий. – Горький, 1978. – 122 с.
123. Возгрин, И. А. Введение в криминалистику: История, основы теории, библиография. – СПб. : 2003.– 473 с.
124. Возгрин, И. А. Криминалистическая методика расследования преступлений. – Минск : Вышэйшая школа, 1983. – 215 с.
125. Волчецкая, Т. С. Криминалистическая ситуалогия : монография. – М. ; Калинингр. ун-т. Калининград, 1997. – 248 с.
126. Волынский, А. Ф. Криминалистика и криминалистическая деятельность. Избранное : научное издание. – М. : Юнити-Дана : Закон и право. 2019. – 426 с.
127. Воробьева А.А. История развития программно- аппаратных средств защиты информации / А.А. Воробьева, И.С. Пантюхин. – СПб. : Университет ИТМО, 2017. – 62 с.
128. Гавло, В. К. Теоретические проблемы и практика расследования отдельных видов преступлений. – Томск, 1985. – 333 с.
129. Герасимов, И. Ф. Общие положения методики расследования преступлений. – М. : Высш. шк., 1994. – 560 с.
130. Головин, А. Ю. Криминалистическая систематика : монография. – М. : ЛексЭст. 2002. – 335 с
131. Голунский, С. А. Криминалистика: методика расследования отдельных видов преступлений / С. А. Голунский, Б. М. Шавер, А. Я. Вышинский. – М. : Юриздат, 1939. – 372 с.
132. Гольдберг, Й. Нейросетевые методы в обработке естественного языка. – М. : ДМК Пресс, 2019. – 282 с.
133. Гончаренко В. И. Использование данных естественных и технических наук в уголовном судопроизводстве. – Киев : Высшая школа, 1980. – 157 с.
134. Гриненко А. В. Уголовно-процессуальный кодекс Российской Федерации: постатейный научно-практический комментарий : учебное пособие. – М. : Проспект, 2019. – 968 с.
135. Девис, Дж. Обучение с малым количеством данных. – Литрес, 2024. – 123 с.
136. Драпкин, Л. Я., Карагодин, В. Н. Криминалистика. – М. : Проспект, 2007. – 663 с.

137. Дунин, В. С., Скрипко, П.Б. Инфокоммуникационные технологии и средства обеспечения информационной безопасности в деятельности подразделений, участвующих в раскрытии и расследовании преступлений в сфере информационно-коммуникационных технологий. – Хабаровск : РИО ДВЮИ МВД России, 2019. – 88 с.
138. Егоров, Н. Н. Собираение вещественных доказательств: понятие, содержание, направления совершенствования : монография. – Хабаровск : Дальневосточный государственный университет путей сообщения, 2005. – 111 с.
139. Ермолович, В. Ф. Криминалистическая характеристика преступлений. – Минск : Амалфея, 2001. – 304 с.
140. Есаков, Г. А. Комментарий к Уголовному кодексу Российской Федерации (постатейный). – М. : Проспект, 2021. – 816 с.
141. Зараменских, Е. П. Управление жизненным циклом информационных систем: монография. – Новосибирск : Издательство «Центр развития научного сотрудничества», 2014. – 270 с.
142. Зверьянская, Л. П. Проблемы выявления и расследования киберпреступлений : монография. – Красноярск : Сиб. федер. ун-т, 2016. – 176 с.
143. Земцова, С. И., Суров, О. А., Галушин, П. В. Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий. – М. : Юрлитинформ, 2019. – 208 с.
144. Зеленский, В. Д. Криминалистика / В. Д. Зеленский, Г. М. Меретуков. – Санкт-Петербург : Юридический центр-Пресс, 2015. – 755 с.
145. Зорин, А. Г. Теоретические основы криминалистики. – Минск : Амалфея, 2000. – 416 с.
146. Ищенко, П. П. Информационное обеспечение следственной деятельности: научно-практическое пособие. – М. : Юрлитинформ, 2011. – 168 с.
147. Каневский, Л. Л. Криминалистические проблемы расследования и профилактики преступлений несовершеннолетних. – Красноярск : Красноярский университет, 1991. – 228 с.
148. Клепицкий, И. А. Комментарий к Уголовному кодексу Российской Федерации (постатейный). – М. : РИОР ИНФРА-М, 2019. – 710 с.
149. Ковалев, С. А. Особенности компьютерного моделирования при расследовании преступлений в сфере компьютерной информации : монография / С. А. Ковалев, В. Б. Вехов. – М. : Буки-Веди, 2015. – 182 с.
150. Колычева, А. Н. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие / А.Н. Колычева, В.Ф. Васюков; под ред. А. Г. Волеводза. – М.: Проспект, 2020 – 200 с.

151. Колдин, В. Я. Типовые модели и алгоритмы криминалистического исследования. – М. : Московский университет, 1989. – 184 с.
152. Корноухов, В. Е., Богданов В. М., Закатов А. А. Основы общей теории криминалистики. – Красноярск : Изд-во Краснояр. ун-та, 1993. – 152 с.
153. Лузгин, И. М. Расследование как процесс познания. – М. : Высшая школа МВД СССР, 1969. – 178 с.
154. Косарев, С. Ю. История и теория криминалистических методик расследования преступлений. – СПб. : Юридический центр Пресс, 2008. – 495 с.
155. Кохендерфер, М. Алгоритмы принятия решений / М. Кохендерфер, К. Рэй, Т. Уилер. – М. : ДМК Пресс, 2023. – 686 с.
156. Куликов, С. С. Тестирование программного обеспечения. Базовый курс. – Минск : Четыре четверти, 2020. – 312 с.
157. Ледащев, В. А. Общие положения криминалистической методики. – Волгоград : М-во внутр. дел СССР, 1976. – 16 с.
158. Лузгин, И. М. Моделирование при расследовании преступлений. – М. : Юрид. лит., 1981. – 152 с.
159. Малашенко, А. В. Становление постиндустриальной цивилизации: от цифровизации до варварства : монография / А. В. Малашенко, Ю. А. Нисневич, А. В. Рябов. – М. : Юрайт, 2024. – 212 с.
160. Маунт, Д. Погружение в аналитику данных. – СПб. : БХВ-Петербург, 2023. – 224 с.
161. Менжега, М. М. Методика расследования создания и использования вредоносных программ для ЭВМ. – М. : Юрлитинформ, 2009. – 184 с.
162. Мещеряков, В. А. Теоретические основы механизма слеодообразования в цифровой криминалистике : монография. – М. : Проспект, 2022. – 176 с.
163. Митричев, С. П. Методика расследования отдельных видов преступлений. – М. : Всесоюз. юрид. заоч. ин-т, 1973. – 38 с.
164. Мишра, П. Объяснимые модели искусственного интеллекта на Python. Модель искусственного интеллекта. Объяснения с использованием библиотек, расширений и фреймворков на основе языка Python. – М. : ДМК Пресс, 2022. – 298 с.
165. Морхат, П. М. Искусственный интеллект: правовой взгляд : монография. – М. : Буки Веди, 2017. – 257 с.
166. Нестеров, А. В. Виртуальные следы в криминалистике : учебник. – М. : КноРус, 2024. – 154 с.
167. Николенко, С. И. Машинное обучение: основы. – СПб. : Питер, 2025. – 608 с.

168. Овчинский, С. С. Оперативно-розыскная информация : монография. – М. : Инфра-М, 2024. – 415 с.
169. Омельченко, В. А., Фаниев, П. А. Использование программного обеспечения категории Open Source, для создания анонимной рабочей среды и проведения разведки OSINT. – М. : Перо, 2024. – 69 с.
170. Остроух, А. В. Введение в искусственный интеллект : монография. – Красноярск : Научно-инновационный центр, 2020. – 250 с.
171. Остроух, А. В. Интеллектуальные системы: монография. – Красноярск : Научно-инновационный центр, 2020. – 316 с.
172. Отюцкий, Г. П. Концепции современного естествознания. – М. : Юрайт, 2025. – 447 с.
173. Пантелеев, И. Ф. Методика расследования преступлений : учеб. пособие. – М. : Всесоюз. юрид. заоч. ин-т, 1975. – 44 с.
174. Петровская, В. Н., Щепин, В. И. Концепции современного естествознания : словарь терминов. – Иркутск : Изд-во ИрГТУ, 2008. – 104 с.
175. Полевой, Н. С Криминалистическая кибернетика. – М. : Изд-во МГУ, 1982. – 208 с.
176. Попов, А. Н. Преступления в сфере компьютерной информации : учебное пособие. – Санкт-Петербург : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. – 68 с.
177. Постолит, А. В. Основы искусственного интеллекта в примерах на Python. – СПб. : БХВ-Петербург, 2024. – 448 с.
178. Пискунова, Е. В. Компьютерные технологии в судебной экспертизе : практикум. – М. : РГУП, 2017 с.
179. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие / под ред. С. В. Зуева, В. Б. Вехова. – М. : Юрайт, – 2025. 243 с.
180. Россинская, Е. Р. Избранное. – М. : Норма, 2021. – 680 с.
181. Россинская, Е. Р. Криминалистика. – М. : Юр. Норма, Инфра-М, 2025. – 608 с.
182. Россинская, Е. Р. Криминалистика : учебник. – М. : Норма : Инфра-М, 2022. – 464 с.
183. Россинская, Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности : монография. – М. : Проспект, 2022. – 256 с.
184. Россинская, Е. Р., Неретина, Н. С., Чубина, Е. А. Современное состояние и перспективы развития машинного обучения и искусственного интеллекта для решения задач судебно-экспертной деятельности : аналитический обзор.

– М. : Консорциум «Инновационная юриспруденция», 2024. – 46 с.

185. Русскевич, Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография. – М. : Инфра-М, 2022. – 352 с.

186. Савельев, А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» : комментарий. – М. : Статут, 2017. – 321 с.

187. Садохин, А. П. Концепции современного естествознания. – М. : Юнити-Дана, 2006. – 447 с.

188. Саркисян, А. А. Цифровизация судебно-экспертной деятельности. – М. : Юрайт, 2025. – 138 с.

189. Себякин, А. Г. Тактика использования знаний в области компьютерной техники : монография. – М. : Юрлитинформ, 2023. – 196

190. Селиванов, Н. А. Математические методы в собирании и исследовании доказательств : монография. – М. : Юридическая литература, 1974. – 120 с.

191. Смушкин, А. Б. Концепция дистанционной криминалистики : монография / под ред. В. Б. Вехова. – М. : Юрлитинформ, 2024. – 256 с.

192. Смушкин, А. Б. Криминалистические аспекты использования киберпространства и обеспечения кибербезопасности: монография / под ред. В. Б. Вехова. – М. : Русайнс, 2024. – 196 с.

193. Соловьева, Т. Н. Информатика. Основы алгоритмизации и программирования. – Пермь : Пермский государственный национальный исследовательский университет, 2018. – 118 с.

194. Сологубова, Г. С. Составляющие цифровой трансформации : монография. – М. : Юрайт, 2024. – 147 с.

195. Станкевич, Л. А. Интеллектуальные системы и технологии : учебник и практикум для вузов. – М. : Юрайт, 2025. – 478 с.

196. Стивен, С. Наука о данных: учебный курс. – СПб. : Диалектика, 2020. – 544 с.

197. Стрижов, В. В. Методы индуктивного порождения регрессионных моделей. – М. : Вычислительный центр им. А. А. Дородницына Российской акад. наук, 2008. – 56 с.

198. Татарникова, Т. М. Интеллектуальный анализ данных : учебное пособие. – М. ; Вологда : Инфра-Инженерия, 2024. – 172 с.

199. Трофимов, В. В. Алгоритмизация и программирование: монография / В. В. Трофимов, Т. А. Павловская. – М. : Юрайт, 2024. – 108 с.

200. Тьюки, Дж. Анализ результатов наблюдений. Разведочный анализ. – М. : Мир, 1981. – 696 с.

201. Тюхтин, В. С. Отражение, системы, кибернетика. Теория отражения в свете кибернетики и системного подхода. – М. : Наука, 1972. – 256 с.
202. Федоров, Г. В., Григорович, В. Л. Инновационные направления развития криминалистики : монография. – М. : Юрлитинформ, 2012. – 270 с.
203. Федотов, Н. Н. Форензика – компьютерная криминалистика. – М. : Юридический мир, 2007. – 432 с.
204. Харисова, З. И. Информационные технологии в управлении органами внутренних дел : учебное пособие / З. И. Харисова, В. В. Антонов, Н. Р. Калимуллин. – Уфа : Уфимский ЮИ МВД России, 2022. – 48 с.
205. Харисова, З. И. Международно-правовые аспекты обеспечения информационной безопасности в сети Интернет : учебное пособие / З. И. Харисова, В. В. Антонов, В. А. Колесников. – Уфа : Уфимский ЮИ МВД России, 2021. – 48 с.
206. Хлынцов, М. Н. Криминалистическая информация и моделирование при расследовании преступлений. – Саратов : Изд-во Саратов. ун-та, 1982. – 159 с.
207. Хултен, Дж. Разработка интеллектуальных систем. – М. : ДМК Пресс, 2019. – 284 с.
208. Шаталов, А. С. Криминалистические алгоритмы и программы: теория, практика, прикладные аспекты. – М. : Лига Разум, 2000. – 250 с.
209. Эксархопуло, А. А. Криминалистика: история и перспективы развития : монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. – М. : Юрайт, 2024. – 167 с.
210. Эксархопуло, А. А. Криминалистика : учебник. – Санкт-Петербург : Лема, 2010. – 904 с.
211. Большая советская энциклопедия : в 35 томах . – Москва : Советская энциклопедия, 1976. – Том 25 : Струнино – Тихорецк. – 663 с.
212. Вещественные доказательства: информационные технологии процессуального доказывания / под ред. В. Я. Колдина. – М. : Норма, 2002. – 768 с.
213. Выявление причин преступности и предупреждение преступлений. Общие положения : учебное пособие / Гришанин П. Ф., Зуйков Г. Г., Кривошеев А. С., Ратинов А. Р. и др. – М. : НИиРИО МВШ МООП СССР, 1967. – 179 с.
214. Инновационные образовательные технологии и методики в образовательных организациях МВД России : аналитический обзор. – М. : Московский ун-т МВД России, 2024. – 132 с.
215. Искусственный интеллект в юридической деятельности : учебник для вузов / под ред. С. Е. Чаннова. – М. : Юрайт, 2025. – 131 с.
216. История науки, техники и транспорта учебник для вузов / под ред. В. В. Фортунатова. – М. : Юрайт, 2024. – 432 с.

217. ИТ-справочник следователя : монография / под ред. С. В. Зуева. – М. : – Юрлитинформ, 2019. – 232 с.

218. Комментарий к Уголовному кодексу РФ в 4 т. Том 3. Особенная часть. Раздел IX / В. М. Лебедев [и др.]. – М. : Юрайт, 2024. – 298 с.

219. Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 года и ожидаемые тенденции ее развития : аналитический обзор / М. В. Гончарова, М. М. Бабаев, Р.В. Черкасов [и др.]. – М. : ФГКУ «ВНИИ МВД России», 2024. – 87 с.

220. Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития : аналитический обзор / М. В. Гончарова, М. М. Бабаев, Р.В. Черкасов [и др.]. – М. : ФГКУ «ВНИИ МВД России», 2025. – 85 с.

221. Криминалистика : учебник для бакалавров / под ред. Л. В. Бертовского. – М. : РГ-Пресс, 2018. – 960 с.

222. Криминалистика : учебник / под ред. А. Ф. Волынского, В. П. Лаврова. – М. : Юнити-Дана, 2015. – 944 с.

223. Криминалистика: методика расследования преступлений / под ред. И. В. Александрова. Т. 5. – М. : Юрайт, 2025. – 242 с.

224. Криминалистика. Теоретический курс : монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин и др. – Уфа : НИИ ППГ, 2022. – 650 с.

225. Криминалистика : учебник / под ред. Н. П. Яблокова, И. В. Александрова. – М. : Норма : Инфра-М, 2017. – 752 с.

226. Криминалистика : учебник / под ред. И. М. Комарова. – М. : Юрлитинформ, 2023. – 712 с.

227. Криминалистическая методика расследования отдельных видов и групп преступлений : учебное пособие / В. Д. Зеленский, Г. М. Меретуков, А. В. Гусев, С. А. Данильян. – Краснодар : КубГАУ, 2013. – 355 с.

228. Криминалистическая техника : учебник / под ред. А. И. Бастрыкина. – М. : Юрайт, 2025. – 204 с.

229. Криминалистическая техника : учебник / под ред. К. Е. Демина. – М. : Юридический институт Российского университета транспорта, 2017. – 426 с.

230. Курс криминалистики : сборник научных трудов : в 3 томах / под ред. О. Н. Коршуновой. Т. 1: Общая теория криминалистики. Криминалистическая техника. Криминалистическая тактика. – СПб. : Юридический центр, 2024. – 720 с.

231. Курс криминалистики : сборник научных трудов : в 3 томах / под ред. О. Н. Коршуновой. Т. 2. Общие положения криминалистической методики. Методика расследования преступлений против личности. Методика расследования

преступлений против собственности. – СПб. : Юрический центр, 2024. – 656 с.

232. Курс криминалистики : сборник научных трудов : в 3 томах / под ред. О. Н. Коршуновой. Т. 3: Методика расследования преступлений в сфере экономической деятельности. Методика расследования преступлений против общественной безопасности, других видов и групп преступлений. – СПб. : Юрический центр, 2024. – 752 с.

233. Кондаков, Н. И. Логический словарь-справочник. – М. : Наука, 1975. – 720 с.

234. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / И. Г. Чекунов, И. А. Рядовский, А. В. Пузарин [и др.] ; МосУ МВД России имени В.Я. Кикотя. – Москва : Московский университет МВД России, 2019. – 175 с.

235. Моделирование систем и процессов: практический курс / отв. ред. В. Н. Волкова. – М. : Юрайт, 2025. – 295 с.

236. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет : монография / под ред. А. С. Дупан. – М. : Изд. дом Высшей школы экономики, 2018. – 343 с.

237. Особенности информационного обеспечения профессиональной деятельности в органах внутренних дел : учебное пособие / З. И. Харисова, В. В. Антонов, В. Р. Гурьянова, Н. Р. Калимуллин. – Уфа : Уфимский ЮИ МВД России, 2022. – 48 с.

238. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, З. И. Харисова, С. Р. Низаева, В. Р. Гайнелзянова. – Уфа : Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2023. – 96 с.

239. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, В. Р. Гайнелзянова, З. И. Харисова. – М. : ГУРЛС МВД России, 2024. – 95 с.

240. Особенности производства предварительного следствия по уголовным делам о преступлениях, связанных с неправомерным доступом к компьютерной информации, в том числе совершенных путем кибератак (сетевых атак) : научно-практическое пособие / Е. А. Пидусов [и др.] ; под ред. Е. А. Пидусова. – Воронеж : Воронежский институт МВД России, 2024. – 59 с.

241. Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования : монография / А. Ф. Абдулвалиев [и др.] ; под ред. Е. В. Смахина, Д. Шарапова, В. И. Морозова.

– Тюмень : Издательство Тюменского государственного университета, 2021. – 376 с.

242. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Червяков Н. И. [и др.]. – М. : Физматлит, 2012. – 279 с.

243. Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий: научно-практическое пособие / А.Л. Аристархов, К.В. Камчатов [и др.]. – Москва : Университет прокуратуры Рос. Федерации., 2023. – 122 с.

244. Противодействие преступлениям, совершаемым с использованием современных информационно-телекоммуникационных технологий: отдельные аспекты : учебное пособие / З. И. Харисова, В. Р. Гурьянова, Г. А. Тугузбаев, А. С. Ишмеева. – Уфа : Уфимский ЮИ МВД России, 2023. – 48 с.

245. Процессуальная деятельность защитника по собиранию и представлению доказательств в российском уголовном судопроизводстве : монография / А. И. Аверьянов [и др.] ; под ред. Н. Р. Мухудиновой. – Саранск : Издательство Мордовского университета, 2008. – 61 с.

246. Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров : методические рекомендации. – М. : ЭКЦ МВД России, Следственный департамент МВД России, ГУНК МВД России, 2020. – 18 с.

247. Сбор и анализ цифровых следов преступления : практическое пособие / С. В. Петраков [и др.]. – СПб. : Санкт-Петербургская академия Следственного комитета Российской Федерации, 2023. – 98 с.

248. Современные направления развития криминалистических методик и технологий в уголовном судопроизводстве : монография / под ред. Д. В. Кима. – Красноярск : Сиб. федер. ун-т, 2020. – 244 с.

249. Справочник по подготовке, организации, назначению и производству судебных экспертиз в судебно-экспертных учреждениях Минюста России. – М. : ФБУ РФЦСЭ при Минюсте России, 2024. – 106 с.

250. Справочник следователя : научно-методическое пособие. Т 2. – М.: ФГКУ ВНИИ МВД России, 2023. – 730 с.

251. Тактика обнаружения, изъятия и осмотра средств электронных носителей информации и их подготовки для назначения судебных экспертиз : учебно-практическое пособие / О. А. Гребенюк, Д. Н. Жидков, Е. Н. Макарова, О. Л. Романова.

– Санкт-Петербург : Санкт-Петербургский университет МВД России, 2020. – 48 с.

252. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под ред. В. Б. Вехова, С. В. Зуева. – М. : Юрайт, 2024. – 490 с.

253. Цифровые следы преступлений : монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. – М. : Проспект, 2023. – 168 с.

254. Шелупанов, А. А., Смолина, А. Р. Форензика. Теория и практика расследования киберпреступлений. – М. : Горячая линия Телеком, 2018. – 104 с.

255. Barik, K. Lecture notes on data engineering and communications technologies / K. Barik, A. Abirami, K. Konar. – Berlin : Springer science and business media, 2022. – 95 p.

256. Baroniya, Y. Cyber and digital forensic. Textbook of forensic science / Y. Baroniya, V. Bharadwaj. – Singapore : Springer, 2023. – 803 p.

257. Carrier, B. Forefile systemnsic analysis / B. Carrier. – Indianapolis : Pearson Education Inc, 2005. – 511 p.

258. Chawki, M. Cybercrime, digital forensics and jurisdiction / M. Chawki, A. Darwish, S. Khan. – Switzerland : Springer international publishing, 2015. – 145 p.

259. Chen, X. Cyber security meets machine learning. Cyber security meets machine learning / X. Chen, W. Susilo, E. Bertino. – Hamburg : Springer Nature, 2021 – 163 p.

260. Cormen, T. H. Introduction to algorithms / T. H. Cormen, C. E. Leiserson. – London : The Massachusetts institute of technology. – 1313 p.

261. Dariusz, S. Legal tech: information technology tools in the administration of justice / S. Dariusz, Z. Mariusz. – Baden-Baden : NomosVerlagsgesellschaft, 2021. – 665 p.

