На правах рукописи

Харисова Зарина Ирековна

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ПРИКЛАДНЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Специальность 5.1.4. Уголовно-правовые науки

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора юридических наук

Уфа – 2025

Работа выполнена на кафедре криминалистики Института права федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий»

Научный консультант: **Макаренко Илона Анатольевна**,
доктор юридических наук, профессор

Официальные оппоненты: **Россинская Елена Рафаиловна**,
доктор юридических наук, профессор,
заслуженный деятель науки Российской Федерации,
заведующий кафедрой судебных экспертиз
федерального государственного автономного
образовательного учреждения высшего образования
«Московский государственный юридический
университет имени О.Е. Кутафина (МГЮА)»

Бессонов Алексей Александрович,
доктор юридических наук, доцент,
ректор федерального государственного казенного
образовательного учреждения высшего образования
«Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева»

Гаврилин Юрий Викторович,
доктор юридических наук, профессор,
начальник кафедры управления органами расследования
преступлений федерального государственного казенного
образовательного учреждения высшего образования
«Ордена Трудового Красного Знамени Академия
управления Министерства внутренних дел
Российской Федерации»

Ведущая организация: Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Воронежский государственный университет»,
г. Воронеж

Защита состоится 01 апреля 2026 г. в 10 ч. 00 мин. на заседании совета по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук 24.2.479.09, созданного на базе ФГБОУ ВО «Уфимский университет науки и технологий», по адресу: 450005, г. Уфа, ул. Достоевского, д. 131, ауд. 317.

С диссертацией можно ознакомиться в библиотеке и на официальном сайте ФГБОУ ВО «Уфимский университет науки и технологий» (https://uust.ru).

Автореферат разослан «____» _____ _____ года

Ученый секретарь
диссертационного совета
кандидат юридических наук, доцент  Гизатуллин Ирек Альфредович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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 технологий[1] (25,83 % от числа зарегистрированных за год), в аналогичном периоде аналитического отчета, сформированного по состоянию на 2024 год[2], 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

[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).

[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).

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 интеллекта[4] на период до 2030 г., которая предусматривает обеспечение национальных интересов страны и 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

---

[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).

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 активами[6]. Новый стек технологий для разработки 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 киберпреступности[7] 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.

---

[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).

[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).

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 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. Пузарина (2019), С. М. Голятиной (2020), А. М. Каминского (2020), Е. Р. Россинской (2021), А. А. Рудых (2020), О. П. Бердниковой (2021), Е. А. Русскевич (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. Нарижного (2009), Р. Р. Шарипова (2011), В. Ю. Агибалова (2012), Т. В. Аверьяновой (2013), Л. П. Зверянской (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. Глимейды (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 B. Carrier (США, 2005), S. Garfinkel (США, 2007), A. Reyes (США, 2007), P. Hunton (США, 2010), A. Khater (Катар, 2010), C. Hooper (Австралия, 2013), F. Iqbal (ОАЭ, 2013), W. Chang (Тайвань, 2014), C. 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 судебно-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 судебно-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.

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 следствие 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 IT-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 России[10].

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» (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

---

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

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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертационного исследования с учетом степени ее научной разработанности, определяются объект, предмет, цель, задачи, основная гипотеза и методология исследования, раскрывается его теоретическая, нормативная и эмпирическая основы, обосновывается научная новизна работы, формулируются положения, выносимые на защиту, раскрывается теоретическая и практическая значимость исследования, приводятся сведения о достоверности и обоснованности полученных результатов, их апробации и внедрении.

Первая глава «Преступления в сфере компьютерной информации как объект криминалистического исследования и моделирования, факторы их эволюции и трансформации» включает три параграфа.

В первом параграфе «Преступления в сфере компьютерной информации как объект криминалистического исследования» изложены результаты анализа понятийного аппарата и современных тенденций трансформации преступной деятельности в исследуемой области. Обосновано, что рассматриваемые преступления представляют собой особый вид преступной деятельности и единый объект криминалистического исследования, поскольку зачастую объединены единым подходом к способу подготовки преступления, его совершению и сокрытию следов, имеют специфику места и времени совершения, обусловленные схожей обстановкой.

Показано, что преступления в сфере компьютерной информации как объект криминалистического исследования во многом характеризуются средой совершения преступного деяния (киберпространством, метапространством, распределенным реестром или квантовой вычислительной средой), которая выступает носителем криминалистически значимой информации. Соответственно, метапреступления, а также иные вариации преступных деяний, определяемые средой их совершения, являются эволюционным видом рассматриваемых преступлений, требующих 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 вычислительные устройства – в качестве высокотехнологичных средств криминалистического обеспечения.

В свете рассмотрения теоретических основ расследования преступлений в сфере компьютерной информации отмечено, что 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.

На основе анализа 284 уголовных дел и 2500 приговоров, размещенных на официальных сайтах судов общей юрисдикции в сети «Интернет» по фактам совершения преступлений в соответствии со ст. ст. 272, 272.1, 273, 274, 274.1 Уголовного кодекса Российской Федерации (за исключением ст. ст. 274.2, 274.3, 274.4, 274.5 указанного кодекса, по которым на момент исследования отсутствовала судебно-следственная практика), а также с учетом результатов анкетирования сотрудников органов дознания, следствия и оперативных подразделений криминалистическую характеристику преступлений в сфере компьютерной информации предложено изложить в совокупности следующих 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.

Во втором параграфе «Криминалистическая модель преступлений в сфере компьютерной информации (структурно-содержательный анализ элементов криминалистической характеристики)» представлены результаты анализа элементов криминалистической характеристики рассматриваемых преступлений с точки зрения системно-структурного, а также кибернетического подходов. Обосновано, что надлежащее формирование системы исходных данных для криминалистической характеристики преступлений может расширить понимание механизма совершения соответствующих преступных деяний, создания алгоритмов их расследования, описания особенностей тактики наиболее характерных для расследования этих преступлений следственных действий.

Показано, что выделение элементов криминалистических характеристик преступлений 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 основой для структурирования обучающего набора данных (датасета), позволяющего получить более полную информационную модель преступного деяния, что, в свою очередь, будет способствовать формированию более точного алгоритма его расследования. Отмечено, что типовая криминалистическая характеристика преступления способствует установлению ретроспективной модели произошедшего события и позволяет оценивать полноту исходной информации о преступном деянии, определять признаки преступления, выдвигать 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 деяния, которые преимущественно являются программными.

В третьем параграфе «Генезис преступлений, совершаемых в сфере компьютерной информации, и их детерминанты» показано, что для выявления эффективных методик расследования рассматриваемых преступлений (как одних из наиболее эволюционно-трансформируемых с течением времени и развитием технологий видов преступных деяний), а также своевременного принятия предупреждающих мер необходимо объединение научных знаний с точки зрения структурно-содержательного и системно-исторического подходов. Так, использование системно-исторического подхода при исследовании генезиса преступлений, совершаемых в сфере компьютерной информации, позволило рассмотреть не только этапы его развития и современное состояние, но и 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.

Обосновано, что дальнейшая эволюция способов совершения преступлений в сфере компьютерной информации будет обусловлена: относительно легкой разработкой и внедрением вредоносных компьютерных сетей (ботнетов), в том числе на основе моделей искусственного интеллекта для совершения кибератак; применением квантовых алгоритмов для взлома защищенных систем; задействованием расширенных методов социальной инженерии, иммерсивного воздействия для манипуляции персональными данными граждан и пр.

Дуализм информационных технологий с точки зрения их интеграции в различные процессы подразумевает цифровизацию применяемых в криминалистике технико-криминалистических средств в целях раскрытия и расследования преступлений, совершаемых в цифровой среде, определяя так называемый четвертый этап развития криминалистики («Криминалистика 4.0»). В рамках формирующейся в настоящее время Индустрии 5.0, в свете возможности 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, предложен принципиально новый подход направления противодействия современной преступности, определяемый подходом «Криминалистика 5.0».