262. Dhanaraj, R. Digital twin technologies for healthcare 4.0 / R. Dhanaraj, S. Murugesan, B. Balusamy. – London : The institution of engineering, 2022. – 207 p.

263. Edwards, J. Mastering cybersecurity strategies, technologies and best practices. – Hamburg : Springer Nature (APress media), 2024 – 790 p.

264. Ganesh, N. S., Lecture notes on data engineering and communications technologies / N. S. Ganesh, N. G. Venkatesh, D. V. Prasad. – Berlin : Springer science and business media, 2022. – 229 p.

265. Garcia-Mateo, C. Voice biometrics: technology, trust and security. voice biometrics: technology, trust and security / C. Garcia-Mateo, G. Chollet. – Stevenage : Institution of engineering and technology, 2021. – 234 p.

266. Jajodia, S. SIEM system. Encyclopedia of cryptography, security and privacy / S. Jajodia, P. Samarati, M. Yung. – Cham : Springer, 2025. – 2412 p.

267. Harisha, A. Advancements in cybercrime investigation and digital forensics. Advancements in cybercrime investigation and digital forensics / A. Harisha, A. Mishra, C. Singh. – New York : Apple Academic Press, 2023. – 403 p.

268. Holt, T. J. Cybercrime and digital forensics. introduction. / T. J. Holt, A. M. Bossler, K. C. Seigfried-Spellar. – Abingdon : Routledge, 2018. – 754 p.
269. Jain, R. Analyzing the procedure for investigation in cybercrime and admissibility of electronic evidence / R. Jain, B. Sonowal. – Cham : Springer, 2025. – 289 p.
270. Josang, A. Cyber organizational structures and regulation. – Cham : Springer, 2025. – 375 p.
271. Lanhamai, M. AI-agents in action. – Shelter island : Manning Publications Co, 2025. – 346 p.
272. Masmoudi, S. Unveiling the human factor in cybercrime and cybersecurity: motivations, behaviors, vulnerabilities, mitigation strategies, and research methods. – Cham : Springer, 2025. – 91 p.
273. Medjedovic, Dz. Algorithms and data structures for massive datasets // Dz. Medjedovic, E. Tahirovic. – New York : Manning Shelter Island, 2024. – 340 p.
274. Mihailescu, M. Quantum algorithms / M. Mihailescu, S. Nita, V. Marascu. – Cham : Springer. – 118 p.
275. Pal, O. Cyber security using modern technologies: artificial intelligence, blockchain and quantum cryptography / O. Pal, V. Kumar, R. Khan. – Clermont : CRC Press, 2023. – 272 p.
276. Parker, D. B. Computer crime: criminal justice resource manual. – Washington : National institute of justice, 1989. – 221 p.
277. Powell, A. Digital criminology: crime and justice in digital society / A. Powell, G. Stratton, R. Cameron. Abingdon-on-Thames : Taylor and Francis, 2018. – 210 p.
278. Raj, E. F. Advancements in cybercrime investigation and digital forensics. – New York : Apple Academic Press, 2023. – 136 p.
279. Reyes, A. Cybercrime investigations: bridging the gaps between security professionals, law enforcement. – Oxford : Syngress Publishing, 2007. – 434 p.
280. Sarker, I. H. AI-Driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability / I. H. Sarker. Perth : Edith Cowan University, 2024. – 207 p.
281. Stamp, M. Malware analysis using artificial intelligence and deep learning / M. Stamp, M. Alazab, A. Shalaginov. – New York : Springer international publishing, 2020. – 651 p.
282. Watters, P. A. Counterintelligence in a cyber world / P. A. Watters. – Switzerland : Springer international publishing, 2023. – 145 p.
283. Xiao, T. Foundations of large language models / T. Xiao, J. Zhu. – Boston : Northeastern University, 2025. – 231 p.

Статьи, тезисы выступлений

284. Аминев, Ф. Г. Организационно-правовые вопросы взаимодействия суда и экспертных организаций при назначении и проведении судебных экспертиз / Ф. Г. Аминев // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической. – Москва : Российский государственный университет правосудия, 2021. – С. 62–67.

285. Антонов, В. В. Проблемы правового регулирования сферы искусственного интеллекта / В. В. Антонов, Н. Р. Калимуллин, З. И. Харисова, М. Р. Гирфанова // Информационные технологии интеллектуальной поддержки принятия решений (ITTDS'2020) : труды VIII Всероссийской научной конференции. – Уфа : Уфимский государственный авиационный технический университет, 2020. – С. 10–14.

286. Бахтеев, Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности / Д. В. Бахтеев // Сибирские уголовно-процессуальные и криминалистические чтения. – 2020. – №2 (28). – С. 32–43.

287. Белей, А. В. Компьютерное криминалистическое исследование вредоносного программного обеспечения / А. В. Белей, С. И. Томская // Правовая информатика. – 2023. – № 2. – С. 102–112.

288. Белей, А. В. Необходимость анализа трендов киберпреступлений и осуществления OSINT для эффективного проведения СКТЭ / А. В. Белей // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции. – Москва : Российский государственный университет правосудия, 2021. – С. 96–101.

289. Бессонов, А. А. Криминалистическая характеристика преступлений в цифровую эпоху / А. А. Бессонов // Развитие научных идей профессора Р. С. Белкина в условиях современных вызовов (к 100-летию со дня рождения) : сборник научных статей по материалам Международной научно-практической конференции. – Москва : Академия управления Министерства внутренних дел Российской Федерации, 2022. – С. 54–62.

290. Бессонов, А. А. О некоторых вопросах использования математических методов в криминалистике и расследовании преступлений / А. А. Бессонов // Математические методы и информационно-технические средства : материалы XVII Всероссийской научно-практической конференции. – Краснодар : Краснодарский университет МВД России, 2021. – С. 33–36.

291. Бессонов, А. А. Современные информационные технологии на службе следствия / А. А. Бессонов // Сибирские уголовно-процессуальные и

криминалистические чтения. – 2022. – № 1. – С. 94–100.

292. Бессонов, А. А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности / А. А. Бессонов. // Академическая мысль. – 2020. – № 4 (13). – С. 58–61.

293. Бортникер, П. В. Сравнительный анализ применения вейвлетов Хаара, Добеши и «Мексиканская шляпа» для обнаружения вторжений в информационные системы // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник материалов XIII Международной научно-технической и научно-методической конференции. – Санкт-Петербург : СПбГУТ, 2024. – С. 126–130.

294. Бычков, В. В. Электронное слеодообразование преступной деятельности в сети Интернет / В. В. Бычков // Расследование преступлений: проблемы и пути их решения. – 2020. – № 1 (27). – С. 106–111.

295. Варданян, А. В. Дискредитация субъектов раскрытия и расследования преступлений и криминалистические методы ее нейтрализации / А. В. Варданян, И. А. Макаренко // Всероссийский криминологический журнал. – 2022. – Т. 16. – № 5. – С. 638–645.

296. Вехов, В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ / В. Б. Вехов // Уголовное право. – 2004. – № 4. – С. 15–17.

297. Вехов, В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства / В. Б. Вехов // Российский следователь. – 2013. – № 10. – С. 22–24.

298. Волеводз, А. Г. О некоторых особенностях получения цифровых доказательств в арабских странах на примере Объединенных Арабских Эмиратов и Королевства Бахрейн / А. Г. Волеводз, А. Д. Цыплакова // Российский следователь. – 2025. – № 1. – С. 45–49.

299. Волчецкая, Т. С. Прикладные аспекты противодействия информационно-мировоззренческим угрозам в цифровом пространстве и особенности их профилактики / Т. С. Волчецкая, М. В. Авакьян // Актуальные проблемы российского права. – 2021. – Т. 16. – № 6 (127). – С. 194–201.

300. Волчецкая, Т. С. Современные направления развития криминалистики как науки и как учебной дисциплины / Т. С. Волчецкая // Вестник Башкирского университета. – 2015. – Т. 20. – № 1. – С. 349–353.

301. Волчецкая, Т. С. Теоретические проблемы использования метода моделирования в криминалистической науке / Т. С. Волчецкая // Социальные и гуманитарные науки на Дальнем Востоке. – 2012. – № 4 (36). – С. 16–20.

302. Воронков, Д. В. О соотношении традиционной криминалистики и цифровой криминалистики / Д. В. Воронков // *Baikal Research Journal*. – 2025. – Т. 16, № 1. – С. 70-75.

303. Гаврилин, Ю. В. Процессуальный порядок собирания доказательств на энергонезависимых локальных электронных носителях информации / Ю. В. Гаврилин, А. А. Балашова // *Сибирский юридический вестник*. – 2020. – № 2 (89). – С. 77–82.

304. Гаврилин, Ю. В. Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин // *Труды Академии управления МВД России*. – 2017. – №4 (44). – С. 45–50.

305. Герасенков, В. М. Объяснения как источник доказательств в уголовном процессе / В. М. Герасенков // *Экономика. Социология. Право*. – 2023. – №3 (31). – С. 92–101.

306. Герасимова, Е. Ю. Следственные ситуации, возникающие на первоначальном и последующем этапах расследования создания, распространения и использования вредоносных компьютерных программ / Е. Ю. Герасимова // *Актуальные проблемы российского права*. – 2024. – Т. 19. – № 1 (158). – С. 166–178.

307. Головин, М. В. Алгоритмизация следственных действий на первоначальном этапе расследования вымогательства / М. В. Головин, Н. М. Шпак // *Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета*. – 2016. – № 123. – С. 930–942.

308. Голубев, Ф. А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации / Ф. Голубев // *Право и политика*. – 2020. – № 10. – С. 50–59.

309. Горбунова, Е. Ю. Проблемы качества судебно-экспертных исследований (судебная компьютерно-техническая экспертиза) / Е. Ю. Горбунова // *Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции*. – Москва : Российский государственный университет правосудия. – 2021. – С. 202–207.

310. Грановский, Г. Л. Криминалистическая ситуационная экспертиза места происшествия / Г. Л. Грановский // *Теоретический семинар – криминалистические чтения : материалы теоретического семинара*. – Москва : ВНИИСЭ МЮ СССР. – 1977. – С. 3–16.

311. Гречкин, В. А. Интеллектуальные алгоритмы обработки информации в многокритериальных системах поддержки принятия решений / В. А. Гречкин // *Вестник Ставропольского государственного университета*. – 2010. – № 5. – С. 35–39.

312. Грибунов, О. П. Концептуальные идеи В. Я. Колдина в криминалистике и судебно-экспертной деятельности / О. П. Грибунов, А. С. Агафонов // *Baikal Research*

Journal. – 2022. – Т. 13. – № 1. – С. 1–8.

313. Грибунов, О. П. Особенности версионной работы по делам о преступлениях против собственности, совершаемых на транспорте / О. П. Грибунов // Библиотека криминалиста. – 2016. – № 4 (27). – С. 135–142.

314. Гуров, О. Н. Искусственные интеллектуальные системы и решение социальных задач: проблема доверия / О. Н. Гуров // Искусственные общества. – 2021. – Т. 16. – № 1. – С. 1–10.

315. Густов, Г. А. Признаки хищений социалистической собственности / Г. А. Густов, В. Г. Танасевич // Вопросы совершенствования предварительного следствия. – 1971. – С. 87–102.

316. Денисов, Е. В. Иерархический кластерный анализ паттернов поведения серийных насильственных преступников / Е. В. Денисов, А. В. Вечерин, Е. Ю. Коростелева // Вестник Воронежского государственного университета. – 2022. – № 3 (50). – С. 300–321.

317. Десницкий, В. А. Подход к обнаружению атак в реальном времени на основе имитационного и графо-ориентированного моделирования / В. А. Десницкий // Информатизация и связь. – 2021. – № 7. – С. 30–35.

318. Драпкин, Л. Я. Принятие оперативно-розыскных и следственных решений в ситуациях информационной неопределенности, конфликта и риска / Л. Я. Драпкин, А. Е. Шуклин // Российский юридический журнал. – 2006. – № 3 (51). – С. 89–96.

319. Драпкин, Л. Я. Проблемы алгоритмизации в криминалистике и следственной деятельности / Л. Я. Драпкин, В. Н. Долинин, А. Е. Шуклин // Российское право: образование, практика, наука. – 2018. – № 6 (108). – С. 31–36.

320. Дроздецкая, А. С. Некоторые проблемы законодательной конструкции состава преступления, предусмотренного статьей 274.2 Уголовного кодекса Российской Федерации // Следственная деятельность: проблемы, их решение, перспективы развития : материалы VII Всероссийской научно-практической конференции. Москва : Московская академия Следственного комитета Российской Федерации. – 2024. – С. 125–130.

321. Дремлюга, Р. И. Проблемы уголовно-правовой регламентации ответственности за преступления, предусмотренные ст. 274.2 УК РФ / Р. И. Дремлюга // Труды Института государства и права РАН. – 2024. – Т. 19. – № 1. – С. 165–189.

322. Долинин, В. Н. Гибкие алгоритмы применения тактических приемов в процессе допроса в бесконфликтной и конфликтной ситуациях / В. Н. Долинин // Вклад Л. Я. Драпкина в криминалистическую науку. Екатеринбург : Уральский государственный юридический университет. – 2019. – С. 110–121.

323. Евдокимов, К. Н. Вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) / К. Н. Евдокимов // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 166–172.

324. Ермолаев, Н. В. К вопросу о разграничении преступлений в сфере компьютерной информации, предусмотренных статьей 272 и ч. 2 ст. 274.1 уголовного кодекса РФ / Н. В. Ермолаев // Вестник Дальневосточного юридического института МВД России. – 2024. – № 2 (67). – С. 41–46.

325. Ефремова, И. А. Киберпространство как новая среда преступности / И. А. Ефремова, А. Б. Смушкин, А. Б. Донченко // Вестник Томского государственного университета. – 2021. – № 472. – С. 248–256.

326. Жбанков, В. А. К вопросу о понятии и содержании поисковой деятельности по установлению личности неизвестного преступника / В. А. Жбанков // Проблемы криминалистической теории и практики: сборник научных трудов. Москва : Юридический институт МВД России. – 1995. – С. 120–130.

327. Жижина, М. В. Возбуждение уголовного дела по факту преступления в сфере компьютерной информации: российский и зарубежный опыт / М. В. Жижина, Д. В. Завьялова // Актуальные проблемы российского права. – 2021. – Т. 16. – № 12 (133). – С. 156–166.

328. Зайцев, О. А. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений / О. А. Зайцев, П. С. Пастухов // Вестник Пермского университета. Юридические науки. – 2022. – № 56. – С. 281–308.

329. Зуйков, Г. Г. «Модус операнди», кибернетика, поиск / Г. Г. Зуйков // Кибернетика и право. – 1970. – № 1 – С. 46–56.

330. Иванов, А. А. Правовая оценка компьютерных преступлений против России на современном этапе / А. А. Иванов, Н. П. Удальцов, С. А. Вавринюк // Человек. Социум. Общество. – 2025. – № 1. – С. 168–175.

331. Иванов, В. В. Зуев, Д. И. Цифровой двойник и цифровая личность: понятие, соотношение, значение в процессе совершения киберпреступлений и в праве в целом / А. А. Иванов, Д. И. Зуев // Правовое государство: теория и практика. – 2022. – № 4. – С. 138–144.

332. Исаенко, В. Н. Криминалистическая характеристика преступлений и ее разновидности / В. Н. Исаенко // Криминалистика. – 2014. – № 1 (14). – С. 41–47.

333. Ищенко, Е. П. У истоков цифровой криминалистики / Е. П. Ищенко // Вестник Университета имени О. Е. Кутафина. – 2019. – № 3 (55). – С. 15–28.

334. Ищенко, Е. П. Типовая информационная модель преступления как основа методики расследования / Е. П. Ищенко, В. Я. Колдин // Известия высших учебных заведений. Правоведение. – 2006. – № 6 (269). – С. 128–144.

335. Калюжный, А. Н. Виды корреляционных взаимосвязей данных криминалистической характеристики преступлений и их значение для процесса расследования / А. Н. Калюжный // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2025. – № 1 (102). – С. 218–226.

336. Каминский, А. М. Криминалистическая категория «след преступления» в анализе правонарушений в сфере компьютерной информации / А. М. Каминский // Уголовно-правовые, уголовно-процессуальные и криминалистические вопросы борьбы с преступностью : сборник научных трудов V Всероссийской научно-практической конференции. – Краснодар: КГАУ, 2021. – С. 169–174.

337. Каминский, М. К. Криминалистическая модель «компьютерных преступлений» / М. К. Каминский // Вестник Удмуртского университета. – 1996. – № 1. – С. 69–73.

338. Каневский, Л. Л. Разработка типовых криминалистических характеристик преступлений и их использование в процессе расследования / Л. Л. Каневский // Российский юридический журнал. – 2000. – № 2 (26). – С. 101–111.

339. Кардашевская, М. В. Предмет преступного посягательства как элемент криминалистической характеристики преступлений / М. В. Кардашевская // Вестник Московского университета МВД России. – № 7. – 2019. – С. 236–238.

340. Ким, Д. В. Криминалистическая характеристика расследования преступлений как результат разрешения следственных ситуаций / Д. В. Ким // Известия Алтайского государственного университета. – 2000. – № 2 (16). – С. 43–48.

341. Ким, А. В. Отдельные вопросы проведения осмотра и экспертизы электронных носителей информации / А. В. Ким // Юридические науки. – 2019. – № 1. – С. 151–156.

342. Козловский, П. В. Участие специалиста в изъятии электронных носителей / П. В. Козловский, П. В. Седельников // Научный вестник Омской академии МВД России. – 2014. – № 1 (52). – С. 17–19.

343. Колдин, В. Я. Типовая информационная модель или криминалистическая характеристика преступления / В. Я. Колдин, Е. П. Ищенко, О. А. Крестовников // Академический юридический журнал. – 2006. – № 4. – С. 1–14.

344. Конькова, Т. А. Агентное моделирование процесса голосования / Т. А. Конькова // Искусственные общества. – 2018. – Т. 13. – № 4. – С. 2–9.

345. Кубасов, И. А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности

оперативных подразделений МВД России / И. А. Кубасов, Л. А. Лекарь // Труды Академии управления МВД России. – 2023. – № 3 (67). – С. 154–161.

346. Левшун, Д. С. Архитектура системы обнаружения и прогнозирования уязвимостей информационных систем на основе методов искусственного интеллекта / Д. С. Левшун // Информатизация и связь. – 2024. – № 3. – С. 91–98.

347. Лозовский, Д. Н. Использование метода криминалистического моделирования в процессе расследования преступлений / Д. Н. Лозовский // Проблемы экономики и юридической практики. – 2010. – № 1. – С. 115–118.

348. Майлис, Н. П. Инновационные технологии, способствующие развитию цифровой трасологии / Н. П. Майлис // Вестник Московского университета МВД России. – 2024. – № 5. – С. 97–99.

349. Макаренко, И. А. Структура частной криминалистической методики: история формирования и перспективы развития / И. А. Макаренко, А. А. Эксархопуло, Р. И. Зайнуллин // Правовое государство: теория и практика. – 2018. – № 4 (54). – С. 146–152.

350. Маликов, А. В. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении / А. В. Маликов, В. С. Авраменко, И. Б. Саенко // Информационно-управляющие системы. – 2019. – № 6 (103). – С. 32–42.

351. Мещеряков, В. А. К вопросу об оценке компетенции судебного эксперта / В. А. Мещеряков, О. Ю. Цурлуй, Ю. С. Кудрявцев // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции. – Москва : Российский государственный университет правосудия. – 2021. – С. 417–422.

352. Мещеряков, В. А. Особенности специальных знаний, используемых в цифровой криминалистике / В. А. Мещеряков // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4 (2). – С. 87–92.

353. Мещеряков, В. А. Следы преступлений в сфере высоких технологий / В. А. Мещеряков // Библиотека криминалиста. – 2013. – № 5 (10). – С. 265–270.

354. Мещеряков, В. А. Формирование доказательств на основе электронной цифровой информации / В. А. Мещеряков, В. В. Трухачев // Вестник Воронежского института МВД России. – 2012. – № 2. – С. 108–110.

355. Михайлова, И. А. О деятельности правоохранительных органов по противодействию преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий / И. А. Михайлова, А. С. Лимарь, Р. И. Гиляев // Вестник экономики, права и социологии. – 2024. – № 2. – С. 109–114.

356. Олиндер, Н. В. Следственные действия на первоначальном этапе расследования преступлений, совершенных с использованием электронных платежных средств и систем / Н. В. Олиндер // Юридический вестник Самарского государственного университета. – 2015. – Т. 1. – № 4. – С. 87–91.

357. Подольный, Н. А. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий / Н. А. Подольный // Библиотека криминалиста. – 2013. – № 5 (10). – С. 116–127.

358. Поляков, В. В. Криминалистическая классификация средств высокотехнологичных преступлений / В. В. Поляков, // Вестник Санкт-Петербургского государственного университета. Право. – 2024. – № 2. – С. 1–21.

359. Потапов, С. М. Принципы криминалистической идентификации / С. М. Потапов // Советское государство и право. – 1940. – № 1. – С. 66–81.

360. Пучков, О. А. Право в зеркале высоких технологий: сравнительный анализ тенденций правового развития / О. А. Пучков // Правовое государство: теория и практика. – 2024. – № 2. – С. 163–172.

361. Россинская, Е. Р. Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений / Е. Р. Россинская // Вестник Восточно-Сибирского института МВД России. – 2021. – № 2 (97). – С. 190–200.

362. Россинская, Е. Р. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова // Вестник Санкт-Петербургского университета. Право. 2020. – Т. 11. – № 3. – С. 745–759.

363. Россинская, Е. Р. Особенности оценки и использования в доказывании результатов судебных экспертиз в условиях цифровизации / Е. Р. Россинская // Законы России: опыт, анализ, практика. – 2021. – № 3. – С. 3–8.

364. Россинская, Е. Р. Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. – 2024. – Т. 19. – № 3. – С. 20–32.

365. Россинская, Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии / Е. Р. Россинская // Вестник Университета имени О. Е. Кутафина. – 2022. – №2 (90). – С. 29–40.

366. Россинская, Е. Р. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Е. Р. Россинская, Т. А. Сааков // Криминалистика: вчера, сегодня, завтра. – 2020. – №3 (15). – С. 106–123.

367. Россинская, Е. Р. Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа») / Е. Р. Россинская, А. И. Семикаленова // Вестник Томского государственного университета. Право. – 2021. – № 42. – С. 68–80.

368. Россинская, Е. Р. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования / Е. Р. Россинская, И. А. Рядовский // Всероссийский криминологический журнал. – 2020. – Т. 14. – № 5. – С. 699–709.

369. Россинская, Е. Р. Современные способы компьютерных преступлений и закономерности их реализации / Е. Р. Россинская, И. А. Рядовский // Lex Russica. – 2019. – № 3 (148). – С. 87–99.

370. Россинская, Е. Р. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика / Е. Р. Россинская, И. А. Рядовский // Lex Russica (Русский закон). – 2021. – Т. 74. – № 9 (178). – С. 102–118.

371. Рудаков, Б. В. К вопросу о проблемах использования цифровых (электронных) данных в доказывании по уголовным делам / Б. В. Рудаков // Правопорядок: история, теория, практика. – 2021. – № 1 (28). – С. 65–71.

372. Семенов, Н. Н. Проблемы использования компьютерной техники при раскрытии, расследовании преступлений и доказыванию по уголовным делам / Н. Н. Семенов // Тактико-методические особенности расследования преступлений. – Казань. – 2018. – С. 138–145.

373. Скобелин, С. Ю. Цифровая криминалистика: объект и направления развития / С. Ю. Скобелин // Российский следователь. – 2020. – № 4. – С. 42–44.

374. Скоревич, А. С., Кулаевский, А. В. Теоретическое и эмпирическое исследование алгоритмизации тактики проведения коммуникативных следственных действий / А. С. Скоревич, А. В. Кулаевский // Вестник Томского государственного университета. – 2023. – № 490. – С. 206–211.

375. Смушкин, А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений / А. Б. Смушкин // Актуальные проблемы российского права. – 2022. – Т. 17. – № 3 (136). – С. 102–111.

376. Смушкин, А. Б. О возможности вероятностного моделирования поведения лица с помощью цифрового двойника преступника / А. Б. Смушкин // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели. Москва : Издательский центр Университета имени О. Е. Кутафина (МГЮА). – 2025. – С. 144–148.

377. Соя-Серко, Л. А. Программирование и творчество в деятельности следователя / Л. А. Соя-Серко // Проблемы предварительного следствия в уголовном судопроизводстве. – 1980. – № 1 – С. 32–47.

378. Старкова, Л. М. Подходы к пониманию и нормативному определению категории «киберпреступность» и смежных понятий в практике региональных международных организаций / Л. М. Старкова // Московский журнал международного права. – № 4. – С. 123–135.

379. Стяжкина, С. А. Уголовно-правовые особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ) / С. А. Стяжкина // Вестник Удмуртского университета. Серия Экономика и право. – 2021. – Т. 31. – № 3. – С. 489–496.

380. Сысенко, А. Р. Особенности осмотра места происшествия при расследовании компьютерных преступлений / А. Р. Сысенко // Закон и право. – 2020. – № 12. – С. 216–218.

381. Сухов, А. В. Цифровая полиция как эргатическая система, функционирующая в цифровой экосистеме / Конюшев, В. В., Сухов, А. В. // Правовая информатика. – 2021. – № 2. – С. 28–39.

382. Танасевич, В. Г. Теоретические основы методики расследования преступлений / В. Г. Танасевич // Советское государство и право. – 1976. – № 6. – С. 84–95.

383. Тисен, О. Н. Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О. Н. Тисен // Уголовное право. – 2024. – № 3. – С. 69–80.

384. Усов, А. И. Стандарты судебной экспертизы как инструмент цифровизации криминалистики / А. И. Усов // Современные технологии и подходы в юридической науке и образовании : сборник материалов международного научно-практического форума. Калининград : Балтийский федеральный университет имени Иммануила Канта. – 2021. – С. 213–221.

385. Усов, А. И. Судебная компьютерно-техническая экспертиза: становление, развитие, методическое обеспечение / А. И. Усов // Теория и практика судебной экспертизы. – 2008. – № 3 (11). – С. 10–22.

386. Федулова, А. Е. Участие специалиста в производстве следственных действий с электронными носителями информации / А. Е. Федулова // Юридическая наука и правоохранительная практика. – 2023. – № 1 (63). – С. 80–87.

387. Халиков, А. Н. Расследование преступлений в аспекте применения психологических знаний / А. Н. Халиков // Мир криминалистики. – 2023. – № 2.

– С. 93–98.

388. Харисова, З. И. Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» / З. И. Харисова // Вестник Уфимского юридического института МВД России. – 2019. – № 3 (85). – С. 92–98.

389. Харисова, З. И. Алгоритмы действий следователя (дознавателя) на стадии возбуждения уголовного дела о преступлениях в сфере компьютерной информации / З. И. Харисова // Вестник Московского университета МВД России им. Кикотя. – 2025. – № 4. – С. 147–152.

390. Харисова, З. И. Верификация информации при управлении социальными системами / З. И. Харисова, Н. Р. Калимуллин // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2020. – № 6-2. – С. 169–173.

391. Харисова, З. И. Генезис преступности в сфере компьютерной информации и ее детерминанты / З. И. Харисова // Общество, право, государственность: ретроспектива и перспектива. – 2025. – № 1 (21). – С. 57–65.

392. Харисова, З. И. Информационно-компьютерная криминалистическая модель преступления в сфере компьютерной информации на примере неправомерного воздействия на критическую информационную инфраструктуру РФ / З. И. Харисова // Право и государство: теория и практика. – 2025. – № 9. – С. 509–512.

393. Харисова, З. И. Информационно-компьютерная криминалистическая модель преступления, связанного с нарушением правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования сети «Интернет» и сети связи общего пользования: теоретико-прогностический подход / З. И. Харисова // Вестник Института права Башкирского государственного университета. – 2025. – № 2. – С. 205–221.

394. Харисова, З. И. Использование возможностей искусственного интеллекта в области пожарной безопасности / З. И. Харисова, Э. И. Хабибрахманов, С. Г. Аксенов // Человек. Социум. Общество. – 2022. – № 14. – С. 37–42.

395. Харисова, З. И. Криминалистическая кодификация преступлений в сфере компьютерной информации и ее роль в унификации процесса / З. И. Харисова // Вестник Санкт-Петербургского университета МВД России. – 2025. – № 4 (108). – С. 134–142.

396. Харисова, З. И. Концепция глобального нейросетевого криминалистического кластера данных в области противодействия преступлениям в сфере компьютерной информации / З. И. Харисова // Вестник Уфимского юридического института МВД России. – 2025. – № 3 (109). – С. 116–125.

397. Харисова, З. И. Криминалистическая модель нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей / З. И. Харисова // *Философия права*. Ростов-на-Дону. – 2025. – № 2 (113). – С. 180–187.

398. Харисова, З. И. Криминалистическая характеристика незаконного использования, передачи, сбора и хранения компьютерной информации, содержащей персональные данные / З. И. Харисова // *Сибирские уголовно-процессуальные и криминалистические чтения*. – 2025. – № 2. – С. 96–108.

399. Харисова, З. И. Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации / З. И. Харисова // *Правовое государство: теория и практика*. – 2025. – № 2. – С. 96–105.

400. Харисова, З. И. Криминалистическая характеристика создания, использования и распространения вредоносных компьютерных программ / З. И. Харисова // *Вестник Балтийского федерального университета им. И. Канта*. Серия: гуманитарные и общественные науки. – 2025. – № 2. – С. 20–33.

401. Харисова, З. И. Международное сотрудничество в области противодействия экономическим преступлениям с использованием криптовалют / З. И. Харисова // *Организация Объединенных Наций и глобальные проблемы человечества в XXI веке : сборник материалов Международной научно-практической конференции*. – Уфа : Башкирский государственный университет. – 2019. – С. 256–263.

402. Харисова, З. И. О возможности применения инновационных информационных технологий в обеспечении безопасности государства и общества от современных киберугроз / З. И. Харисова, Т. А. Денисова, Я. А. Калашникова // *Актуальные проблемы права и государства*. – 2020. – Т. 12. № 1. – С. 282–287.

403. Харисова, З. И. О возможности проведения практико-ориентированного обучения в рамках реализации дисциплин, связанных с расследованием IT-преступлений / З. И. Харисова // *Современное образование: традиции и инновации : материалы международной научно-методической конференции*. – Волгоград : ВА МВД России, 2023. – С. 103–105.

404. Харисова, З. И. О некоторых проблемах обеспечения информационной безопасности государства и общества от современных киберугроз / З. И. Харисова // *Актуальные проблемы права и государства в XXI веке*. – 2019. – Т. 11. № 1. – С. 387–391.

405. Харисова, З. И. О структурных элементах криминалистической характеристики преступлений в сфере компьютерной информации / З. И. Харисова

// Журнал прикладных исследований. – 2025. – № 9. – С. 199–203.

406. Харисова, З. И. Оптимизация процесса поиска, анализа и интерпретации цифровых доказательств с использованием алгоритмов искусственного интеллекта / З. И. Харисова // Общество, право, государственность: ретроспектива и перспектива. – 2025. – № 3 (23). – С. 60–69.

407. Харисова, З. И. Особенности возбуждения уголовных дел о преступлениях в сфере компьютерной информации / З. И. Харисова // Право и государство: теория и практика. – 2025. – № 9. – С. 501–504.

408. Харисова, З. И. Отдельные инструменты работы с криминалистически значимой информацией / З. И. Харисова, А. Р. Лонщикова // Теория и практика расследования преступлений : материалы Международной научно-практической конференции. – Краснодар : ФГКОУ ВО КрУ МВД России. – 2020. – С. 236–240.

409. Харисова, З. И. Отдельные криминалистические и процессуальные ошибки, допускаемые при подготовке и проведении опознания по делам о насильственных преступлениях / А. Р. Лонщикова, З. И. Харисова, В. В. Антонов // Евразийский юридический журнал. – 2020. – № 6 (145). – С. 361–362.

410. Харисова, З. И. Отдельные проблемы процессуальных решений и тактические ошибки при осуществлении мер безопасности (на примере раскрытия и расследования насильственных преступлений) / З. И. Харисова, А. Р. Лонщикова // Актуальные проблемы деятельности органов внутренних дел по обеспечению безопасности лиц, подлежащих государственной защите : материалы научно-практической конференции. – Уфа : Уфимский ЮИ МВД России. – 2020. – С. 94–97.

411. Харисова, З. И. Право международной безопасности: современное состояние и тенденции развития / З. И. Харисова, О. А. Филиппов // Вестник Института права Башкирского государственного университета. – 2020. – № 1 (5). – С. 46–50.

412. Харисова, З. И. Проблемы и пути совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации / З. И. Харисова // Вестник Уфимского юридического института МВД России. – 2025. – № 2 (108). – С. 116–126.

413. Харисова, З. И. Программные технико-криминалистические средства как основа современной методики расследования преступлений в сфере компьютерной информации / З. И. Харисова // Вестник Института права Башкирского государственного университета. – 2025. – № 3. – С. 237–250.

414. Харисова, З. И. Процессуальные аспекты использования специальных знаний и производства судебных экспертиз по электронным носителям при проверке сообщения о преступлении, совершенном с использованием

информационно-коммуникационных технологий / Э. Д. Нугаева, З. И. Харисова // Информационный бюллетень Следственного департамента МВД России. – 2025. – № 4 (206). – С. 126–143.

415. Харисова, З. И. Отдельные аспекты защиты электронных информационных ресурсов от несанкционированного доступа / З. И. Харисова // Использование современных цифровых технологий в деятельности образовательных организаций силовых ведомств. Актуальные проблемы и тенденции развития : материалы Международной научно-практической конференции. – Уфа : Уфимский ЮИ МВД России. – 2019. – С. 50–53.

416. Харисова, З. И. О возможностях анализа метаданных при расследовании киберпреступлений в программном комплексе «metadox» / З. И. Харисова, Д. И. Аглетдинова, А. С. Ишмеева // Цифровые системы и модели: теория и практика проектирования, разработки и применения : материалы национальной научно-практической конференции. – Казань : Казанский государственный энергетический университет. – 2024. – С. 1396–1400.

417. Харисова, З. И., Об особенностях применения современных технических возможностей при расследовании пожаров / З. И. Харисова, А. И. Сулейманова, С. Г. Аксенов // Государственная служба и кадры. – 2022. – № 2. – С. 231–234.

418. Харисова, З. И. О перспективах перехода органов внутренних дел на отечественное программное обеспечение в рамках импортозамещения / З. И. Харисова, А. А. Катянова // Организация Объединенных Наций и глобальные проблемы человечества в XXI веке : материалы Международной научно-практической конференции. – Уфа : Башкирский государственный университет. – 2019. – С. 250–256.

419. Харисова, З. И. Обеспечение прав и свобод гражданина в области использования цифровых финансовых активов / З. И. Харисова, А. Р. Лонцакова // Евразийский юридический журнал. – 2020. – № 3 (142). – С. 167–168.

420. Харисова, З. И. Обеспечение достоверности и информационной безопасности проведения психофизиологических исследований в рамках уголовного судопроизводства в Российской Федерации и за рубежом / З. И. Харисова, А. Р. Лонцакова, В. В. Антонов // Евразийский юридический журнал. – 2019. – № 9 (136). – С. 240–242.

421. Харисова, З. И., Лонцакова, А. Р. Особенности обеспечения прав и свобод гражданина в области использования цифровых финансовых активов / З. И. Харисова, А. Р. Лонцакова // Современные проблемы уголовного процесса: пути решения : сборник материалов Международной научно-практической конференции. – Уфа : ФГКОУ ВО УЮИ МВД России. – 2020. – С. 201–204.

422. Харисова, З. И. Возможности применения средств видеофиксации с обработкой данных на основе искусственного интеллекта при производстве следственных / З. И. Харисова, Э. Д. Нугаева, А. С. Ишмеева // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2023. – № 9. – С. 81–86.

423. Харисова, З. И. Защита электронных ресурсов от несанкционированного доступа в информационных системах образовательных учреждений / З. И. Харисова, А. Ф. Острякова // Современные цифровые технологии в силовых ведомствах: концепция, практика, инновации : материалы II Международной научно-практической конференции. – Уфа : ФГКОУ ВО УЮИ МВД России. – 2020. – С. 79–81.

424. Харисова, З. И. О возможности использования программного обеспечения при отработке навыков расследования и раскрытия киберпреступлений / З. И. Харисова, А. И. Рафиков // Теория и практика расследования преступлений : материалы X Международной научно-практической конференции. – Краснодар : ФГКОУ ВО КрУ МВД России. – 2022. – С. 548–552.

425. Харисова, З. И. Изъятие криминалистически значимой информации с мобильных средств связи в рамках расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий / З. И. Харисова, Э. Д. Нугаева, О. А. Филиппов // Вестник Института права Башкирского государственного университета. – 2023. – № 1(17). – С. 57–64.

426. Харисова, З. И. Современные угрозы информационной безопасности в условиях глобализации информационного пространства / З. И. Харисова, Р. Р. Файзулова, Д. С. Дюсьмекеева // Актуальные проблемы кибербезопасности в сети Интернет : сборник научных трудов Всероссийской конференции. – Москва : МосУ МВД России им. В.Я. Кикотя. – 2020. – С. 163–165.

427. Харисова, З. И. Искусственный интеллект в государственном управлении / З. И. Харисова, Д. А. Федоров, О. А. Филиппов // Информационные технологии интеллектуальной поддержки принятия решений (ITTDS'2020) : материалы руды VIII Всероссийской научной конференции. – Уфа : Уфимский государственный авиационный технический университет. – 2020. – С. 26–29.

428. Хисамова, З. И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики / З. И. Хисамова // Российский следователь. – 2018. – № 9. – С. 43–47.

429. Чечнев, В. Б. Анализ и классификация многокритериальных методов принятия решений / В. Б. Чечнев // Онтология проектирования. – 2024. – Т.14. – № 4 (54). – С. 607–624.

430. Шабанов, В. Б. Соотношение криминалистической характеристики преступлений со следственными ситуациями, предметом доказывания, версиями и задачами расследования преступления / В. Б. Шабанов, В. Ф. Ермолович // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2012. – № 1 (27). – С. 79–84.

431. Шаталов, А. С. Алгоритмизация и программирование расследования преступлений в системе криминалистической методики / А. С. Шаталов // Право. Журнал Высшей школы экономики. – 2017. – № 2. – С. 155–172.

432. Шигуров, А. В. Новеллы и проблемы правового регулирования порядка проведения следственных действий, связанных с изъятием электронных носителей информации / А. В. Шигуров // Гуманитарные и политико-правовые исследования. – 2021. – № 2 (13). – С. 64–73.

433. Чекунов, И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы / И. Г. Чекунов // Молодые ученые. – 2012. – № 3. – С. 178–186.

434. Яблоков, Н. П. Обстановка совершения преступления как элемент его криминалистической характеристики / Н. П. Яблоков // Криминалистическая характеристика преступления. – М. : Издательство Всесоюзного института по изучению причин и разработке мер предупреждения преступности. – 1984. – С. 34–40.

435. Янгаева, М. О. Актуальные способы неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / М. О. Янгаева, Н. В. Шепель // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2024. – № 4 (68). – С. 180–185.

436. Аналитическая обработка больших массивов данных о событиях кибербезопасности с применением суперкомпьютерных вычислений / И. В. Котенко, И. Б. Саенко, И. Б. Паращук [и др.] // Программные продукты и системы. – 2024. – № 4. – С. 487–494.

437. К вопросу о создании цифровой криминалистической модели для сбора электронных доказательств при расследовании киберпреступлений / У. А. Мусаева, Т. Б. Нгуен, Т. Х. Нгуен [и др.] // Всероссийский криминологический журнал. – 2024. – Т. 18. – № 4. – С. 398–411.

438. Возможности применения средств видеофиксации с обработкой данных на основе искусственного интеллекта при производстве следственных действий / З. И. Харисова, Д. С. Алексеева, В. В. Антонов, А. С. Ишмеева // IV Международная научная конференция по междисциплинарным исследованиям : сборник статей. – Екатеринбург : Институт Цифровой Экономики и Права. – 2023. – С. 374–380.

439. Концепция программно-аналитического комплекса образовательного процесса на основе онтологии и искусственных нейронных сетей / В. В. Антонов,

Г. Г. Куликов, Л. А. Кромина [и др.] // Онтология проектирования. – 2021. – Т. 11. – № 3 (41). – С. 339–350.

440. О применении технических средств при расследовании пожаров / З. И. Харисова, С. Г. Аксенов, Э. И. Хабибрахманов [и др.] // Закон и право. – 2022. – № 8. – С. 221–225.

441. Об алгоритмах расследования пожаров на объектах нефтяной промышленности / З. И. Харисова, С. Г. Аксенов, А. С. Ишмеева [и др.] // Закон и право. – 2022. – № 7. – С. 132–135.

442. Системная модель интеллектуальной предметно-ориентированной профайлинг-системы / В. В. Антонов, З. И. Харисова, З. Р. Мансурова [и др.] // Онтология проектирования. – 2020. – Т. 10. – № 3 (37). – С. 338–350.

443. Теоретико-множественный подход к построению дуальной системной модели ПАК для исследуемой области деятельности со смешанными реальными и виртуальными объектами / З. И. Харисова, Г. Г. Куликов, В. В. Антонов [и др.] // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2020. – Т. 20. – № 1. – С. 5–15.

444. Формализация процесса определения вероятности реализации компьютерных преступлений при их расследовании / М. М. Голембиовский, М. Ю. Рытов, Е. В. Кондрашова // Промышленные АСУ и контроллеры. – 2023. – № 5. – С. 20–28.

445. Adams, T. A. Trends, challenges and opportunities of engaging digital forensics for cybercrime investigation / T. A. Adams // Advances in Multidisciplinary and Scientific Research Journal Publication. – 2024. – V. 15. – № 1. – P. 1–12.

446. Ahmad, S. Machine learning approaches in cybersecurity to enhance security in future network technologies / S. Ahmad, M. Haque // Springer Nature Computer Science. – 2025. – № 6. – P. 301–315.

447. Al-Khater, W. Comprehensive review of cybercrime detection techniques / W. Al-Khater, S. Al-Maadeed, A. Ahmed et al. // IEEE access. – 2020. – V. 8. – P. 137293–137311.

448. Ali, S. Foundation models for the digital twins creation of cyber-physical systems / S. Ali, P. Arcaini, A. Arrieta // Leveraging applications of formal methods, verification and validation. – 2025. – № 15223. – P. 9–26.

449. Amoo, O. The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system / O. Amoo, A. Atadoga, T. Abrahams // World journal of advanced research and reviews. – 2024. – № 21 (02). – P. 205–217.

450. Arevalo-Herrera Assessing SDN controller vulnerabilities: a survey on attack typologies, detection mechanisms, controller selection, and dataset application in machine learning / J. Arevalo-Herrera, J. Camargo, J. Martinez // Wireless personal communications. – 2025. – V. 140. – P. 739–775.

451. Barrenechea, M. M. A systematic literature review on the use of artificial intelligence for cybercrime rate forecasting / M. M. Barrenechea, M. A. Lengua // Bulletin of Electrical Engineering and Informatics. – 2025. – №. 14 (3). – P. 2042–2054.

452. Benington, H. D. Production of large computer programs / H. D. Benington // Annals of the history of computing. – 1983. – V. 5. – № 4. – P. 350–361.

453. Brown, C. Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice / C. Brown // International journal of cyber criminology. – 2015. – № 9 (1). – P. 1–65.

454. Caneppele, S. Observing, measuring, and researching cybercrime: a scoping review of systematic reviews since 2010s / S. Caneppele // Understanding crime trends in a hybrid society. – 2025. – P. 101–123.

455. Cantelli-Forti A. A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence / A. Cantelli-Forti, G. Longo, F. Lupia et al. // International journal of information security. – 2025. – №24 (2). – P. 1–81.

456. Carrington, A. M. Deep ROC analysis and AUC as balanced average accuracy, for improved classifier selection, audit and explanation / A. M. Carrington, D. G. Manuel, P. W. Fieguth // IEEE transactions on pattern analysis and machine intelligence. – 2022. – V. 45. – №. 1. – P. 329–341.

457. Casey, E. The chequered past and risky future of digital forensics / E. Casey // Australian journal of forensic sciences. – 2019. – № 51. – P. 649–664.

458. Chang, W. Knowledge management in cybercrime investigation – a case study of identifying cybercrime investigation knowledge in Taiwan / W. Chang, P. Chung // Pacific-Asia workshop on intelligence and security informatics. – 2014. – № 1. – P. 8–17.

459. Chechulin, A. Cybercrime investigation model / A. Chechulin, M. Gorda // Communication Systems and Networks. – 2024. – № 11. – P. 37–42.

460. Cheong, B. Avatars in the metaverse: potential legal issues and remedies / B. Cheong // International cybersecurity law review. – 2022. – № 3. – P. 467–494.

461. Djenna, A. Artificial intelligence-based malware detection, analysis, and mitigation / A. Djenna, A. Bouridane, S. Rubab et al. // Symmetry. – 2023. – № 15. – P. 677–680.