В совокупности основных способов получения новых знаний и методов решения задач в рамках обозначенного подхода выделены обнаружение, фиксация, изъятие и исследование цифровых доказательств, а также автоматизация процесса расследования и обеспечение целостности собранной информации, что, соответственно, позволяет определить ключевым для его реализации стек технологий Web 4.0 и Web 5.0, представленными совокупностью технологий искусственного интеллекта, распределенного реестра, сверхвысокой передачи данных 5G, Интернета вещей, а также виртуальной и дополненной реальности.

Вторая глава «Криминалистическое обеспечение расследования преступлений в сфере компьютерной информации и основы исследования цифровой информации» включает три параграфа.

В первом параграфе «Криминалистические средства расследования преступлений в сфере компьютерной информации» отмечено, что основой для распознавания способа совершения преступления в сфере компьютерной информации служит следовая картина в виде материальных цифровых следов, которые возможно идентифицировать исключительно с использованием технико-криминалистических средств. Обозначено, что разрыв между возможностями преступников и инструментами, доступными правоохранительным органам, подчеркивает необходимость адаптации правовых механизмов к динамической природе преступлений в сфере компьютерной информации, а сложность идентификации цифровых следов и собирания доказательственной базы требует совершенствования криминалистических методов и средств расследования. В этих целях была сформирована упрощенная модель этапов расследования преступных деяний рассматриваемого вида, в которой способ совершения преступления, как исходный вектор, влияет на тип оставляемых цифровых следов, а сами 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.

Отмечено, что технико-криминалистические средства включают в себя широкий круг аппаратных, программно-аппаратных и программных средств, которые могут быть классифицированы по различным основаниям (проведена их общая классификация 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, используемые для поиска и анализа цифровых доказательств, 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.

В результате исследования сделан вывод, что основа расследования преступлений в сфере компьютерной информации базируется на обнаружении, фиксации, изъятии и исследовании цифровых доказательств, осуществляемых с использованием технико-криминалистических средств в виде программного обеспечения.

Во втором параграфе «Роль программных технико-криминалистических средств при расследовании преступлений в сфере компьютерной информации» констатируется, 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. Делается вывод об индивидуальности указанных следов, определение которых возможно исключительно с применением цифровых инструментов, что обусловлено неприменимостью традиционных методов собирания доказательств к среде цифровых данных, кроме того, отмечается, что 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.

Проведенное исследование позволило сформулировать вывод о стратегическом значении программных технико-криминалистических средств в борьбе с преступностью в условиях цифровизации общества, которыми обеспечивается, во-первых, непосредственное обнаружение, фиксация, изъятие и исследование цифровых доказательств (за счет использования экспертных и поисковых систем), во-вторых, их верификация и проверка подлинности и сохранности, 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).

Обозначен предполагаемый вектор развития киберпреступности, заключающийся в использовании генеративных алгоритмов машинного обучения, соответственно, в целях расследования таких преступлений становится необходимым использование программных средств, способных 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 и т. п. Отмечается также, что определенную трудность будут представлять возможности квантовых компьютеров, способных взламывать современные криптографические алгоритмы, в противовес формируется предположение о выстраивании системы противодействия указанным угрозам в виде программных комплексов, способных работать с гибридными квантовыми алгоритмами (в том числе по взлому шифрования), сочетающими традиционные методы криптоанализа с вероятностными вычислениями квантовых устройств. Таким образом, только программные технико-криминалистических средства смогут эффективно бороться с атаками, управляемыми искусственным интеллектом, в будущем, что подчеркивает насущность их рассмотрения в настоящее время.