462. Dunsin, D. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response / D. Dunsin, M. Ghanem,

K. Ouazzane et al. // Forensic science international: digital investigation. – 2024. – № 48. – P. 301675- 301695.

463. Elhoseny, M. Optimal deep learning based convolution neural network for digital forensics face sketch synthesis in internet of things (IoT) / M. Elhoseny, M. Selim, K. Shankar // International journal of machine learning and cybernetics. – 2021. – № 12 (11). – P. 3249–3260.

464. Florido-Benitez, L. The types of hackers and cyberattacks in the aviation industry / L. Florido-Benitez // Journal of Transportation Security. – 2024. – V. 17. – P. 13–32.

465. Gao, C. A survey of graph neural networks for recommender systems: challenges, methods, and directions / C. Gao, Y. Zheng, N. Li // ACM transactions on recommender systems. – 2023. – V. 1. – № 1. – P. 1–51.

466. Garfinkel, S. Anti-forensics: techniques, detection and countermeasures / S. Garfinkel // Warfare and Security. – 2007. – № 20087. – P. 77-84.

467. Gautam, Y. Integrating artificial intelligence into cybercrime investigation: challenges and future directions / Y. Gautam // International journal for multidisciplinary research. – 2024. – V. 6. – № 5. – P. 1–13.

468. Gomathy, C. K. Legal frameworks for regulating cybercrime and cyber terrorism / C. K. Gomathy, P. V. Rajesh, D. S. Manohar, V. Geetha // International journal of scientific research in engineering and management. – 2024. – V. 8. – № 9. – P. 1–7.

469. Gomathy, C. K. Cybercrime in the era of mobile and wireless devices / C. K. Gomathy, V. Geetha, S. T. Ramacharla, A. Vustepalle // International journal of scientific research in engineering and management. – 2024. – V. 8. № 9. – P. 1–4.

470. Hartono, W. Challenges of criminal investigation cybercrime / W. Hartono, D. Muhardi, A. Akhiruddin et al. // Awang long law review. – 2024. – V. 7. – № 1. – P. 11–19.

471. Hashemi, A. AI-generated or AI touch-up. Identifying AI contribution in text data / A. Hashemi, W. Shi, J. Corriveau // International journal of data science and analytics. – 2024. – V. 1. – P. 1–12.

472. Homaei, M., Mogollon-Gutierrez, O., Sancho, J. A review of digital twins and their application in cybersecurity based on artificial intelligence / Homaei, M., Mogollon-Gutierrez, O., Sancho, J. // Artificial Intelligence Review. – 2024. – V. 57. – № 201. – P. 1–65.

473. Hooper, C. Cloud computing and its implications for cybercrime investigations in Australia / C. Hooper, B. Martini, K. Choo // Computer law and security review. – 2013. – № 29 (2). – P. 152–163.

474. Hou, J. A survey on digital forensics in internet of things. / J. Hou, Y. Li, J. Yu et al. // IEEE Internet of things journal. – 2020. – № 7 (1). – P. 1–15.

475. Hunton P. Cybercrime and security: a new model of law enforcement investigation / P. Hunton // Policing: a journal of policy and practice. – 2010. – №. 4. – P. 385-395.

476. Iqbal, F. Mining writeprints from anonymous e-mails for forensic investigation / F. Iqbal, H. Binsalleeh, B. Fung // Digital Investigation. – 2010. – №7. – P. 56–64.

477. Javed, A. R. A comprehensive survey on computer forensics: state-of-the-art, tools, techniques, challenges, and future directions / A. R. Javed, W. Ahmed, M. Alazab // IEEE Access. – 2022. – № 10. – P. 11065–11089.

478. Jenkins, J. Exploring deep convolutional generative adversarial networks (DCGAN) in biometric systems: a survey study / J. Jenkins, K. Roy // Discover artificial intelligence. – 2024. – №. 4 (42). – P. 1–22.

479. Jian, X. Towards a joint semantic analysis in mobile forensics environments / X. Jian, M. Siegel // Digital investigation. – 2025. – № 52. – P. 301846-301868.

480. Karimi, A. Cybercrime detection using semi-supervised neural network / A. Karimi, S. Abbasabadei, J. Torkestani // Computer science journal of Moldova. – 2020. – № 86 (2). – P. 155–183.

481. Kebande, V. R. A UML-Based approach for analysing potential digital forensic evidence / V. R. Kebande, N. M. Karie // International journal of electronic security and digital forensics. – 2018. – № 7 (4). – P. 354–362.

482. Kreso, I. Using blockchain technology for preserving digital evidence in digital forensics / I. Kreso // Knowledge international journal. – 2025. – № 68 (3). – P. 331–336.

483. Leevy, J. Detecting cybersecurity attacks across different network features and learners / J. Leevy, J. Hancock, R. Zuech // Journal of big data. – 2021. – №. 8 (1). – P. 1–29.

484. Li, J. Multi-governance model of new cybercrime under the risk of new technologies risks and responses / J. Li // Lecture notes in education psychology and public media. – 2024. – № 73 (1). – P. 22–29.

485. Liu, G. Graph neural networks embedded with domain knowledge for cyber threat intelligence entity and relationship mining / G. Liu, K. Lu, S. Pi // PeerJ Computer Science. – 2025. – №. 11. – P. 12–29.

486. Lundberg, E. The potential effects of deepfakes on news media and entertainment / E. Lundberg, P. Mozelius // AI & Society. – 2024. – № 1 – P. 1–12.

487. Mahima, A. DeepFake image, video and audio detection / A. Mahima, M. Monica, S. Neha // Computing technologies for sustainable development. Communications in computer and information science. – 2025. – №. 2361. – P. 29–41.

488. Mbaziira, A. An empirical study on detecting deception and cybercrime using artificial neural networks / A. Mbaziira, D. Murphy // Association for computing machinery.

– 2018. – № 1 – P. 42–46.

489. Metwally, W. The role of the data analytics and digital twin for establishing intelligent city / W. Metwally, V. Ibrahim // *Proceedings of the ICSDI*. – 2025. – № 3. – P. 295–305.

490. Modi, P. Using a structured composition of correlation coefficient functions to optimize machine learning-driven cyberattack detection models / P. Modi // *2025 IEEE conference on artificial intelligence*. – 2025. – № 1. – P. 1004–1009.

491. Narayana, Y. Deep neural system for identifying cybercrime activities in networks / Y. Narayana, M. Sreedevi // *Journal of theoretical and applied information technology*. – 2023. – № 101 (6). – P. 6414–6424.

492. Nath, S. Digital evidence chain of custody: navigating new realities of digital forensics / S. Nath, K. Summers, B. Jaejong // *Intelligent systems, and applications*. – 2024. – № 6. – P. 11–20.

493. Nelufule N. Intersection of electronic security and digital forensics: data protecting techniques and uncovering data clues / N. Nelufule, B. Nkwe, D. Shadung et al. // *E-infrastructure and e-services for developing countries*. – 2023. – № 1. – P. 351–367.

494. Nicholls, J. Financial cybercrime: a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape / J. Nicholls, A. Kuppa, N. Le-Khac // *IEEE Access*. – 2021. – № 9. – P. 163965–163986.

495. Nuradiah, R. A comparative analysis of logistic regression and random forest algorithm for cyberattacks classification / R. Nuradiah, A. Sudiarjo, D. Yunautama // *Telecommunication systems, services, and applications*. – 2024. – № 1. – P. 197–204.

496. Pachimatla, D. Advanced algorithms to detect and prevent the spread of manipulated images and videos using deep learning and AI / D. Pachimatla, R. Kilari, I. Ranitha // *Trends in machine learning, IoT, smart cities and applications*. – 2025. – № 1182. – P. 415–427.

497. Pinney, J. Exploring applications and implications of big data predictive analytics in policing cyberspace / J. Pinney, V. Bentotahewa, M. Tomlinson // *Navigating the Intersection of artificial intelligence, security, and ethical governance*. – 2025. – № 1. – P. 1–18.

498. Qin, H. Identity, crimes, and law enforcement in the Metaverse / H. Qin, Y. Wang, P. Hui // *Humanities and social sciences communications*. – 2025. – № 12 (194). – P. 1–15.

499. Radoniewicz, F. Cyberspace, cybercrime, cyberterrorism / F. Radoniewicz // *Cybersecurity in Poland*. – 2024. – № 1. – P.33–51.

500. Ritterbusch, G. D. Defining the metaverse: a systematic literature review / G. D. Ritterbusch, M. R. Teichmann // *Ieee Access*. – 2023. – № 11. – P. 12368–12377.

501. Roberts, A. The importance of OSINT / A. Roberts // Cyber threat intelligence. – 2021. – № 1 – P. 131-152.
502. Ryu, J. H. A blockchain-based decentralized efficient investigation framework for IoT digital forensics / J. H. Ryu, P. K. Sharma, J.H. Jo // The journal of supercomputing. – 2019. – № 75. – P. 4372–4387.
503. Sadegh-Zadeh, S. An unsupervised machine learning approach for cyber threat detection using geographic profiling and domain name system data / S. Sadegh-Zadeh, M. Tajdini // Decision analytics journal. – 2025. – № 1. – P. 100576–100590.
504. Sadovnichiy, V. A. Modeling and forecasting the evolutionary economic development of the BRICS and G7 countries in the first half of the twenty-first century / V. A. Sadovnichiy, A. A. Akaev, O. I. Davydova // Journal of globalization studies. – 2024. – № 15 (2). – P.3–41.
505. Sengupta, A. Ensuring the privacy of digital forensic reports using searchable symmetric encryption / A. Sengupta, P. Kumar, A. Sahani // Advances in digital forensics XX Digital Forensics. – 2025. – №. 724. – P. 25–40.
506. Shamoo, Y. Cybercrime investigation and fraud detection with AI / Y. Shamoo // IGI Global. – 2025. – № 1. – P. 83–114.
507. Shetty, S. Learning Systems in Forgery Image Detection / S. Shetty, D. Ganesh, R. Poojary et al. // Intelligent systems in computing and communication. – 2025. – № 2232. – P. 342–353.
508. Saha, I. Phishing attacks detection using deep learning approach / I. Saha, D. Sarma, R. Chakma et al. // Smart systems and inventive technology, – 2020. – № 1. – P. 1180-1185.
509. Tao, F. Digital twin-driven product design, manufacturing and service with big data / F. Tao, J. Cheng, Q. Qi // International journal of advanced manufacturing technology. – 2018. – № 94. – P. 3563– 3576.
510. Tical, G. M. Artificial intelligence and big data analysis in crime prevention and combat / G. M. Tical // Annals academy of romanian scientists series on military sciences. – №17 (1). – 2025. – P. 36–51.
511. Tiutiunyk, I. Classifying cybercrime networks: organized and transnational schemes in the digital era / I. Tiutiunyk, D. Toptunencko, A. Flaumer // Socio-economic relations in the digital society. – 2024. – № 53. – P. 121–129.
512. Thakur, K. Safeguarding justice employing blockchain-enabled secure chain of custody framework for digital evidence / K. Thakur, R. Ahuja // Innovations in electrical and electronic engineering. – 2024. – № 115. – P. 1–11.
513. Thapaliya, S. Cyber forensic investigation in iot using deep learning based feature fusion in big data / S. Thapaliya, P. Sharm // International journal of wireless

information networks. – 2023. – № 30. – P. 16–29.

514. Tzavara, V. Tracing the evolution of cyber resilience: a historical and conceptual review / V. Tzavara, S. Vassiliadis // *International journal of information security*. – 2024. – V. 23. – P. 1–25.

515. Venkateshwarprasad, K. Efficient prediction of cybercrime breaches using decision tree compared with Naïve Bayes with improved accuracy / Venkateshwarprasad, K. Sashirekha // *AIP conference proceedings*. – 2025. – №3270 (1). – P. 20–65.

516. Vincze, E. A. Challenges in digital forensics. / E. A. Vincze // *Police practice and research*. – 2016. – № 17 (2). – P. 183–194.

517. Vinayakumar, R. Deep learning approach for intelligent intrusion detection system / R. Vinayakumar, M. Alazab, K. Soman et al. // *IEEE Access*. – 2019. – № 7. – P. 41525–41550.

518. Volchetskaya, T. S. Problems of using modern proof technologies in jury trial / T. S. Volchetskaya, I. Yu. Pankina, O. A. Makarova et al. // *Conference proceedings: Vth Khmyrovsky criminalistic readings*. – 2022. – № 1. – P. 68–74.

519. Xiong, J. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption / J. Xiong, L. Shen, Y. Liu // *Scientific reports*. – 2025. – № 15 (3). – P. 1–15.

520. Yaqoob, I. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges / I. Yaqoob, I. Hashem, A. Ahmed // *Future generation computer systems*. – 2019. – № 92. – P. 265–275.

521. Yi, X. Digital rights management scheme based on redactable blockchain and perceptual hash / X. Yi, Y. Zhou, Y. Lin et al. // *Peer-to-peer networking and applications*. – 2023. – № 16. – P. 2630–2648.

522. Wang, H. Feature selection strategies: a comparative analysis of SHAP-value and importance-based methods / H. Wang, Q. Liang, J. Hancock // *Journal of big data*. – 2024. – № 11 (1). – P. 1–16.

523. Zhou, Y. Metacrime and cybercrime: exploring the convergence and divergence in digital criminality / Y. Zhou, M. Tiwari, A. Bernot et al. // *Asian journal of criminology*. – 2024. – № 19. – P. 419–439.

524. Modeling problems legal regulation of the field of artificial intelligence / Z. I. Kharisova, V. V. Antonov, N. R. Kalimullin et al. // *IOP conference series: materials science and engineering*. – 2021. – V. 1069. – № 1. – P. 012002-012009.

525. Model of a domain-specific profiling system based on explainable AI technologies / Z. I. Kharisova, V. V. Antonov, L. E. Rodionova et al. // *IOP conference series: materials science and engineering*. – 2021. – V. 1069. – № 1. – P. 012001-012011.

Диссертации и авторефераты диссертаций

526. Ахмедшин, Р. Л. Криминалистическая характеристика личности преступника : 12.00.09 : дис. ... докт. юрид. наук / Ахмедшин Рамиль Линарович. – Томск, 2006. – 413 с.

527. Балашова, А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : 12.00.09 : дис. ... канд. юрид. наук / Балашова Анна Александровна. – Москва, 2020. – 216 с.

528. Бахтеев, Д. В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений : 5.1.4 : дис. ... докт. юрид. наук / Бахтеев Дмитрий Валерьевич. – Екатеринбург, 2022. – 504 с.

529. Бегишев, И. Р. Уголовно-правовая охрана общественных отношений, связанных с робототехникой : 12.00.08 : дис. ... докт. юрид. наук : 12.00.08 / Бегишев Ильдар Рустамович. – Казань, 2022. – 506 с.

530. Белевский, Р. А. Методика расследования преступлений, связанных с неправомерным доступом к компьютерной информации в сетях ЭВМ : 12.00.09 : дис. ... канд. юрид. наук / Белевский Роман Александрович. – СПб., 2006. – 176с.

531. Бессонов, А. А. Частная теория криминалистической характеристики преступлений : 12.00.12 : дис. ... докт. юрид. наук / Бессонов Алексей Александрович. – Москва, 2017. – 456 с.

532. Буйнов, Д. О. Теория и практика собирания и экспертного исследования цифровых следов по уголовным делам в сфере экономической деятельности : 5.1.4 : дис. ... канд. юрид. наук / Буйнов Дмитрий Олегович. – Москва, 2024. – 229 с.

533. Вехов, В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : 12.00.09 : дисс. ... докт. юрид. наук / Вехов Виталий Борисович. – Волгоград, 2008. – 561 с.

534. Волчецкая, Т. С. Криминалистическая ситуалогия : 12.00.09 : дис. ... докт. юрид. наук / Волчецкая Татьяна Станиславовна. – Москва, 1997. – 395 с.

535. Гаврилин, Ю. В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы : 12.00.09 : дис. ... докт. юрид. наук / Гаврилин Юрий Викторович. – Москва, 2009. – 248 с.

536. Глимейда, В. В. Применение технических средств и цифровых технологий при производстве следственных действий : 5.1.4 : дис. ... канд. юрид. наук / Глимейда Виталий Витальевич. – Москва, 2024. – 241 с.

537. Глоба, В. В. Допустимость использования тактических приемов допроса обвиняемого (подозреваемого) : 5.1.4 : дис. ... канд. юрид. наук / Глоба Валерия Витальевна. – Краснодар, 2025. – 214 с.

538. Голятина, С. М. Методика расследования хищений электронных денежных средств : 12.00.12 : дис. ... канд. юрид. наук / Голятина Светлана Михайловна. – Волгоград, 2022. – 196 с.

539. Гостевский, Д. Ю. Техничко-криминалистическое обеспечение производства следственных действий : 12.00.09 : автореф. дис. ... канд. юрид. наук / Гостевский Денис Юрьевич. – Люберцы, 2010. – 48 с.

540. Давыдов, В. О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей : 12.00.09 : автореф. дис. ... канд. юрид. наук / Давыдов Владимир Олегович. – Тула, 2013. – 29 с.

541. Драпкин, Л. Я. Построение и проверка следственных версий : 12.00.12 : автореф. дис. ... канд. юрид. наук / Драпкин Леонид Яковлевич – Москва, 1972. – 28 с.

542. Дремлюга, Р. И. Интернет-преступность : 12.00.08 : дис. ... канд. юрид. наук / Дремлюга Роман Игоревич. – Владивосток, 2008. – 248 с.

543. Евдокимов, К. Н. Противодействие компьютерной преступности : теория, законодательство, практика : 12.00.08 : дис. ... докт. юрид. наук / Евдокимов Константин Николаевич. – Москва, 2022. – 557 с.

544. Еркенов, С. Е. Взаимодействие правоохранительных органов стран СНГ при раскрытии и расследовании транснациональных преступлений : 12.00.09 : автореф. дис. ... канд. юрид. наук / Еркенов Серик Есжанович. – Москва, 1999. 47 с.

545. Егорышев, А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации : 12.00.09 : дис. ... канд. юрид. наук / Егорышев Александр Сергеевич. – Уфа, 2004. – 230 с.

546. Зигура, Н. А. Компьютерная информация как вид доказательств в уголовном процессе России : 12.00.09 : автореф. дис. ... канд. юрид. наук / Зигура Надежда Анатольевна. – Челябинск, 2010. – 26 с.

547. Зуйков, Г. Г. Криминалистическое учение о способе совершения преступления : дис. ... докт. юрид. наук / Зуйков Георгий Георгиевич. – Москва, 1970. – 220 с.

548. Иванова, И. Г. Выявление и расследование неправомерного доступа к компьютерной информации : 12.00.09 : дис. ... канд. юрид. наук / Иванова Инна Геннадьевна. – Красноярск, 2007. – 197 с.

549. Игнатьев, М. Е. Криминалистическая теория и практика установления причинно-следственных связей в расследовании преступлений : 12.00.12 : автореф.

дис. ... докт. юрид. наук / Игнатъев Михаил Евгеньевич. – Рост.-на-Дону, 2020. – 53 с.

550. Калюжный, А. Н. Общая методика расследования преступлений против свободы личности : 12.00.1 : автореф. дис. ... докт. юрид. наук / Калюжный Александр Николаевич. – Орел, 2022. – 54 с.

551. Касаткин, А. В. Тактика собирания и использования компьютерной информации при расследовании преступлений : 12.00.09 : дис. ... канд. юрид. наук / Касаткин Андрей Валерьевич. – Москва, 1997. – 215 с.

552. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : 12.00.12 : автореф. дис. ... канд. юрид. наук / Коломинов Вячеслав Валентинович. – Краснодар, 2017. – 25 с.

553. Коробко, А. В. Технология информационно-аналитической поддержки принятия решений на основе федерализации разнородной информации в концепции многомерного представления данных : 2.3.8 : дис. ... докт. техн. наук / Коробко Анна Владимировна. – Красноярск, 2024. – 250 с.

554. Косынкин, А. А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации : 12.00.09 : автореф. дис. ... канд. юрид. наук / Косынкин Александр Александрович. – Саратов, 2012. – 23 с.

555. Кравец, Е. Г. Информационно-коммуникационные технологии как элемент технико-криминалистического обеспечения расследования преступлений : 12.00.12 : дис. ... канд. юрид. наук / Кравец Евгений Григорьевич. – Волгоград, 2016. – 208 с.

556. Краснова, Л. Б. Компьютерные объекты в уголовном процессе и криминалистике : 12.00.09 : автореф. дис. ... канд. юрид. наук / Краснова Людмила Борисовна. – Воронеж, 2005. – 28 с.

557. Крыгин, С. В. Расследование преступлений, совершаемых в сфере компьютерной информации : 12.00.09 : дис. ... канд. юрид. наук / Крыгин Сергей Владимирович. – Нижний Новгород, 2002. – 200 с.

558. Лихачев, Н. А. Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и доктринальный аспекты : 5.1.4 : дис. ... канд. юрид. наук / Лихачев Никита Александрович. – Краснодар, 2024. – 237 с.

559. Малыгин, И. И. Уголовно-правовое противодействие неправомерному воздействию на критическую информационную инфраструктуру : 5.1.4 : дис. ... канд. юрид. наук / Малыгин Иван Игоревич. – Москва, 2023. – 196 с.

560. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации : 12.00.09 : дис. ... докт. юрид. наук / Мещеряков Владимир Алексеевич. – Воронеж, 2001. – 387 с.

561. Нарижный, А. В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий : 12.00.09 : автореф. дис. ... канд. юрид. наук / Нарижный Александр Викторович. – Краснодар, 2009. – 21 с.

562. Остроушко, А. В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации : 12.00.09 : дис. ... канд. юрид. наук / Остроушко Александр Владимирович. – Волгоград, 2000. – 231 с.

563. Охлупина, А. Н. Теоретические, методические и организационно-тактические основы применения интеллектуальных систем в судебно-почерковедческом исследовании подписей : 12.00.12 : дис. ... канд. юрид. наук / Охлупина Анастасия Николаевна. – Москва, 2019. – 192 с.

564. Пантюхин, И. С. Методика и методы обеспечения аудита средств вычислительной техники для расследования компьютерных инцидентов : 2.3.6 : дис. ... канд. техн. наук / Пантюхин Игорь Сергеевич. – Санкт-Петербург, 2023. – 143 с.

565. Рассолов, И. М. Право и интернет: теоретические проблемы : 12.00.14 : дис. ... докт. юрид. наук / Рассолов Илья Михайлович. – Москва, 2008. – 357 с.

566. Россинская, Е. Р. Концептуальные основы теории неразрушающих методов исследования вещественных доказательств : 12.00.09 : автореф. дис. ... докт. юрид. наук / Россинская Елена Рафаиловна. – Москва, 1993. – 32 с.

567. Рудых, А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : 12.00.12 : автореф. дис. ... канд. юрид. наук / Рудых Алексей Александрович. – Ростов-на-Дону, 2020. – 25 с.

568. Семикаленова, А. И. Судебная программно-компьютерная экспертиза по уголовным делам : 12.00.09 : дис. ... канд. юрид. наук / Семикаленова Анастасия Игоревна. – Москва, 2005. – 228 с.

569. Соколов, Ю. Н. Информационные технологии и оборот цифровых данных в криминалистике : вопросы теории и практики : 5.1.4 : автореф. дис. ... докт. юрид. наук / Соколов Юрий Николаевич. – Екатеринбург, 2023. – 44 с.

570. Соловьев, Л. Н. Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ : 12.00.09 : дис. ... канд. юрид. наук / Соловьев Леонид Николаевич. – Москва, 2003. – 275 с.

571. Соколов, Ю. Н. Информационные технологии и оборот цифровых данных в криминалистике: вопросы теории и практики : 5.1.4 : дис. ... докт. юрид. наук / Соколов Юрий Николаевич. – Краснодар, 2023. – 440 с.

572. Старостенко, Н. И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-

телекоммуникационных технологий : 5.1.4 : автореф. дис. ... канд. юрид. наук / Старостенко Нина Игоревна. – Краснодар, 2023. – 30 с.

573. Усов, А. И. Концептуальные основы судебной компьютерно-технической экспертизы : 12.00.09 : дис. ... докт. юрид. наук / Усов Александр Иванович. – Москва, 2002. – 402 с.

574. Харина, Е. А. Особенности методики расследования мошенничества в сфере компьютерной информации : 5.1.4 : автореф. дис. ... канд. юрид. наук / Харина Елена Алексеевна. – Краснодар, 2023. – 33 с.

575. Хомколов, В. П. Организационно-правовые аспекты расследования и предупреждения преступлений в сфере компьютерной информации : 12.00.09 : дис. ... канд. юрид. наук / Хомколов Виктор Петрович. – Иркутск, 2004. – 184 с.

576. Чекунов, И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : 12.00.08 : дис. ... канд. юрид. наук / Чекунов Игорь Геннадьевич. – Москва, 2013. – 223 с.

577. Шавалеев, Б. Э. Мошенничество с использованием электронных средств платежа: уголовно-правовой и криминологический аспекты : 5.1.4 : дис. ... канд. юрид. наук / Шавалеев Булат Эдуардович. – Казань, 2023. – 222 с.

578. Шаевич, А. А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений : 12.00.09 : автореф. дис. ... канд. юрид. наук / Шаевич Антон Александрович. – Иркутск, 2007. – 24 с.

579. Шарипов, Р. Р. Экспертиза подлинности документов на основе компьютерных методов обработки информации : 05.13.01 : автореф. дис. ... техн. юрид. наук / Шарипов, Руслан Радикович. – Волгоград, 2011. – 21 с.

580. Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступлений : 12.00.12 : автореф. дис. ... канд. юрид. наук / Шевченко Елизавета Сергеевна. – Москва, 2016. – 29 с.

581. Шипулин, Г. Ф. Предупреждение преступлений, совершаемых с использованием компьютерных сетей : 5.1.4 : дис. ... канд. юрид. наук / Шипулин Георгий Фаризович. – Москва, 2024. – 201 с.

582. Эксархопуло, А. А. Криминалистическая теория: формирование и перспективы развития в условиях научно-технического прогресса : 12.00.09 : дис. ... докт. юрид. наук / Эксархопуло Алексей Алексеевич. – СПб, 1993. – 263 с.

583. Яковенко, И. Н. Современное состояние и перспективы использования информационных технологий в раскрытии и расследовании преступлений : 12.00.09 : дис. ... канд. юрид. наук / Яковенко Игорь Николаевич. – Краснодар, 2005. – 228 с.

Интернет-ресурсы

584. Аналитический обзор «Инструменты противодействия кибермошенничеству: анализ системы вывода денежных средств, похищенных у граждан». – Текст : электронный // ПАО Сбербанк : офиц. сайт. – URL: https://www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhn_y_h_sredstv (дата обращения: 27.05.2025).

585. Аналитический отчет «Кибератаки на финансовый сектор в 2024 году». – Текст : электронный // Акционерное общество «Солар секьюрити» : офиц. сайт. – URL: <https://rt-solar.ru/analytics/reports/5206> (дата обращения: 28.03.2025).

586. Аналитический отчет «Прогноз кибербезопасности Google Cloud 2024». – Текст : электронный // Транснациональная корпорация «Google LLC» : офиц. сайт. – URL: <https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf> (дата обращения: 08.02.2025).

587. Аналитический отчет «Отчет по кибербезопасности Check Point 2024». – Текст : электронный // Компания с ограниченной ответственностью «Check Point Software Technologies Ltd» : офиц. сайт. – URL: <https://www.checkpoint.com/resources/report-3854/2024-cyber-security-report> (дата обращения: 08.02.2025).

588. Аналитический отчет «Техники и тактики киберпреступников». – Текст : электронный // ООО «Солар секьюрити» : офиц. сайт. – URL: <https://rt-solar.ru/analytics/reports> (дата обращения: 22.10.2025).

589. База данных угроз безопасности информации «Mitre Att&ck». – Текст : электронный // Некоммерческая организация «Mitre» : офиц. сайт. – URL: <https://attack.mitre.org> (дата обращения: 28.10.2025).

590. Банк данных угроз безопасности информации. – Текст : электронный // ГНИИИ ПТЗИ ФСТЭК России : офиц. сайт. – URL: <https://bdu.fstec.ru/threat> (дата обращения: 31.01.2025).

591. Библиографическая база данных Google Scholar (Академия Google). – Текст : электронный // Академия Google : офиц. сайт. – URL: <https://scholar.google.com> (дата обращения: 27.05.2025).

592. Европейский центр по борьбе с киберпреступностью. – Текст : электронный // ЕСЗ полицейская служба Европейского союза (Европол) : офиц. сайт. – URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (дата обращения: 11.01.2025).

593. Всестороннее исследование проблемы киберпреступности. – Текст : электронный // Управление Организации Объединенных Наций по наркотикам и преступлениям : офиц. сайт. – URL: <https://www.unodc.org/documents/organized->

crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 08.02.2025).

594. Выборочное федеральное статистическое наблюдение по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей. – Текст : электронный // Федеральная служба государственной статистики : офиц. сайт. – URL: https://rosstat.gov.ru/free_doc/new_site/business/it/ikt23/index.html (дата обращения: 08.02.2025).

595. Глобальный атлас регулирования искусственного интеллекта. – Текст : электронный // ООО «Сбер Бизнес Софт» : офиц. сайт. – URL: <https://ai.sber.ru/book> (дата обращения: 08.02.2025).

596. Глобальное число пользователей сети «Интернет». – Текст : электронный // Международный союз электросвязи МСЭ (ITU): офиц. сайт. – URL: <https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use> (дата обращения: 08.02.2025).

597. Глобальный отчет по цифровым технологиям по состоянию на октябрь 2024 года. – Текст : электронный // Международный статистический сервис «Datareportal» : офиц. сайт. – URL: <https://datareportal.com/reports/digital-2024-october-global-statshot> (дата обращения: 08.02.2025).

598. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. – Текст : электронный // Национальный координационный центр по компьютерным инцидентам : офиц. сайт. – URL: <https://gossopka.ru> (дата обращения 07.05.2025).

599. Дропперы: связующее звено преступной цепи. – Текст : электронный // Национальный исследовательский университет «Высшая школа экономики» : офиц. сайт. – URL: <https://daily.hse.ru/post/zizn-dropper-a-pomenyat-krossovki-na-svobodu> (дата обращения: 07.05.2025).

600. Единая государственная платформа по противодействию мошенничеству «ТелекомЦерт». – Текст : электронный // Автономная некоммерческая организация «Информационно-аналитический центр стратегии использования радиочастотного спектра» : офиц. сайт. – URL: <https://rspectr.com/novosti/golosa-moshennikov-soberut-v-biometricheskoj-baze> (дата обращения: 04.04.2025).

601. Ежемесячный отчет Центра мониторинга и управления сетью связи общего пользования. – Текст : электронный // Федеральное государственное унитарное предприятие «Главный радиочастотный центр» : офиц. сайт. – URL: https://portal.nsc.gov.ru/documents/235/Публичный_отчет_декабрь_2024_итог_.pdf (дата обращения: 22.03.2025).

602. Информационно-аналитический отчет «Риски безопасности генеративного искусственного интеллекта». – Текст : электронный // Министерство цифрового

развития, связи и массовых коммуникаций Российской Федерации. ФГБУ «Научно-исследовательский институт «Интеграл» : офиц. сайт. – URL: <https://digital.gov.ru/ru/ministry/departments/46> (дата обращения: 08.02.2025).

603. Информационно-аналитический отчет «Результаты работы информационной системы «Антифишинг». – Текст : электронный // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. ФГБУ «Научно-исследовательский институт «Интеграл» : офиц. сайт. – URL: <https://digital.gov.ru/ru/ministry/departments/46> (дата обращения: 08.02.2025).

604. Индустрия 5.0 : на пути к устойчивой, ориентированной на человека парадигме. – Текст : электронный // Европейский союз : офиц. сайт. – URL: <https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1> (дата обращения: 27.05.2025).

605. Информационная кампания «Подумай дважды» по повышению осведомленности граждан о растущих киберугрозах «Think Twice before falling victim to online scams». – Текст : электронный // Международная организация уголовной полиции (Интерпол) : офиц. сайт. – URL: <https://www.interpol.int/news-and-events/news/2024/interpol-campaign-warns-against-cyber-and-financial-crimes> (дата обращения: 31.01.2025).

606. Кибербезопасность и новые технологии. Руководство для персонала оперативного реагирования по изъятию цифровых устройств. – Текст : электронный // Контртеррористическое управление Организации Объединенных Наций : офиц. сайт. – URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/guide_for_first_responders_on_the_collection_of_digital_devices_in_the_battlefield_final_out_web_ru.pdf (дата обращения: 08.02.2025).

607. Кибермошенничество: портрет пострадавшего. – Текст : электронный // Центральный банк Российской Федерации (Банк России) : офиц. сайт. – URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024 (дата обращения: 28.03.2025).

608. Классификация и типы вредоносного программного обеспечения. – Текст : электронный // Акционерное общество «Лаборатория Касперского» : офиц. сайт. – URL: <https://www.kaspersky.ru/resource-center/threats/malware-classifications> (дата обращения: 22.10.2025).

609. Координационный центр по киберпреступлениям «Indian Cybercrime Coordination Centre I4C». – Текст : электронный // Центр Министерства внутренних дел правительства Индии : офиц. сайт. – URL: <https://i4c.mha.gov.in> (дата обращения: 07.05.2025).

610. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2021 года. – Текст : электронный // Министерство внутренних дел Российской Федерации : офиц. сайт. – URL: <https://media.mvd.ru/files/application/2315310> (дата обращения: 22.10.2025).

611. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2024 года. – Текст : электронный // Министерство внутренних дел Российской Федерации : офиц. сайт. – URL: <https://media.mvd.ru/files/application/9209203> (дата обращения: 22.01.2025).

612. Метавселенная, особенности внедрения: аналитический отчет. – Текст : электронный // Компания Gartner Inc : офиц. сайт. – URL: <https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026> (дата обращения: 22.10.2025).

613. Метавселенная: взгляд правоохранительных органов «Metaverse – A law enforcement perspective: white paper». – Текст : электронный // Международная организация уголовной полиции (Интерпол) : офиц. сайт. – URL: <https://www.interpol.int/content/download/20828/file/Metaverse%20-> (дата обращения: 11.01.2025).

614. Методические рекомендации по организационной защите физическим лицом своих персональных данных. – Текст : электронный // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций : офиц. сайт. – URL: https://rkn.gov.ru/docs/MR_itog.docx (дата обращения: 02.02.2025).

615. Методические рекомендации по разработке плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации. – Текст : электронный // Национальный координационный центр по компьютерным инцидентам – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : офиц. сайт. – URL: <https://gossopka.ru/upload/iblock/a9f/3va55amvsxqelhuo1oufo9y6998nbtwzmetodicheskie-rekomendatsii-po-razrabotke-plana-reagirovaniya.pdf> (дата обращения: 31.01.2025).

616. Мониторинг развития информационного общества в Российской Федерации. – Текст : электронный // Федеральная служба государственной статистики : офиц. сайт. – URL: <https://rosstat.gov.ru/storage/mediabank/monitor.xlsx> (дата обращения: 08.02.2025).

617. Набор добровольных руководящих принципов кибербезопасности Национального института стандартов и технологий «NIST». – Текст : электронный // Национальный институт стандартов и технологий NIST : офиц. сайт. – URL:

<https://www.nist.gov/cyberframework> (дата обращения: 31.01.2025).

618. Национальный центр по борьбе с мошенничеством и киберпреступностью Action Fraud. – Текст : электронный // Центр «Action Fraud» Великобритании : офиц. сайт. – URL: <https://www.actionfraud.police.uk> (дата обращения: 07.05.2025).

619. О вводе в эксплуатацию интеллектуального чат-бота AI на горячую линию по принятию заявлений о киберпреступности. – Текст : электронный // Портал «Indiatimes»: офиц. сайт. – URL: https://timesofindia.indiatimes.com/city/hyderabad/telangana-adds-ai-chatbot-to-cybercrime-helpline-193q-to-speed-up-help-in-golden-hour/articleshow/120939276.cms?utm_source=chatgpt.coir (дата обращения: 07.05.2025).

620. О возможности подачи заявления о киберпреступлении через портал «Госуслуги». – Текст : электронный // Акционерное общество Интерфакс : офиц. сайт. – URL: <https://www.interfax.ru/russia/1021371> (дата обращения: 07.05.2025).

621. О порядке получения объяснений: разъяснения прокуратуры Саратовской области. – Текст : электронный // Генеральная прокуратура Российской Федерации : офиц. сайт. – URL: https://epp.genproc.gov.ru/web/proc_64/activity/legal-education/explain?item=67698817 (дата обращения: 07.05.2025).

622. О раскрываемости преступлений со взломом аккаунтов. – Текст : электронный // Информационное телеграфное агентство России (ИТАР-ТАСС) : офиц. сайт. – URL: <https://tass.ru/obschestvo/24104331> (дата обращения: 07.05.2025).

623. Обзор набора данных «Forensic Toolkit Dataset». – Текст : электронный // Платформа коллективной разработки моделей, наборов данных и приложений в сфере машинного обучения компании «Hugging Face» : офиц. сайт. – URL: https://huggingface.co/datasets/darkknight25/forensic_toolkit_dataset (дата обращения: 08.08.2025).

624. Обзор набора данных «Kali linux toolkit dataset». – Текст : электронный // Платформа коллективной разработки моделей, наборов данных и приложений в сфере машинного обучения компании «Hugging Face» : офиц. сайт. – URL: https://huggingface.co/datasets/darkknight25/kali_linux_toolkit_dataset (дата обращения: 08.08.2025).

625. Обзор набора данных «Modern cyber threat simulation dataset». – Текст : электронный // Платформа коллективной разработки моделей, наборов данных и приложений в сфере машинного обучения компании «Hugging Face» : офиц. сайт. – URL: https://huggingface.co/datasets/darkknight25/modern_cyber_threat_simulation_Dataset (дата обращения: 08.08.2025).

626. Общие проблемы киберпреступности: аналитический отчет за 2024 год. – Текст : электронный // Агентство Европейского союза по сотрудничеству в области правоохранительной деятельности (Евроюст) : офиц. сайт. – URL: <https://www.eurojust.europa.eu/publication/common-challenges-cybercrime> (дата обращения: 31.01.2025).

627. Окинавская хартия Глобального информационного общества. – Текст : электронный // Президент Российской Федерации : офиц. сайт : офиц. сайт. – URL: <http://www.kremlin.ru/supplement/3170> (дата обращения: 22.10.2025).

628. Отчет о преступности в сети «Интернет» : аналитический обзор Центра приема сообщений о преступлениях в сети «Интернет». – Текст : электронный // Центр IC3 Федерального бюро расследований США : офиц. сайт. – URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (дата обращения: 07.05.2025).

629. Понимание киберпреступности: явления, проблемы и правовой ответ. – Текст : электронный // Международный союз электросвязи МСЭ (ITU) : офиц. сайт. – URL: <https://www.itu.int/en/itu-d/Cybersecurity/Documents/cybercrime2014.pdf> (дата обращения: 08.02.2025).

630. Практическое руководство по истребованию электронных доказательств. – Текст : электронный // Управление Организации Объединенных Наций по наркотикам и преступлениям, УНП ООН : офиц. сайт. – URL: <https://sherloc.unodc.org/cld/ru/st/evidence/electronic-evidence.html> (дата обращения: 08.02.2025).

631. Программное обеспечение «Мобильный Криминалист Эксперт Плюс». – Текст : электронный // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации : офиц. сайт. – URL: https://reestr.digital.gov.ru/reestr/423110/?sphrase_id=5937674 (дата обращения: 07.04.2025).

632. Программное обеспечение «Elcomsoft Premium Forensic Bundle». – Текст : электронный // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации : офиц. сайт. – URL: https://reestr.digital.gov.ru/reestr/436808/?sphrase_id=5929589 (дата обращения: 07.04.2025).

633. Программное обеспечение «PC-3000 Portable». – Текст : электронный // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации URL: https://reestr.digital.gov.ru/reestr/310277/?sphrase_id=5929598 (дата обращения: 07.04.2025).

634. Программное обеспечение «Поисковая система SEUS». – Текст : электронный // Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации : офиц. сайт. – URL: https://reestr.digital.gov.ru/reestr/305124/?sphrase_id=5929711 (дата обращения: 07.04.2025).

635. Рамочная конвенция об искусственном интеллекте, правах человека, демократии и верховенстве права. – Текст : электронный // Совет Европы : офиц. сайт. – URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225> (дата обращения: 11.01.2025).

636. Регламент взаимодействия Национального координационного центра по компьютерным инцидентам и владельцев информационных ресурсов Российской Федерации при информировании ФСБ России о компьютерных инцидентах, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак. – Текст : электронный // Национальный координационный центр по компьютерным инцидентам : офиц. сайт. – URL: <https://www.cert.gov.ru/materialy/organizatsiya-vzaimodeystviya/reglament-vzaimodeystviya-nktski-i-vladeltsev-informatsionnykh-resurov-rossiyskoy-federatsii-pri-in> (дата обращения: 31.01.2025).

637. Руководство по разработке национальной стратегии кибербезопасности» Международного союза электросвязи ITU. – Текст : электронный // Международный союз электросвязи МСЭ (ITU) : офиц. сайт. – URL: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-cyb_guide.01-2018-pdf-e.pdf (дата обращения: 08.02.2025).

638. Сервис проверки данных на предмет скомпрометированности. – Текст : электронный // Национальный координационный центр по компьютерным инцидентам Федеральной службы государственной статистики : офиц. сайт. – URL: <https://chk.safe-surf.ru> (дата обращения 30.03.2025).

639. Стандарт наименования уязвимостей информационной безопасности «Common Vulnerabilities and Exposures – CVE». – Текст : электронный // Некоммерческая организация «Mitre» : офиц. сайт. – URL: <https://msm.mitre.org/docs/cve-intro-handout.pdf> (дата обращения: 31.01.2025).

640. Тренды киберугроз будущего. – Текст : электронный // Акционерное общество «Лаборатория Касперского» : офиц. сайт. – URL: <https://www.kaspersky.ru/blog/cyberthreats-and-trends-predictions-in-2025/38852> (дата обращения: 11.01.2025).

641. Цели в области устойчивого развития (sustainable development goals). – Текст : электронный // Организация объединенных наций : офиц. сайт. – URL: <https://www.un.org/sustainabledevelopment/ru/sustainable-development-goals> (дата обращения: 08.02.2025).

642. Центр кибербезопасности Australian Cyber Security Centre. – Текст : электронный // Центр ACSC Австралии : офиц. сайт. – URL: <https://www.cyber.gov.au/acsc/report> (дата обращения: 07.05.2025).

643. Центр приема сообщений о преступлениях в сети «Интернет» Internet crime complaint center (IC3). – Текст : электронный // Федеральное бюро расследований

США : офиц. сайт. – URL: <https://www.ic3.gov> (дата обращения: 07.05.2025).

644. Центр приема сообщений о преступлениях Европейского центра по борьбе с киберпреступностью. – Текст : электронный // Центр ЕСЗ полицейской службы Европейского союза (Европол) : офиц. сайт. – URL: <https://www.europol.europa.eu/report-a-crime> (дата обращения: 07.05.2025).

645. Энциклопедия «Касперского»: глоссарий «Антифрод-системы». – Текст : электронный // Акционерное общество «Лаборатория Касперского» : офиц. сайт. – URL: <https://encyclopedia.kaspersky.ru/glossary/antifraud/> (дата обращения: 11.01.2025).

646. Toolkit for handling and admissibility of electronic evidence empowering legal practitioners to critically. Review electronic evidence from the procedural rights perspective. – Текст : электронный // Научно-исследовательский центр «ZRS Koper»: офиц. сайт. – URL: https://www.zrs-kp.si/wp-content/uploads/2024/07/innocent_monografija_online_edition.pdf (дата обращения: 07.04.2025).

647. Guidelines for digital forensics first responders. Best practices for search and seizure of electronic and digital evidence. – Текст : электронный // Международная организация уголовной полиции (Интерпол) : офиц. сайт. – URL: <https://www.interpol.int/content/download/16243/file/Guideline> (дата обращения: 07.04.2025).

648. National cybercrime strategy : guidebook. – Текст : электронный // Международная организация уголовной полиции (Интерпол) : офиц. сайт. – URL: https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf (дата обращения: 11.01.2025).

649. Recommendation of the council on artificial intelligence. – Текст : электронный // Организация экономического сотрудничества и развития : офиц. сайт. – URL: <https://legalinstruments.oecd.org> (дата обращения: 12.03.2025).

650. Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence. – Текст : электронный // Портал законодательства Европейского союза : офиц. сайт. – URL: <https://eur-lex.europa.eu/legal-content> (дата обращения: 12.03.2025).

Свидетельства о государственной регистрации программы для ЭВМ

651. Свидетельство о государственной регистрации программы для ЭВМ № 2020610510 Российская Федерация. Базис – базовый анализ защищенности информационных систем : № 2019666679 : заявл. 17.12.2019 : опубл. 15.01.2020 / З. И. Харисова.

652. Свидетельство о государственной регистрации программы для ЭВМ № 2020661720 Российская Федерация. Программно-аналитический комплекс «Киберпреступность» : № 2020660996 : заявл. 23.09.2020 : опубл. 30.09.2020

/ З. И. Харисова, А. Р. Лонцакова.