В третьем параграфе «Проблемы и пути совершенствования деятельности по собиранию, исследованию, оценке и использованию цифровых доказательств при расследовании преступлений в сфере компьютерной информации» приводятся тенденции, способствующие беспрецедентному росту преступлений в сфере компьютерной информации, противодействие которым до настоящего времени осложняется несовершенством процесса собирания, исследования, оценки и использования криминалистически значимой компьютерной информации, а также отсутствием необходимых технико-криминалистических средств. Отмечаются основные проблемы, возникающие при расследовании рассматриваемых преступлений, к которым относятся фрагментарность и изменчивость цифровой информации, возможность шифрования и анонимизации данных преступниками, разнообразие среды исследования и невозможность стандартизации процесса выявления доказательств.

Решение отмеченных проблем заключается в автоматизации указанных процессов путем использования программных технико-криминалистических средств, поскольку автоматическую классификацию и выявление 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.

Приведена совокупность принципов, позволяющих повысить эффективность расследования рассматриваемых преступлений, обеспечить юридическую и техническую состоятельность цифровых доказательств, а также усилить взаимодействие между государственными органами и частным сектором в борьбе с киберугрозами. Так, показано, что в целях соблюдения принципа целостности и аутентичности цифровых доказательств целесообразно придерживаться широко распространенного в настоящее время принципа хронологической документации, который сможет обеспечить фиксацию всех этапов работы с доказательством. Предотвратить утрату данных можно путем организации центров обработки данных на основе распределенных баз и массивов облачных, независимых дисковых данных с возможностью расчета контрольных сумм и контроля версий хранилищ, либо внедрения блокчейн-технологий с временными метками, что обеспечит неизменность данных и прозрачность процесса их хранения. При этом защиту цифровых доказательств от посягательств можно обеспечить использованием квантово-устойчивых алгоритмов шифрования, что является одним из перспективных направлений реализации подобных систем в будущем. Констатируется, что реализация выдвигаемых предложений позволит повысить эффективность расследования рассматриваемых преступных деяний, обеспечить юридическую и техническую состоятельность цифровых доказательств, а также усилить взаимодействие между государственными органами и частным сектором в борьбе с киберугрозами.

Отдельное внимание уделяется сложностям, возникающим при исследовании больших объемов цифровых данных в рамках расследования преступлений в сфере компьютерной информации. При этом, как правило, лишь малая часть из массивов анализируемых сведений может представлять собой криминалистически значимую информацию.

В подтверждение выводов, сделанных в двух предыдущих параграфах второй главы диссертационного исследования, констатируется возможность автоматизации процесса собирания и исследования цифровых доказательств с минимальными трудозатратами на основе интеллектуального программного обеспечения, при этом точность и прозрачность анализа данных смогут обеспечить самоинтерпретируемые модели (XAI-системы), способные объяснять принимаемые решения адаптированным для человека языком, что особенно важно для исключения проблем предвзятости алгоритмов.

Обосновано предложение о рациональности закрепления за следователем (дознавателем) права, но не обязанности привлечения специалиста при изъятии электронных носителей информации, исходя из собственных компетенций, так, 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 самостоятельно. Ввиду того, что обращение с простыми носителями информации является на сегодняшний день бытовым навыком целесообразным представляется дополнение ч. 2 ст. 164.1 Уголовно-процессуального кодекса Российской Федерации – «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».

Приводятся 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 развитии систем сертификации специалистов, задействованных в расследовании и раскрытии 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.

Третья глава «Основы расследования преступлений в сфере компьютерной информации и организационно-тактические особенности производства отдельных следственных действий» включает два параграфа.

В первом параграфе «Особенности возбуждения уголовных дел о преступлениях в сфере компьютерной информации» приведен анализ материалов судебно-следственной практики при изучении особенностей возбуждения уголовных дел о преступлениях в сфере компьютерной информации, который показал особую важность процедуры получения объяснений на стадии проверки сообщения о преступном деянии.

Отмечена сложность расследования рассматриваемых преступлений, которая зачастую объясняется бесперспективной практикой стохастического 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 технических возможностей.