653. Свидетельство о государственной регистрации программы для ЭВМ № 2021665929 Российская Федерация. Алгоритмический комплекс процессуальных действий при дистанционном мошенничестве «АКПД Дистант» : № 2021662179 : заявл. 29.07.2021 : опубл. 05.10.2021 / З. И. Харисова, Э. Д. Нугаева, В. В. Антонов.

654. Свидетельство о государственной регистрации программы для ЭВМ № 2022660543 Российская Федерация. Fire process – расследование пожаров : № 2022619900 : заявл. 27.05.2022 : опубл. 06.06.2022 / З. И. Харисова, С. Г. Аксенов, Ф. К. Синагатуллин [и др.].

655. Свидетельство о государственной регистрации программы для ЭВМ № 2022661783 Российская Федерация. Оптимизация базы данных на основе символьного анализа : № 2022660010 : заявл. 01.06.2022 : опубл. 27.06.2022 / З. И. Харисова, А. И. Рафиков, В. В. Антонов.

656. Свидетельство о государственной регистрации программы для ЭВМ № 2022611631 Российская Федерация. Система мониторинга киберинцидентов Local SIEM : № 2022610610 : заявл. 19.01.2022 : опубл. 28.01.2022 / З. И. Харисова, В. В. Антонов, А. И. Рафиков.

657. Свидетельство о государственной регистрации программы для ЭВМ № 2022619449 Российская Федерация. Программа для разработки процессуальных документов при расследовании пожаров – Fire Investigation : № 2022612480 : заявл. 22.02.2022 : опубл. 23.05.2022 / З. И. Харисова, С. Г. Аксенов, Ф. К. Синагатуллин.

658. Свидетельство о государственной регистрации программы для ЭВМ № 2022611631 Российская Федерация. Система мониторинга киберинцидентов local SIEM : № 2022610610 : заявл. 19.01.2022 : опубл. 28.01.2022 / З. И. Харисова, В. В. Антонов, А. И. Рафиков.

659. Свидетельство о государственной регистрации программы для ЭВМ № 2023667481 Российская Федерация. BioScan – Интеллектуальная система распознавания биометрических данных на основе машинного обучения (ML), компьютерного зрения (CV) и искусственного интеллекта (AI) : № 2023666662 : заявл. 08.08.2023 : опубл. 15.08.2023 / З. И. Харисова, Э. Д. Нугаева.

660. Свидетельство о государственной регистрации программы для ЭВМ № 2023667143 Российская Федерация. Тактика производства отдельных видов осмотра при расследовании преступлений, совершенных с использованием информационных технологий : № 2023666488 : заявл. 04.08.2023 : опубл. 10.08.2023 / З. И. Харисова, Э. Д. Нугаева, В. В. Антонов.

661. Свидетельство о государственной регистрации программы для ЭВМ № 2024661188 Российская Федерация. Blockchain analytics [Аналитика блокчейна] расследование преступлений, связанных с использованием криптовалют и сети блокчейн : № 2024619990 : заявл. 06.05.2024 : опубл. 16.05.2024 / З. И. Харисова, Э. Д. Нугаева, А. С. Ишмеева.

662. Свидетельство о государственной регистрации программы для ЭВМ № 2024661082 Российская Федерация. Macdev V.1.0 [mobile and Computer devices inspection] – производство осмотра компьютерной техники и мобильных устройств при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий : № 2024619987 : заявл. 06.05.2024 : опубл. 15.05.2024 / З. И. Харисова, Э. Д. Нугаева, В. В. Антонов.

663. Свидетельство о государственной регистрации программы для ЭВМ № 2024610017. Программа обнаружения угроз безопасности моделей искусственного интеллекта, использующихся в интеллектуальных системах поддержки принятия решения автоматизированных систем управления : № 2023684809 : заявл. 20.11.2023 : опубл. 09.01.2024 / Н. А. Васильев, В. Е. Садовников, О. С. Лаута [и др.].

664. Свидетельство о государственной регистрации программы для ЭВМ № 2025682275 Российская Федерация. «Blockchain & CFA analytics [Аналитика блокчейна и ЦФА] – Расследование преступлений, связанных с использованием цифровых финансовых активов и сети блокчейн : № 2025680132 : заявл. 31.07.2025 : опубл. 22.08.2025 / З. И. Харисова, Э. Д. Нугаева, И. Х. Еркеев.

665. Свидетельство о государственной регистрации программы для ЭВМ № 2025682276 Российская Федерация. MacDEV TechView [Осмотр технических средств] – Производство осмотра компьютерной техники и мобильных устройств при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий : № 2025680135 : заявл. 31.07.2025 : опубл. 22.08.2025 / З. И. Харисова, Э. Д. Нугаева.

666. Свидетельство о государственной регистрации программы для ЭВМ № 2025680704 Российская Федерация. Cybercrime DT Model (AI) [Цифровой двойник киберпреступления] – цифровая криминалистическая модель преступления в сфере компьютерной информации : № 2025669600 : заявл. 31.07.2025 : опубл. 07.08.2025 / З. И. Харисова.

667. Свидетельство о государственной регистрации программы для ЭВМ № 2025682277 Российская Федерация. CyberCodex [КиберКодекс] – Программное технико-криминалистическое средство «Киберпреступность» с кодификатором преступлений в сфере компьютерной информации: № 2025680136 : заявл. 31.07.2025 : опубл. 22.08.2025 / З. И. Харисова, И. А. Макаренко.

ПРИЛОЖЕНИЯ

Приложение 1

«Обобщенные данные по результатам опроса сотрудников органов дознания, следствия и оперативных подразделений (с указанием результатов опроса 560 человек)»

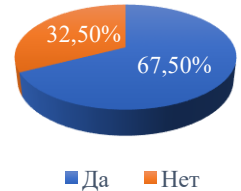
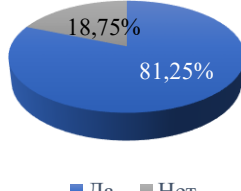
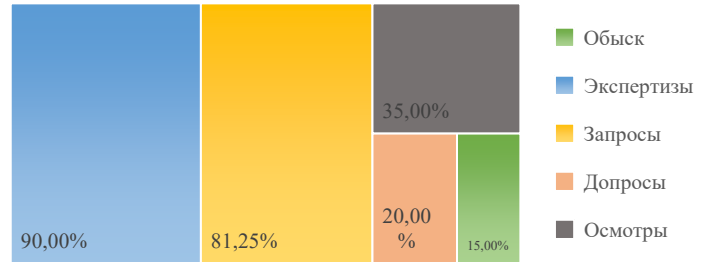
В ходе анкетирования, проводившегося в период с 2024 по 2025 г.г., было изучено мнение 560 сотрудников органов дознания, следствия и оперативных подразделений по вопросам использования программных средств при расследовании преступлений в сфере компьютерной информации и криминалистических характеристик указанных деяний в качестве основы для формирования методик их расследования.

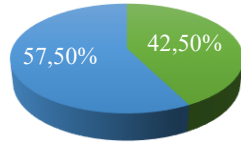
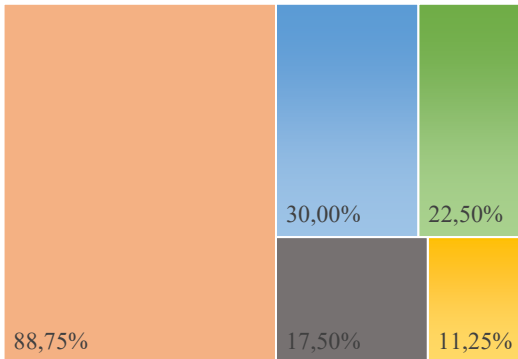
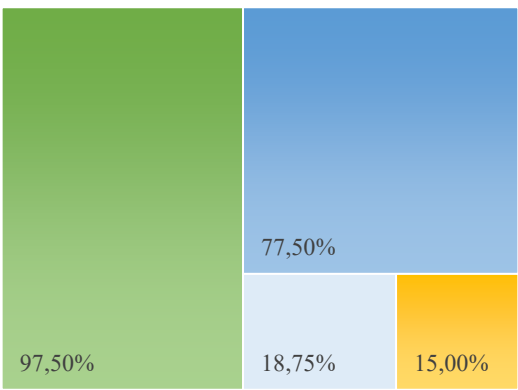
№ п/п	Вопрос	Результат опроса	Количество	%	Интерпретация полученных данных (распределение ответов)																					
1.	Ваша должность	Следователь	413	73,75	<table><tr><th>Должность</th><th>Количество</th><th>%</th></tr><tr><td>Следователь</td><td>413</td><td>73,75</td></tr><tr><td>Дознаватель</td><td>49</td><td>8,75</td></tr><tr><td>Оперативный сотрудник</td><td>98</td><td>17,50</td></tr></table>	Должность	Количество	%	Следователь	413	73,75	Дознаватель	49	8,75	Оперативный сотрудник	98	17,50									
		Должность	Количество	%																						
		Следователь	413	73,75																						
Дознаватель	49	8,75																								
Оперативный сотрудник	98	17,50																								
Дознаватель	49	8,75																								
Оперативный сотрудник	98	17,50																								
2.	Стаж работы в занимаемой должности	1-3 лет	175	31,25	<table><tr><th>Стаж работы</th><th>Количество</th><th>%</th></tr><tr><td>1-3 лет</td><td>175</td><td>31,25</td></tr><tr><td>3-5 лет</td><td>196</td><td>35,00</td></tr><tr><td>5-10 лет</td><td>119</td><td>21,25</td></tr><tr><td>10-15 лет</td><td>56</td><td>10,00</td></tr><tr><td>15-20 лет</td><td>14</td><td>2,50</td></tr><tr><td>Более 20 лет</td><td>0</td><td>0,00</td></tr></table>	Стаж работы	Количество	%	1-3 лет	175	31,25	3-5 лет	196	35,00	5-10 лет	119	21,25	10-15 лет	56	10,00	15-20 лет	14	2,50	Более 20 лет	0	0,00
		Стаж работы	Количество	%																						
		1-3 лет	175	31,25																						
		3-5 лет	196	35,00																						
		5-10 лет	119	21,25																						
		10-15 лет	56	10,00																						
15-20 лет	14	2,50																								
Более 20 лет	0	0,00																								
3-5 лет	196	35,00																								
5-10 лет	119	21,25																								
10-15 лет	56	10,00																								
15-20 лет	14	2,50																								
Более 20 лет	0	0,00																								

3.	Сталкивались ли Вы с необходимостью расследования преступлений в сфере компьютерной информации?	Да	553	98,75	100,00 50,00 0,00 98,75% 1,25% ■ Да ■ Нет
		Нет	7	1,25	
4.	По каким составам преступлений в сфере компьютерной информации Вам приходилось работать чаще всего?	Статья 272 УК РФ «Неправомерный доступ к компьютерной информации»	434	77,50	77,50% 18,75% 2,50% 1,25% 0,00% 0,00% 0,00% ■ 272 УК РФ ■ 272.1 УК РФ ■ 273 УК РФ ■ 274 УК РФ ■ 274.1 УК РФ ■ 274.2 УК РФ ■ 274.3 УК РФ ■ 274.4 УК РФ ■ 274.5 УК РФ
		Статья 272.1 УК РФ «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения»	0	0,00	
		Статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»	105	18,75	
		Статья 274. УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»	7	1,25	
		Статья 274.1. УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»	14	2,50	
		Статья 274.2. УК РФ «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования»	0	0,00	

		Статья 274.3 УК РФ «Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции»	0	0,00											
		Статья 274.4 УК РФ «Организация деятельности по передаче абонентских номеров с нарушением требований законодательства РФ»	0	0,00											
		Статья 274.5 УК РФ «Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям информационного ресурса»	0	0,00											
5.	Какими материалами Вы чаще всего пользуетесь при расследовании преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Алгоритмы действий при расследовании преступлений в сфере компьютерной информации	427	76,25	Множественный выбор (%) <table><thead><tr><th>Материал</th><th>Процент</th></tr></thead><tbody><tr><td>Алгоритмы действий</td><td>76,25%</td></tr><tr><td>Литература</td><td>30,00%</td></tr><tr><td>Научные статьи</td><td>10,00%</td></tr><tr><td>Другое</td><td>2,50%</td></tr></tbody></table>	Материал	Процент	Алгоритмы действий	76,25%	Литература	30,00%	Научные статьи	10,00%	Другое	2,50%
		Материал	Процент												
		Алгоритмы действий	76,25%												
		Литература	30,00%												
		Научные статьи	10,00%												
Другое	2,50%														
Учебные пособия и иная специальная литература	168	30,00													
Научные статьи прикладного характера	56	10,00													
Другое	14	2,50													
Комментарий: респонденты не совсем корректно указали в варианте «Другое» программное обеспечение для анализа цифровых доказательств															
6.	Исходя из Вашего опыта, укажите, какие виды компьютерной информации чаще выступают предметом преступления в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Учетные данные пользователей (логины, пароли и пр.)	455	81,25	Множественный выбор (%) <table><thead><tr><th>Вид информации</th><th>Процент</th></tr></thead><tbody><tr><td>Учетные данные пользователей</td><td>81,25%</td></tr><tr><td>Персональные данные</td><td>42,50%</td></tr><tr><td>Биометрические данные</td><td>10,00%</td></tr><tr><td>Банковские данные и реквизиты</td><td>72,50%</td></tr></tbody></table>	Вид информации	Процент	Учетные данные пользователей	81,25%	Персональные данные	42,50%	Биометрические данные	10,00%	Банковские данные и реквизиты	72,50%
		Вид информации	Процент												
		Учетные данные пользователей	81,25%												
		Персональные данные	42,50%												
		Биометрические данные	10,00%												
Банковские данные и реквизиты	72,50%														
Персональные данные	238	42,50													
Биометрические данные	56	10,00													
Банковские данные и реквизиты	406	72,50													

7.	Какой, по Вашему мнению, основной мотив совершения преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Корыстные побуждения (получение материальной выгоды)	525	93,75	Множественный выбор (%) <table><thead><tr><th>Мотив</th><th>Число</th><th>Процент</th></tr></thead><tbody><tr><td>Корыстные побуждения</td><td>525</td><td>93,75%</td></tr><tr><td>Шпионаж</td><td>63</td><td>11,25%</td></tr><tr><td>Вандализм</td><td>56</td><td>10,00%</td></tr><tr><td>Хулиганство</td><td>35</td><td>6,25%</td></tr><tr><td>Личная неприязнь</td><td>21</td><td>3,75%</td></tr></tbody></table>	Мотив	Число	Процент	Корыстные побуждения	525	93,75%	Шпионаж	63	11,25%	Вандализм	56	10,00%	Хулиганство	35	6,25%	Личная неприязнь	21	3,75%
		Мотив	Число	Процент																			
		Корыстные побуждения	525	93,75%																			
		Шпионаж	63	11,25%																			
		Вандализм	56	10,00%																			
Хулиганство	35	6,25%																					
Личная неприязнь	21	3,75%																					
Личная неприязнь к собственнику информации	21	3,75																					
Хулиганство	35	6,25																					
Вандализм (разрушение информационных систем, атаки на технические средства пр.)	56	10,00																					
Шпионаж (например, получение сведений экономической направленности, личной жизни и пр.)	63	11,25																					
8.	Какие проблемы при расследовании преступлений в сфере компьютерной информации существуют и требуют решения? (можно выбрать несколько вариантов ответов)	Отсутствие четких алгоритмов действий при расследовании преступлений в сфере компьютерной информации	427	76,25	Множественный выбор (%) <table><thead><tr><th>Проблема</th><th>Число</th><th>Процент</th></tr></thead><tbody><tr><td>Отсутствие алгоритмов</td><td>427</td><td>76,25%</td></tr><tr><td>Отсутствие технических средств</td><td>420</td><td>75,00%</td></tr><tr><td>Отсутствие средств по поиску цифровых доказательств</td><td>525</td><td>93,75%</td></tr><tr><td>Сложность выявления из-за средств анонимизации</td><td>322</td><td>57,50%</td></tr><tr><td>Другое</td><td>35</td><td>6,25%</td></tr></tbody></table>	Проблема	Число	Процент	Отсутствие алгоритмов	427	76,25%	Отсутствие технических средств	420	75,00%	Отсутствие средств по поиску цифровых доказательств	525	93,75%	Сложность выявления из-за средств анонимизации	322	57,50%	Другое	35	6,25%
		Проблема	Число	Процент																			
		Отсутствие алгоритмов	427	76,25%																			
		Отсутствие технических средств	420	75,00%																			
		Отсутствие средств по поиску цифровых доказательств	525	93,75%																			
		Сложность выявления из-за средств анонимизации	322	57,50%																			
Другое	35	6,25%																					
Отсутствие необходимых для расследования технических средств	420	75,00																					
Отсутствие действенных средств по обнаружению, фиксации, изъятию и исследованию цифровых доказательств	525	93,75																					
Сложность выявления преступников ввиду использования ими средств анонимизации	322	57,50																					
Другое	35	6,25																					
Комментарий: вариант «Другое» объединен по смыслу из различных формулировок и отражает нехватку времени сотрудника на детальное изучение больших массивов цифровых данных																							
9.	При начале производства по уголовному делу обращаетесь ли Вы к методической и научной литературе, содержащей сведения о типичной криминалистической характеристике того вида преступления, которое предстоит расследовать?	Да	294	52,50	<table><thead><tr><th>Ответ</th><th>Число</th><th>Процент</th></tr></thead><tbody><tr><td>Да</td><td>294</td><td>52,50%</td></tr><tr><td>Нет</td><td>266</td><td>47,50%</td></tr></tbody></table>	Ответ	Число	Процент	Да	294	52,50%	Нет	266	47,50%									
		Ответ	Число	Процент																			
Да	294	52,50%																					
Нет	266	47,50%																					
	Нет	266	47,50																				

10.	Имеет ли, по Вашему мнению, криминалистическая характеристика преступлений практическое значение для расследования преступлений в сфере компьютерной информации?	Да	378	67,50	
		Нет	182	32,50	
11.	Согласны ли Вы, что несмотря на большое количество методических рекомендаций, отсутствует четкий алгоритм действий, направленный на эффективное расследование преступлений в сфере компьютерной информации?	Да	455	81,25	
		Нет	105	18,75	
12.	Как Вы считаете, какие действия являются наиболее эффективными по установлению преступника при расследовании преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Обыск	84	15,00	Множественный выбор (%) 
		Назначение и производство судебных экспертиз	504	90,00	
		Направление запросов (операторам сотовой связи, провайдерам, финансово-кредитным учреждениям)	455	81,25	
		Допросы (свидетелей, потерпевших, подозреваемых)	112	20,00	
		Осмотр предметов (компьютерных и мобильных устройств)	196	35,00	

13.	В целях сокращения сроков расследования преступлений в сфере компьютерной информации проводили ли Вы осмотр компьютерных и мобильных устройств с участием специалиста взамен производства судебной компьютерной экспертизы?	Да	238	42,50	 ■ Да ■ Нет
		Нет	322	57,50	
14.	Исходя из Вашего опыта, укажите наиболее характерные способы совершения неправомерного доступа к компьютерной информации (ст. 272 УК РФ) (можно выбрать несколько вариантов ответов)	Преодоление систем защиты информации	126	22,50	Множественный выбор (%)  ■ Преодоление систем защиты ■ Вредоносное программное обеспечение ■ Уязвимости программного обеспечения ■ Доступ к техническим средствам и информационным системам ■ DDoS-атаки
		Использование вредоносного программного обеспечения для несанкционированного доступа к информации	168	30,00	
		Использования уязвимостей в программном обеспечении	63	11,25	
		Несанкционированное подключение к техническим средствам и информационным системам	497	88,75	
		DDoS-атаки, направленные на перегрузку систем и получение доступа к их ресурсам	98	17,50	
15.	Исходя из Вашего опыта, назовите типичные средства совершения неправомерного доступа к компьютерной информации (ст. 272 УК РФ) (можно выбрать несколько вариантов ответов)	Сетевое оборудование и средства доступа в информационные системы (средства вычислительной техники, мобильные средства связи и пр.)	546	97,50	Множественный выбор (%)  ■ Средства вычислительной техники, мобильные средства ■ Программное обеспечение анонимизации ■ Программное обеспечение для тестов ■ Носители информации
		Программное обеспечение (VPN-сервисы, системы прокси-серверов и пр.), в том числе вредоносное	434	77,50	
		Программное обеспечение, предназначенное для проведения тестов на проникновение	84	15,00	
		Носители информации, эксплуатируемые с техническим средством	105	18,75	

16.	Исходя из Вашего опыта, назовите типичные следы, оставляемые при совершении неправомерного доступа к компьютерной информации (ст. 272 УК РФ) (можно выбрать несколько вариантов ответов)	Цифровые следы установленного программного обеспечения для несанкционированного доступа	385	68,75	Множественный выбор (%) Цифровые следы программного обеспечения Изменения в конфигурации операционной системы Журналы подключений Изменения в данных Материальные следы
		Изменения в конфигурации операционной системы устройства	525	93,75	
		Журналы подключений к компьютерам или информационным системам	532	95,00	
		Модифицированные или заблокированные файлы данных и т. п.	357	63,75	
		Материальные следы на компьютерной периферии	21	3,75	
17.	Исходя из Вашего опыта, укажите основные, наиболее часто встречающиеся на практике способы выявления цифровых следов при расследовании неправомерного доступа к компьютерной информации (ст. 272 УК РФ) (можно выбрать несколько вариантов ответов)	Анализ системного и прикладного программного обеспечения	448	80,00	Множественный выбор (%) Анализ программного обеспечения Анализ электронных носителей информации Анализ идентификаторов Анализ реестра операционной системы Анализ сетевого трафика
		Анализ поименованной области записей на электронных носителях информации и электронных файлов	203	36,25	
		Анализ идентификаторов в сети передачи данных (например, IP-адрес устройства или MAC-адрес его сетевой карты)	546	97,50	
		Анализ реестра операционной системы	357	63,75	
		Анализ сетевого трафика	511	91,25	

18.	Укажите наиболее вероятные способы незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а равно создания и (или) обеспечения функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ) (можно выбрать несколько вариантов ответов)	Преодоление систем защиты информации в виде хищения учетных данных пользователей с целью получения персональных данных, использование несовершенств информационных систем персональных данных	483	86,25	Множественный выбор (%) Преодоление систем защиты информации Использование уязвимостей программного обеспечения Подключение к техническим средствам и т.п. Неправомерный доступ к средствам обработки данных
		Использование уязвимостей программного обеспечения и операционных систем, эксплуатирующих информационные системы персональных данных	371	66,25	
		Несанкционированное подключение к техническим средствам, а также вспомогательному компьютерному оборудованию, эксплуатирующему информационные системы персональных данных	252	45,00	
		Неправомерный доступ к средствам обработки персональных данных	343	61,25	
19.	Укажите наиболее вероятные средства незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а равно создания и (или) обеспечения функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ) (можно выбрать несколько вариантов ответов)	Программное обеспечение для сбора персональных данных с персональных компьютеров и мобильных устройств, способное перехватывать совокупность действий пользователей (нажатия клавиш, записей звонков и сбора конфиденциальных данных)	532	95,00	Множественный выбор (%) Программное обеспечение для сбора персональных данных с технических средств Сетевые sniffеры Теневые маркетплейсы Электронные носители информации
		Сетевые sniffеры (анализаторы сетевого трафика, содержащие персональные данные)	357	63,75	
		Теневые маркетплейсы для распространения персональных данных	525	93,75	
		Носители информации, эксплуатируемые с техническими средствами	350	62,50	

20.	Укажите наиболее вероятные следы, оставляемые при незаконном использовании и (или) передаче, сборе (или) хранении компьютерной информации, содержащей персональные данные, а равно созданию и (или) обеспечении функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ) (можно выбрать несколько вариантов ответов)	Цифровые следы установленного программного обеспечения, используемого для незаконной обработки или хранения персональных данных	469	83,75	Множественный выбор (%) Цифровые следы программного обеспечения Изменения в конфигурации операционной системы Журналы подключений Материальные следы
		Изменения в конфигурации операционной системы устройства	434	77,50	
		Журналы подключений к компьютерам или информационным системам персональных данных	413	73,75	
		Материальные следы на компьютерной периферии	35	6,25	
21.	Укажите наиболее вероятные способы выявления цифровых следов при расследовании незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а равно создания и (или) обеспечения функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ) (можно выбрать несколько вариантов ответов)	Анализ системного и прикладного программного обеспечения	434	77,50	Множественный выбор (%) Анализ программного обеспечения Анализ электронных носителей информации Анализ идентификаторов Анализ реестра операционной системы Анализ сетевого трафика
		Анализ электронных носителей информации и электронных файлов	182	32,50	
		Анализ идентификаторов в сети передачи данных (например, IP-адрес устройства или MAC-адрес его сетевой карты)	476	85,00	
		Анализ реестра операционной системы	280	50,00	
		Анализ сетевого трафика	434	77,50	

22.	Исходя из Вашего опыта, укажите наиболее характерные способы распространения вредоносных компьютерных программ (ст. 273 УК РФ) (можно выбрать несколько вариантов ответов)	Использование специализированных сервисов в виде автоматизированных конструкторов вредоносного программного обеспечения	168	30,00	Множественный выбор (%) Использование специализированных сервисов Распространение ссылок и программного обеспечения Заражение электронных носителей информации и IoT-устройств
		Распространение вредоносных ссылок и программного обеспечения на веб-ресурсах	525	93,75	
		Заражение электронных носителей информации и IoT-устройств	175	31,25	
23.	Исходя из Вашего опыта, назовите типичные средства распространения вредоносных компьютерных программ (ст. 273 УК РФ) (можно выбрать несколько вариантов ответов)	Электронные носители информации, эксплуатируемые со средствами вычислительной техники	525	93,75	Множественный выбор (%) Электронные носители информации Сетевое оборудование Средства вычислительной техники, мобильные средства связи и пр. Программное обеспечение (кейлоггеры, руткиты и пр.)
		Сетевое оборудование	98	17,50	
		Средства доступа в информационные системы (средства вычислительной техники, мобильные средства связи и пр.)	504	90,00	
		Программное обеспечение (кейлоггеры, руткиты, трояны и пр.)	539	96,25	
24.	Исходя из Вашего опыта, назовите типичные следы, оставляемые при распространении вредоносных компьютерных программ (ст. 273 УК РФ) (можно выбрать несколько вариантов ответов)	Следы установленного программного обеспечения с признаками вредоносного функционала	455	81,25	Множественный выбор (%) Следы установленного программного обеспечения Изменения в конфигурации операционной системы Измененные файлы данных Следы вредоносного программного обеспечения в сети Интернет Следы вредоносного программного обеспечения в рассылках
		Изменения в конфигурации операционной системы, журналах подключений к компьютерам, информационным системам	455	81,25	
		Удаленные, модифицированные или заблокированные файлы данных	210	37,50	
		Следы распространения вредоносного программного обеспечения в сети «Интернет»	203	36,25	
		Следы распространения вредоносного программного обеспечения в фишинговых электронных рассылках	98	17,50	

25.	Исходя из Вашего опыта, укажите основные, наиболее часто встречающиеся на практике способы выявления цифровых следов, образующихся в результате распространения вредоносных компьютерных программ (ст. 273 УК РФ) (можно выбрать несколько вариантов ответов)	Анализ системного и прикладного программного обеспечения	448	80,00	Множественный выбор (%) 85,00% 80,00% 30,00% 27,50% Анализ программного обеспечения Анализ электронных носителей информации Анализ электронных файлов и баз данных Анализ идентификаторов
		Анализ записей на электронных носителях информации	154	27,50	
		Анализ электронных файлов и баз данных	168	30,00	
		Анализ идентификаторов в сети передачи данных (IP-адрес устройства или MAC-адрес его сетевой карты), IMEI-кодов мобильных устройств, DNS-адресов	476	85,00	
		Анализ реестров операционных систем и сетевого трафика	357	63,75	
26.	Исходя из Вашего опыта (или предположений), укажите наиболее характерные способы нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) (можно выбрать несколько вариантов ответов)	Предоставление посторонним лицам прав доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации или сетям	427	76,25	Множественный выбор (%) 80,00% 76,25% 72,50% 51,25% 46,25% Предоставление посторонним прав доступа Разглашение учетных данных Нарушение регламента подключения Несанкционированная модификация программного обеспечения Отключение средств защиты информации и пр.
		Разглашение учетных данных (логина и пароля для доступа к информационным системам или сетям)	406	72,50	
		Нарушение запрета на подключение оконечного оборудования к сети «Интернет»	287	51,25	
		Несанкционированная модификация программного обеспечения	259	46,25	
		Отключение средств защиты информации и пр.	448	80,00	
27.	Исходя из Вашего опыта (или предположений), назовите типичные средства нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) (можно выбрать несколько вариантов ответов)	Сетевое и серверное оборудование,	357	63,75	Множественный выбор (%) 87,50% 81,25% 76,25% 63,75% 30,00% 22,50% Сетевое и серверное оборудование Мобильные устройства и средства доступа в информационные системы Виртуальные машины Облачные сервисы Программное обеспечение Средства защиты информации
		Мобильные устройства и средства доступа в информационные системы и информационно-телекоммуникационные сети	427	76,25	
		Виртуальные машины	490	87,50	
		Облачные сервисы	126	22,50	
		Программное обеспечение, в том числе вредоносное	455	81,25	
		Средства защиты информации (антивирусное программное обеспечение, брандмауэры, системы обнаружения вторжений, системы аутентификации)	168	30,00	

28.	Исходя из Вашего опыта (или предположений), назовите типичные следы, оставляемые при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) (можно выбрать несколько вариантов ответов)	Следы установленного программного обеспечения с признаками вредоносного функционала	245	43,75	Множественный выбор (%) 72,50% 61,25% 43,75% 51,25% 3,75 % - Следы установленного программного обеспечения - Изменения в конфигурации операционной системы - Следы в журналах событий - Изменения в журналах - Материальные следы
		Изменения в конфигурации операционной системы, журналах подключений к компьютерам, информационным системам	343	61,25	
		Следы в журналах событий, протоколирующих входы в систему и изменения привилегий доступа к информационным системам или сетям	406	72,50	
		Изменения в журналах межсетевых экранов	287	51,25	
		Материальные следы на компьютерной периферии	21	3,75	
29.	Исходя из Вашего опыта (или предположений), укажите основные, наиболее часто встречающиеся на практике способы выявления цифровых следов при расследовании нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ) (можно выбрать несколько вариантов ответов)	Анализ системного и прикладного программного обеспечения	476	85,00	Множественный выбор (%) 97,50% 96,25% 85,00% 65,00% 58,75% - Анализ программного обеспечения - Анализ электронных носителей информации - Анализ идентификаторов - Анализ реестра операционной системы - Анализ сетевого трафика
		Анализ поименованных областей записей на электронных носителях информации	329	58,75	
		Анализ идентификаторов в сети передачи данных (IP-адрес устройства или MAC-адрес его сетевой карты), IMEI-кодов, DNS-адресов	539	96,25	
		Анализ реестров операционных систем	364	65,00	
		Анализ сетевого трафика	546	97,50	
30.	Исходя из Вашего опыта (или предположений), укажите основные, наиболее часто встречающиеся на практике способы неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) (можно выбрать несколько вариантов ответов)	Нарушение правил доступа к информации, содержащейся в критической информационной инфраструктуре РФ	427	76,25	Множественный выбор (%) 87,50% 77,50% 65,00% 80,00% 76,25% 63,75% 35,00% - Нарушение правил доступа - Изменение настроек - Отключение систем защиты информации - Подключение к оборудованию - Изменение информации - Использование нагрузочного тестирования - Перехват сетевого трафика
		Несанкционированное изменение настроек оборудования	364	65,00	
		Отключение средств защиты информации и программного обеспечения резервирования данных	434	77,50	
		Несанкционированное подключение к оборудованию или системам объекта	490	87,50	
		Несанкционированный доступ к объекту или внесение в систему объекта недостоверной информации	448	80,00	
		Использование веб-сервисов сети «Интернет», предназначенных для нагрузочного тестирования	196	35,00	
		Перехват сетевого трафика	357	63,75	

31.	Исходя из Вашего опыта (или предположений), назовите типичные средства совершения неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) (можно выбрать несколько вариантов ответов)	Сетевое и серверное оборудование, а также информационные системы, функционирующие на объекте критической информационной инфраструктуры РФ	371	66,25	Множественный выбор (%) 81,25% 72,50% 71,25% 66,25% Сетевое и серверное оборудование Средства доступа в информационные системы Виртуальные машины Облачные сервисы Программное обеспечение Средства защиты информации Системы обнаружения вторжений Персональные средства аутентификации
		Средства доступа в информационные системы, функционирующие на объекте и эксплуатируемые носители данных	455	81,25	
		Виртуальные машины	203	36,25	
		Облачные сервисы	168	30,00	
		Программное обеспечение, в том числе вредоносное	371	66,25	
		Средства защиты информации (антивирусное программное обеспечение, брандмауэры, системы обнаружения вторжений, системы аутентификации)	399	71,25	
		Системы обнаружения вторжений	434	77,50	
		Персональные средства аутентификации (электронные цифровые подписи, учетные записи, API-ключи)	406	72,50	
32.	Исходя из Вашего опыта (или предположений), назовите типичные следы, остающиеся при совершении неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) (можно выбрать несколько вариантов ответов)	Следы установленного программного обеспечения с признаками вредоносного функционала	476	85,00	Множественный выбор (%) 90,00% 85,00% 87,50% 65,00% 2,50 % Следы установленного программного обеспечения Изменения в конфигурации операционной системы Следы в журналах событий Изменения в журналах межсетевых экранов Материальные следы
		Изменения в конфигурации операционной системы, журналах подключений к компьютерам, информационным системам	490	87,50	
		Следы в журналах событий, протоколирующих входы в систему и изменения привилегий доступа к информационным системам сетям	504	90,00	
		Изменения в журналах межсетевых экранов	364	65,00	
		Материальные следы на компьютерной периферии	14	2,50	

33.	Исходя из Вашего опыта (или предположений), укажите основные, наиболее часто встречающиеся на практике способы выявления цифровых следов при расследовании неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) (можно выбрать несколько вариантов ответов)	Анализ журналов событий в системе и реестров сетевых подключений	406	72,50	Множественный выбор (%) Анализ журналов событий в системе Анализ идентификаторов Анализ журналов соединений Анализ серийных номеров носителей информации Анализ журналов файловых систем и метаданных Анализ журналов функционирования систем мониторинга киберинцидентами
		Анализ IP-адресов, MAC-идентификаторов, используемых устройств, IMEI/IMSI-кодов корпоративных мобильных средств связи	476	85,00	
		Анализ журналов функционирования систем мониторинга киберинцидентами, протоколирующих аномальные события в работе оборудования, ошибки, сбои, фиксацию параметров нагрузки	413	73,75	
		Анализ серийных номеров носителей информации	147	26,25	
		Анализ журналов файловых систем и метаданных с отображением лог-файлов, временных меток, атрибутов доступа и пр.	413	73,75	
		Анализ журналов соединений, изменений в прошивках устройств, входящих в инфраструктуру объекта критической информационной инфраструктуры РФ	350	62,50	
34.	Исходя из Вашего опыта, укажите основные, наиболее часто встречающиеся на практике недостатки проведения осмотра места происшествия и проверки показаний на месте при расследовании преступления в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Проводятся поверхностно, без должного установления обстоятельств события преступления	406	72,50	Множественный выбор (%) Проводятся поверхностно Проводятся в момент, когда следы могут утрачены Проводятся в отсутствие специалиста Проводятся без выдвижения и проверки версий
		Проводятся в момент, когда многие следы объективно могут утрачены	476	85,00	
		Проводятся в отсутствие специалиста	168	30,00	
		Проводятся наспех, без предварительного выдвижения и проверки версий	490	87,50	

35.	Исходя из Вашего опыта, укажите основные, наиболее часто встречающиеся на практике недостатки проведения допроса подозреваемого по делам, связанным с преступлениями в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Проводятся поверхностно, без должного установления обстоятельств события преступления	413	73,75	Множественный выбор (%) Проводятся поверхностно 73,75% Проводятся в момент, когда соучастники могут скрыться 50,00% Проводятся в отсутствие специалиста 30,00% Проводятся без выдвижения и проверки версий 60,00%
		Проводятся в момент, когда возможные соучастники могут скрыться и (или) скрыть следы преступной деятельности (инсценировки и др.)	280	50,00	
		Проводятся в отсутствие специалиста	168	30,00	
		Проводятся наспех, без предварительного выдвижения и проверки версий	336	60,00	
36.	Исходя из Вашего опыта, укажите основные, наиболее часто встречающиеся на практике недостатки при назначении судебной компьютерно-технической экспертизы? (можно выбрать несколько вариантов ответов)	Вопросы эксперту формулируются неточно, без учета специфики преступлений в сфере компьютерной информации	105	18,75	Множественный выбор (%) Вопросы эксперту формулируются неточно 18,75 % Проводится без выдвижения и проверки версий 25,00% Вопросы эксперту формулируются не в полном объеме 61,25% Эксперту задаются вопросы юр. характера 48,75% Эксперту задаются вопросы, не относящиеся к его компетенции 63,75%
		Проводится наспех, без предварительного выдвижения и проверки версий	140	25,00	
		Вопросы эксперту формулируются в объеме, который не позволяет в полной мере установить обстоятельства события	343	61,25	
		Эксперту задаются вопросы юридического характера	273	48,75	
		Эксперту задаются вопросы, не относящиеся к его компетенции	357	63,75	

37.	Взаимодействие правоохранителей с какими государственными органами и другими субъектами Вы считаете наиболее целесообразным для целей повышения эффективности расследования преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Национальное центральное бюро Интерпола	84	15,00	Множественный выбор (%) 97,50% 27,50% 67,50% 50,00% 15,00% Интерпола ГосСОПКА ФинЦЕРТ Мицифры Роскомнадзор
		Национальный координационный центр по компьютерным инцидентам (система «ГосСОПКА»)	154	27,50	
		Департамент информационной безопасности Банка России («ФинЦЕРТ»)	378	67,50	
		Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (система «Антифишинг»)	546	97,50	
		Департамент информационной безопасности Банка России Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор (система «Антифрод»)	280	50,00	
38.	Исходя из Вашего опыта, каковы основные причины недостаточной эффективности расследования преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Низкая квалификация кадров правоохранительных органов	84	15,00	Множественный выбор (%) 70,00% 15,00% 10,00% 3,75% Низкая квалификация Отсутствие рекомендаций Недостаточное взаимодействие Недобросовестность
		Отсутствие полноценных методических рекомендаций	392	70,00	
		Недостаточное взаимодействие между следствием, субъектами оперативно-розыскной деятельности, государственным обвинителем	56	10,00	
		Недобросовестность отдельных сотрудников	21	3,75	
39.	Как Вы оцениваете потенциал программных средств, применяемых при расследовании преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Очень высокий, программные технико-криминалистические средства должны быть использованы в числе первых	518	92,50	Множественный выбор (%) 92,50% 90,00% 15,00% Очень высокий Высокий Средний Низкий
		Высокий, программные технико-криминалистические средства эффективны, но их количество достаточно ограниченное	504	90,00	
		Средний, программные технико-криминалистические средства эффективны лишь в отношении самых «примитивных» преступлений в сфере компьютерной информации	84	15,00	

		Низкий, программные технико-криминалистические средства малоэффективны	0	0,00	
40.	Как Вы оцениваете потенциал интеллектуальных программных средств (разработанных на основе искусственного интеллекта), способствующих расследованию преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Высокий, интеллектуальные программные технико-криминалистические средства будут являться действенным решением проблем, возникающих при расследовании преступлений в сфере компьютерной информации	504	90,00	Множественный выбор (%) 90,00% 30,00% 2,50% ■ Высокий ■ Средний ■ Низкий
		Средний, интеллектуальные программные технико-криминалистические средства эффективны, но их использование может вызывать проблемы, связанные с отсутствием доверия к результатам его функционирования	168	30,00	
		Низкий, интеллектуальные программные технико-криминалистические средства будут малоэффективны	14	2,50	
41.	По Вашему мнению, смогли бы Вы на практике использовать программные средства без участия специалиста при наличии четко определенных алгоритмов действий при расследовании преступлений в сфере компьютерной информации?	Да	546	97,50	Да; 97,50% Нет; 2,50% ■ Да ■ Нет
		Нет	14	2,50	

42.	По Вашему мнению, что является наиболее актуальной причиной низкого качества расследования преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Незнание механизма совершения преступления	490	87,50	Множественный выбор (%) 87,50% 85,00% 55,00% 80,00% - Незнание механизма совершения преступления - Отсутствие доп. Образования - Отсутствие алгоритма действий - Отсутствие ПТКС для их расследования
		Отсутствие дополнительного образования в сфере информационных технологий	308	55,00	
		Отсутствие четкого алгоритма действий при расследовании	448	80,00	
		Отсутствие программных технико-криминалистических средств для их расследования	476	85,00	
43.	По Вашему мнению, что послужит «катализатором» повышения эффективности расследования преступлений в сфере компьютерной информации? (можно выбрать несколько вариантов ответов)	Формирование новых информационно-поисковых систем, аккумулирующих криминалистически-значимую компьютерную информацию (цифровые доказательства)	539	96,25	Множественный выбор (%) 96,25% 92,50% 95,00% 87,50% - Формирование новых информационно-поисковых систем - Формирование новых учетов - Совершенствование имеющихся крим. учетов - Оптимизация процесса сбора цифровых
		Формирование новых учетов криминалистически-значимой компьютерной информации (цифровых доказательств)	490	87,50	
		Совершенствование уже имеющихся криминалистических учетов	532	95,00	
		Оптимизация процесса сбора цифровых доказательств	518	92,50	

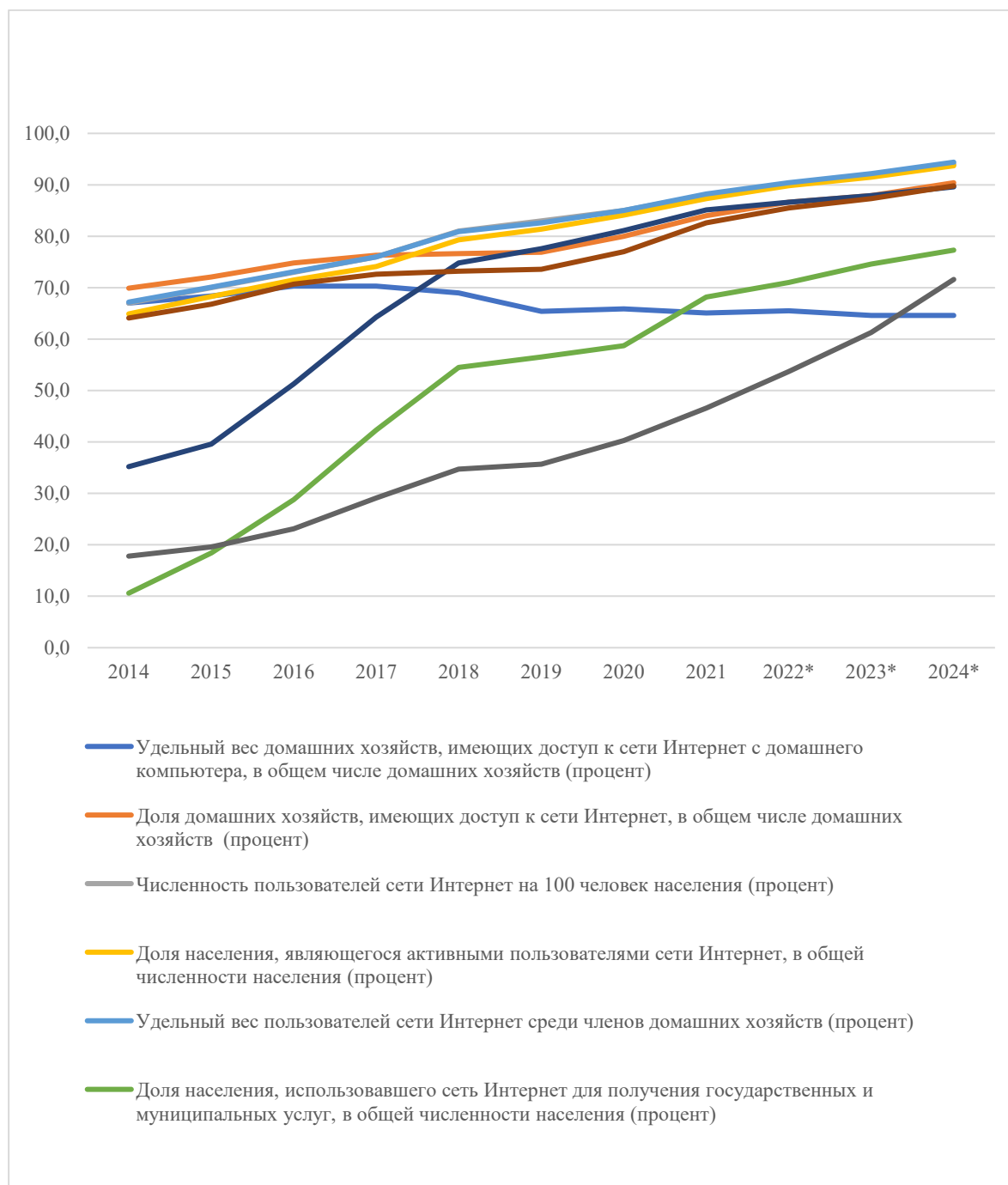
44.	В настоящее время во всем мире активно ведутся работы по созданию цифровых двойников различных явлений и процессов (цифровых моделей предполагаемого или реального физического продукта, системы или процесса, которые служат его цифровым аналогом (прототипом) для таких целей, как моделирование, мониторинг, тестирование и проверка гипотез). По Вашему мнению, будет ли способствовать наличие интеллектуального цифрового двойника преступления в сфере компьютерной информации повышению эффективности его расследования при условии, что он будет обучен на множестве раскрытых уголовных дел указанной категории?	Да	532	95,00
		Нет	7	1,25
		Затрудняюсь ответить	21	3,75

Donut chart illustrating the distribution of responses for question 44:

- Да (Yes): 95,00%
- Нет (No): 1,25%
- Затрудняюсь ответить (Don't know): 3,75%

Приложение 2

«Динамика использования населением РФ сети «Интернет» за период с 2014 по 2024 г.г.»