Показано, что систематичность при планировании следственных действий может быть достигнута использованием заранее сформированного исходя из сложившейся практики расследования алгоритма действий. В связи с этим в ходе исследования была рассмотрена последовательность шагов в виде алгоритмов и их типичных вариаций, складывающихся на этапе возбуждения уголовного дела, которая была отражена на примере действующих в настоящее время алгоритмов действий следователей и дознавателей при проверке сообщений о преступлениях, совершаемых в сфере компьютерной информации.

Во втором параграфе «Организационно-тактические особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации» обоснован вывод о том, что 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.

Сделано заключение о том, что типовая следственная ситуация может обуславливать соответствующий ей типовой алгоритм расследования с выделением на каждом из этапов ряда ключевых признаков модели преступного деяния (ввиду наличия взаимосвязей между следственными ситуациями (характеризуются отсутствием информации о личности преступника и наличием информации о том или ином способе совершенного преступления) и алгоритмами расследования).

Четвертая глава «Организационные и методические основы алгоритмизации расследования преступлений в сфере компьютерной информации» включает три параграфа.

В первом параграфе «Соотношение следственных ситуаций и алгоритмов расследования преступлений в сфере компьютерной информации» приводятся результаты исследования, которые позволили выявить признаки, определяющие минимально необходимые элементы, входящие в материал проверки сообщения (заявления) о преступлении, а также в материалы первоначального и последующего этапов расследования, отмечено, что именно они могут быть заложены в основу информационно-компьютерной модели (цифрового двойника) преступного деяния, совершенного в сфере компьютерной информации. Формируется вывод о возможности аккумуляции вышеуказанных признаков в набор данных для определения наиболее подходящего и эффективного алгоритма его расследования, а также вероятности раскрытия смоделированного преступления.

Приведено определение алгоритма расследования, под которым понимается 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. Также аргументировано понятие программы расследования как совокупности описанных алгоритмов.

Проведенное исследование позволило определить структуру частной криминалистической методики расследования преступлений в сфере компьютерной информации, которую 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 преступления (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. Приводится заключение о том, что преступления в сфере компьютерной информации – это один из наиболее подходящих под критерий «оцифрованности» видов преступных деяний, позволяющих сформировать цифровой двойник преступления. Аргументируется позиция, согласно которой предложенный подход к формированию методик расследования преступлений возможно распространить и на другие родовые группы преступных деяний при условии аккумулирования знаний о типичных следственных ситуациях, совокупности элементов криминалистической характеристики преступления (типичных их признаках), а также имеющейся криминалистически значимой

информации, 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.

Во втором параграфе «Криминалистическое кодирование преступлений в сфере компьютерной информации и его роль в формировании типовых алгоритмов расследования» представлена идея о возможности формирования универсальной системы криминалистического кодирования преступлений в сфере компьютерной информации (в значении упорядочивания, как одного из видов работ в области инженерии знаний, присвоения криминальным актам уникальных кодов, однозначно идентифицирующих как распространенные в настоящее время, так и вновь появляющиеся средства и способы совершения рассматриваемых 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, после чего была представлена система присвоения им уникальных кодов, что нашло свое отражение в программном технико-криминалистическом средстве «КиберКодекс [CyberCodex] с кодификатором преступлений в сфере компьютерной информации»[11].

Предложенная система кодирования позволила заложить основу стандартизированного учета преступлений в сфере компьютерной информации, упрощающую процесс идентификации их составов. Отмечается, что теоретико-правовыми основами классификации и последующего кодирования преступлений в сфере компьютерной информации выступили три уровня: уровень норм, представленных статьями главы 28 Уголовного кодекса Российской Федерации «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, сформированный на базе матрицы угроз безопасности «Mitre Att&ck»[12], отражающий способы, используемые преступниками, а также возможности противодействия им. Результаты проведенного сопоставления рассматриваемых категорий преступлений техникам указанной матрицы позволили сформировать новую универсальную систему криминалистического кодирования преступлений, использование которой может выступить основой формирования методик их расследования в условиях эволюции способов совершения преступных деяний. В основе кодирования лежат

---

[11] 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.