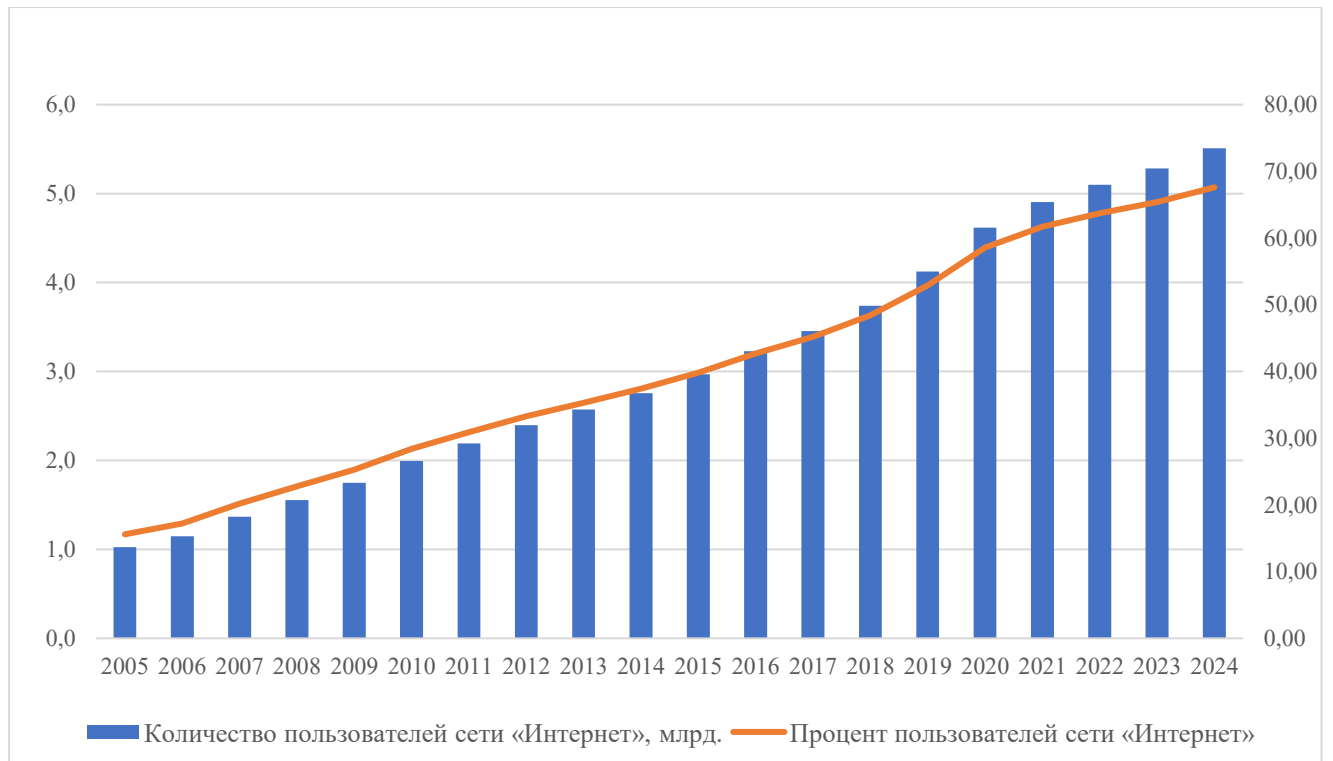


* Без учета статистической информации по Донецкой Народной Республике (ДНР), Луганской Народной Республике (ЛНР), Запорожской и Херсонским областям⁶³⁷.

⁶³⁷ Мониторинг развития информационного общества в Российской Федерации // Официальный сайт Федеральной службы государственной статистики. URL: <https://rosstat.gov.ru/storage/mediabank/monitor.xlsx> (дата обращения: 25.03.2025).

Приложение 3

«Динамика количества подключенных к сети «Интернет»
пользователей в мире за период с 2005 по 2024 г.г.»



Приложение 4

«Динамика зарегистрированных преступлений, совершаемых в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий, за период с 2020 по 2024 г.г.»

Статья УК РФ	2020	2021	2022	2023	2024	Прирост / снижение, %
137	643	756	862	893	939	5,2
138	306	437	353	326	151	-53,7
138 ¹	172	107	91	95	94	-1,1
146	298	249	189	127	101	-20,5
158	173 416	156 792	113 565	119 212	105 937	-11,1
159	210 493	238 560	249 984	353 201	379 762	7,5
159 ³	25 820	10 258	7 288	2 461	27	-88,9
159 ⁶	761	431	334	417	309	-25,9
163	3 157	4 020	5 721	6 495	5 474	-15,7
171 ²	747	614	583	580	368	-36,6
183	208	443	259	298	198	-33,6
187	804	1 755	2 647	4 188	4 822	15,1
205 ¹	—	-	251	202	258	27,7
205 ²	232	315	490	548	892	62,8
207	—	—	21 424	17 574	14 648	-16,6
228	—	—	19 643 643	20 926	21 485	2,7
228 ¹	47 060	51 444	62 209	81 520	94 645	16,1
234	392	544	447	727	1 360	87,1
242	1 372	1 511	1 630	2 147	2 426	13,0
242 ¹	545	541	813	866	957	10,5
242 ²	182	247	145	114	171	50,0
272	4 105	6 392	9 308	36 788	105 311	186,3
273	371	317	200	196	309	57,7
274 ¹	22	159	519	114	—	—

Приложение 5

«Формы направления заявлений (сообщений) о преступлениях»

Internet Crime Complaint Center (IC3)

File A Complaint Public Info Industry Info Cyber Private Sector Crime Info

1 Who is Filing this Complaint?

2 Complainant Information 3 Financial Transaction(s) 4 Information About The Subject(s) 5 Description of Incident 6 Other Information 7 Privacy & Signature

1

- A red asterisk (*) indicates a required field.
- All other fields are optional. Please provide all requested information if possible, but these fields may be left blank.
- Do NOT provide complainant Personally Identifiable Information (PII) such as Social Security numbers or dates of birth anywhere in this form.

Who is Filing this Complaint?

If you were the one affected by this incident, please indicate so below. In the event that you are completing this form on behalf of another individual or business, please select NO and provide your contact information.

***Were you the one affected in this incident?**

☐ Yes ☐ No

Your Contact Information

If you are the one affected by this incident, the information below will be transferred to the Complainant section.

***Name:**

Business Name:

***Phone Number:**

***Email Address:**

Next (step 2)

Форма направления обращения по факту совершения преступления в сети «Интернет» службы «Internet crime complaint center (IC3)» (США)

Action Fraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

REPORTING TYPES OF FRAUD PREVENTION NEWSROOM ABOUT US

Report fraud

What did the fraud relate to?

 A letter, phone call or email

 Buying / Selling

 Hacking, viruses & malware

 Identity theft

 Dating fraud

 Pension frauds

 Bank account / Plastic cards

 Financial investments

[I can't find the relevant option](#)

[BACK](#)

Форма направления обращения по факту совершения киберпреступления центра «Action Fraud» (Великобритания)

1. ЛИЧНЫЕ ДАННЫЕ ЗАЯВИТЕЛЯ

Фамилия *

Имя *

Отчество

Контактный телефон *

Электронная почта *

Адрес проживания

2. ИНФОРМАЦИЯ О ПРЕСТУПЛЕНИИ

Тип преступления *

-- Выберите тип преступления --

СВЕДЕНИЯ ПО ПРЕСТУПЛЕНИЮ (ПРИ НАЛИЧИИ)

Способ совершения *

Выберите способ

Среда совершения *

Выберите среду

Средство совершения *

Выберите средство

Выберите основной способ совершения преступления

Цифровые следы *

Выберите след

Расположение цифровых следов *

Выберите расположение

Способ сокрытия следов *

Выберите способ

Место совершения *

Выберите место

Дата происшествия *

Время происшествия

Подробное описание происшествия *

Укажите все известные вам детали: что именно произошло, какие действия были совершены, какие последствия наступили

Очистить форму

— Вернуться на главную

3. ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Информация о предполагаемом преступнике (если известна)

Дополнительная информация

4. ИМЕЮЩИЕСЯ ДОКАЗАТЕЛЬСТВА

Прикрепите файлы с доказательствами

Нажмите для выбора файлов или перетащите файлы сюда

Поддерживаемые форматы: изображения (JPG, PNG), документы (PDF, DOC, DOCX), логи (TXT, LOG)

Выбрать файлы

Файл не выбран

Ссылки на ресурсы, связанные с инцидентом

5. СОГЛАСИЕ И ПОДТВЕРЖДЕНИЕ

☐ Я даю согласие на обработку моих персональных данных в соответствии с Федеральным законом № 152-ФЗ "О персональных данных" *

☐ Я подтверждаю, что предоставленная информация является достоверной и полной *

ОТПРАВИТЬ ЗАЯВЛЕНИЕ

ОТПРАВИТЬ ЧЕРЕЗ ГОСУСЛУГИ

Вариант формы направления заявления (сообщения) о преступлении в сфере компьютерной информации

Приложение 6

«Свидетельства о государственной регистрации программ для ЭВМ
(программные технико-криминалистические средства,
применяемые при расследовании преступлений в сфере компьютерной информации)»

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО
о государственной регистрации программы для ЭВМ

№ 2020610510

**«БАЗИС - БАЗОВЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ
ИНФОРМАЦИОННЫХ СИСТЕМ»**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования «Уфимский
юридический институт Министерства внутренних дел
Российской Федерации» (RU)*

Автор: *Харисова Зарина Ирековна (RU)*

Заявка № **2019666679**
Дата поступления **17 декабря 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ **15 января 2020 г.**

Руководитель Федеральной службы
по интеллектуальной собственности



Г.П. Илизов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО
о государственной регистрации программы для ЭВМ

№ 2020661720

**ПРОГРАММНО-АНАЛИТИЧЕСКИЙ КОМПЛЕКС
«КИБЕРПРЕСТУПНОСТЬ»**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования «Уфимский
юридический институт Министерства внутренних дел
Российской Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU),
Лоницакова Анжелла Рашитовна (RU)*

Заявка № **2020660996**
Дата поступления **23 сентября 2020 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ **30 сентября 2020 г.**

Руководитель Федеральной службы
по интеллектуальной собственности



Г.П. Илизов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2021665929

**Алгоритмический комплекс процессуальных действий
при дистанционном мошенничестве «АКПД ДИСТАНТ»**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования
«Уфимский юридический институт Министерства
внутренних дел Российской Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Нугаева Эльвира
Дамировна (RU), Антонов Вячеслав Викторович (RU)*



Заявка № 2021662179

Дата поступления 29 июля 2021 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 05 октября 2021 г.

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ильев

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022611631

**СИСТЕМА МОНИТОРИНГА КИБЕРИНЦИДЕНТОВ
LOCAL SIEM**

Правообладатели: *Харисова Зарина Ирековна (RU), Антонов
Вячеслав Викторович (RU), Рафиков Арслан Ильфатович (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Антонов Вячеслав
Викторович (RU), Рафиков Арслан Ильфатович (RU)*



Заявка № 2022610610

Дата поступления 19 января 2022 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 28 января 2022 г.

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ильев

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023667481

BIOSCAN - Интеллектуальная система распознавания биометрических данных на основе машинного обучения (ML), компьютерного зрения (CV) и искусственного интеллекта (AI)

Правообладатель: *Федеральное государственное казенное образовательное учреждение высшего образования «Уфимский юридический институт Министерства внутренних дел Российской Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Нугаева Эльвира Дамировна (RU)*

Заявка № 2023666662

Дата поступления 08 августа 2023 г.

Дата государственной регистрации

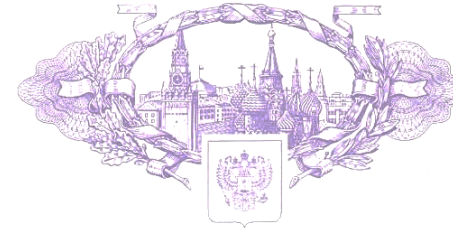
в Реестре программ для ЭВМ 15 августа 2023 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023667143

**ТАКТИКА ПРОИЗВОДСТВА ОТДЕЛЬНЫХ ВИДОВ
ОСМОТРА ПРИ РАССЛЕДОВАНИИ
ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С
ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ**

Правообладатель: *Федеральное государственное казенное образовательное учреждение высшего образования «Уфимский юридический институт Министерства внутренних дел Российской Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Нугаева Эльвира Дамировна (RU), Антонов Вячеслав Викторович (RU)*

Заявка № 2023666488

Дата поступления 04 августа 2023 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 10 августа 2023 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024661188

**BLOCKCHAIN ANALYTICS [АНАЛИТИКА
БЛОКЧЕЙНА] РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ,
СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ
КРИПТОВАЛЮТ И СЕТИ БЛОКЧЕЙН**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования
«Уфимский юридический институт Министерства
внутренних дел Российской Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Нугаева Эльвира
Дамировна (RU), Ишмеева Анастасия Сергеевна (RU)*

Заявка № 2024619990

Дата поступления 06 мая 2024 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 16 мая 2024 г.

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов



РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024661082

**MACDEV V.1.0 [MOBILE AND COMPUTER DEVICES
INSPECTION] - ПРОИЗВОДСТВО ОСМОТРА
КОМПЬЮТЕРНОЙ ТЕХНИКИ И МОБИЛЬНЫХ УСТРОЙСТВ
ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования «Уфимский
юридический институт Министерства внутренних дел Российской
Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Нугаева Эльвира Дамировна
(RU), Антонов Вячеслав Викторович (RU)*

Заявка № 2024619987

Дата поступления 06 мая 2024 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 15 мая 2024 г.

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов



РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025682275

**BLOCKCHAIN & CFA ANALYTICS [АНАЛИТИКА
БЛОКЧЕЙНА И ЦФА] – РАССЛЕДОВАНИЕ
ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ
ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ И СЕТИ
БЛОКЧЕЙН**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования «Уфимский
юридический институт Министерства внутренних дел
Российской Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Нугаева Эльвира
Дамировна (RU), Еркеев Ильшат Хамитович (RU)*

Заявка № 2025680132

Дата поступления 31 июля 2025 г.

Дата государственной регистрации

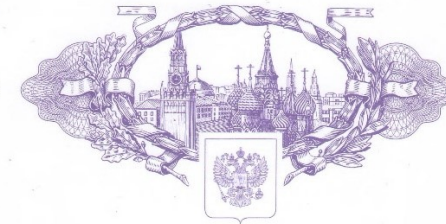
в Реестре программ для ЭВМ 22 августа 2025 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025682276

**MASDEV TECHVIEW [ОСМОТР ТЕХНИЧЕСКИХ СРЕДСТВ]
– ПРОИЗВОДСТВО ОСМОТРА КОМПЬЮТЕРНОЙ ТЕХНИКИ
И МОБИЛЬНЫХ УСТРОЙСТВ ПРИ РАССЛЕДОВАНИИ
ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования «Уфимский
юридический институт Министерства внутренних дел Российской
Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Нугаева Эльвира Дамировна
(RU)*

Заявка № 2025680135

Дата поступления 31 июля 2025 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 22 августа 2025 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025682277

**CYBERCODEX [КИБЕРКОДЕКС] – ПРОГРАММНОЕ
ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОЕ СРЕДСТВО С
КОДИФИКАТОРОМ ПРЕСТУПЛЕНИЙ В СФЕРЕ
КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования
«Уфимский юридический институт Министерства
внутренних дел Российской Федерации» (RU)*

Авторы: *Харисова Зарина Ирековна (RU), Макаренко Илона
Анатольевна (RU)*

Заявка № 2025680136

Дата поступления 31 июля 2025 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 22 августа 2025 г.

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов



РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025680704

**CYBERCRIME DT MODEL (AI) [ЦИФРОВОЙ
ДВОЙНИК КИБЕРПРЕСТУПЛЕНИЯ] - ЦИФРОВАЯ
КРИМИНАЛИСТИЧЕСКАЯ МОДЕЛЬ
ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ
ИНФОРМАЦИИ**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования
«Уфимский юридический институт Министерства
внутренних дел Российской Федерации» (RU)*

Автор(ы): *Харисова Зарина Ирековна (RU)*

Заявка № 2025669600

Дата поступления 31 июля 2025 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 07 августа 2025 г.

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов



Приложение 7

«Аналитическая справка по результатам исследования материалов уголовных дел о преступлениях в сфере компьютерной информации (обобщенные данные о наиболее значимых признаках рассматриваемых преступных деяний)»

Для формирования цифровой криминалистической модели преступления в сфере компьютерной информации были задействованы переменные (признаки), вносящие наибольший вклад в прогноз вероятности раскрытия преступного деяния и отобранные по результатам анализа 284 материалов уголовных дел о преступлениях в сфере компьютерной информации, совершенных за период с 2020 по 2025 г.г. на территориях 17 регионов Российской Федерации.

Содержание переменных, исходя из собранного эмпирического материала, было представлено категориальными, бинарными и числовыми данными в виде отдельных признаков или их совокупности следующим набором:

– вид преступления в соответствии со статьей УК РФ «Crime_ID_Cx»: «272»; «272.1»; «273»; «274»; «274.1»;

– способ совершения преступления «Method_Mxxx»:
 M048 «Использование информационно-телекоммуникационной сети «Интернет»; M049 «Использование средств мобильной связи»; M055 «Использование вредоносного программного обеспечения»; M057 «Использование компьютерной техники»; M059 «Использование программных средств (любое программное обеспечение, установленное на компьютере, смартфоне или иной технике)»; M060 «Использование фиктивных электронных платежей»; M072 «Создание вредоносного программного обеспечения»; M073 «Распространение вредоносного программного обеспечения»; M086 «Использование социальных сетей»; M087 «Использование интернет-мессенджеров»; M088 «Использование электронных платежных систем»; M089 «Операции с цифровой валютой»; M092 «Использование SIP-телефонии»; M094 «Неправомерный доступ к информации»; M095 «Операции с цифровыми финансовыми активами»; M126 «Использование сети даркнет»; M127 «Фишинговые сайты и ссылки»; M128 «Программы-шифровальщики»; M130 «Бот-сети (ботнеты)»; M131 «DDoS-атаки»; M132 «Использование технологии «дипфейк»; M133 «Компрометация банковских устройств самообслуживания»; M134 «Использование информационной инфраструктуры (зарубежных серверов (услуг

хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменных зон, телефонных сетей и т. п.) иностранного государства»; М135 «Использование информационной инфраструктуры стран-участников СНГ»;

- среда совершения преступления «Score»: «cyberspace» (киберпространство), «metaverse» (метасреда), «blockchain» (сеть блокчейн (распределенный реестр));

- средство совершения преступления «Means» – «PC» (персональный компьютер), «mobile» (мобильное устройство связи), «software» (программное обеспечение), «hardware» (аппаратное обеспечение), «malware» (вредоносное программное обеспечение), «webservice» (веб-ресурс), «system» (информационная система);

- цифровые следы преступления «Traces» – «IP» (IP-адрес), «MAC» (MAC-адрес), «IMEI» (IMEI-код), «phone number» (номер телефона), «e-mail» (электронная почта), «cookie» (файлы cookie), «browser history» (история браузера), «journals event logs» (журнал событий в системе), «transaction» (транзакция);

- расположение цифровых следов преступления «Trace_location» – «PC drive» (носитель информации компьютера), «mobile drive» (носитель информации мобильного устройства), «software» (программное обеспечение), «hardware» (аппаратное обеспечение), «flash drive» (носитель информации flash-диск), «cloud storage» (облачное хранилище), «external_storage» (внешний носитель информации), «RAM» (оперативная память), «log.txt» (лог-файлы), «config.sys» (файлы конфигурации), «database» (баз данных), «script.ps1» (файл сценария);

- способ сокрытия следов «Trace_hidden» – «VPN» (VPN-сервер), «Proxu» (прокси-сервер), «SIP» (SIP-телефония), «Tor» (Tor-маршрутизатор), «GSM» (GSM-шлюз);

- серийность преступления «Seriality» – «IP» (IP-адрес), «MAC» (MAC-адрес), «IMEI» (IMEI-код), «phone number» (номер телефона), «e-mail» (электронная почта);

- место совершения преступления «Place» – «home» (дом), «office» (служебное помещение), «public» (общественное место);

- дата совершения преступления «Date»;

- время совершения преступления «Time»;

– личность преступника [«Criminal_name» – идентификатор преступника (ID), «Criminal_age» – возраст преступника (лет), «Criminal_gender» – пол преступника (мужской, женский), «Criminal_edu» – образование преступника (без образования, среднее, среднее специальное, высшее), «Criminal_job» – род занятий преступника (безработный, специалист в области информационных технологий, учащийся, работник), «Criminal_court» – судимость преступника (да, нет)];

– личность потерпевшего [«Victim_name» – идентификатор потерпевшего (ID), «Victim_age» – возраст потерпевшего (лет), «Victim_gender» – пол потерпевшего (мужской, женский), «Victim_edu» – образование потерпевшего (без образования, среднее, среднее специальное, высшее), «Victim_job» – род занятий потерпевшего (безработный, специалист в области информационных технологий, учащийся, работник), «Victim_vulnerability» – предмет посягательства («PC» (персональный компьютер), «mobile» (мобильное устройство связи), «software» (программное обеспечение), «hardware» (аппаратное обеспечение), «websource» (веб-ресурс), «system» (информационная система), «Victim_damage» – ущерб потерпевшего (рублей)];

- техника совершения преступления «Txxxx»;
- подтехника совершения преступления «Sxxx»;
- меры выявления «Dxxxx»;
- меры реагирования «Rxxxx»;
- раскрытие преступления «Revealed» – (да, нет);
- алгоритм расследования «Algorithm» – (последовательность действий).