[12] База данных угроз безопасности информации «Mitre Att&ck» // Некоммерческая организация «Mitre» : офиц. сайт. URL: https://attack.mitre.org (дата обращения: 22.10.2025).

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.

В третьем параграфе «Правовые, методические, организационные и технические основы применения типовых алгоритмов расследования преступлений в сфере компьютерной информации» обозначена особенность начальной стадии досудебного расследования рассматриваемого вида преступлений, которая заключается в том, что в условиях неочевидности преступного события она характеризуется выраженным дефицитом 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.

Отмечено, что 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.

Аргументирована позиция, согласно которой 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. Предложен 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.

Раскрывается обоснование принятия процесса получения объяснений в качестве отправной точки алгоритмизации процесса расследования преступлений в сфере компьютерной информации и процесса поддержки принятия решений по уголовному делу должностным лицом, а также исходя из анализа зарубежной практики приводится предложение о допустимости получения объяснений по факту совершения преступления и возможности их представления (в качестве альтернативной возможности) удаленно посредством сети «Интернет» по специально разработанной на основе интеллектуальных алгоритмов обработки данных форме, отражающей типичные следственные ситуации. Такой подход обосновывается тем, что он позволяет не только снизить временные затраты на процесс подачи заявления о преступном деянии, но и автоматизировать процесс

обработки криминалистически значимой информации.

Таким образом, характер инженерной разработки, направленной на создание программного обеспечения или интеллектуальной системы в рамках ситуационного моделирования, может определить возможность формирования алгоритмов, позволяющих на основе введенных 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 преступления, информации о механизме преступления, а также лицах его совершивших.

Пятая глава «Интеллектуализация процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности как основа развития теории информационно-компьютерного обеспечения криминалистической деятельности» включает три параграфа.

В первом параграфе «Концептуальные основы учения об интеллектуализации процесса расследования преступлений в сфере компьютерной информации и принятия решений в условиях неопределенности» отмечается, что снизить степень влияния факторов, затрудняющих процесс расследования преступлений в сфере компьютерной информации, в настоящее время можно 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 технологий искусственного интеллекта, направленных на интеллектуализацию процесса расследования, анализ больших объемов цифровых данных и выявление скрытых связей между событиями, что позволит повысить эффективность расследования рассматриваемого вида преступлений.

Обосновывается необходимость расширения предмета теории информационно-компьютерного обеспечения криминалистической деятельности с учетом современных вызовов и технологических реалий внесением ряда закономерностей (дополнений), обусловленных внедрением в практику расследования технологий искусственного интеллекта. С этой целью описываются закономерности, затрагивающие имеющиеся в указанной теории учения, по этой причине формулируется заключение о дополнении указанной теории учением 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.

Отмечается перспективное направление, объединяющее достижения квантовых вычислений и современных технологий, в том числе технологии искусственного интеллекта, для повышения эффективности расследования преступлений – квантовое криминалистическое обеспечение, которое стоит рассматривать как перспективу развития интеллектуализации процесса расследования преступлений.

Во втором параграфе «Концепция нейросетевого криминалистического кластера данных как основа систематизации криминалистически значимой компьютерной информации» 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.

Сделано заключение о том, что 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.

Изложенное дает основания предполагать, что криминалистика приобретает новые исследовательские и практико-ориентированные возможности благодаря применению современного стека индустрий Web 4.0 и Web 5.0 (в виде набора доступных в настоящее время и используемых инструментов или информационных технологий), 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.

В третьем параграфе «Цифровая криминалистическая модель преступления в сфере компьютерной информации (модель цифрового двойника преступления) на основе нейросетевого криминалистического кластера данных» на примере преступления в сфере компьютерной информации приводится определение цифрового двойника преступного деяния (виртуальная модель, отражающая состояние и динамику реального преступления в сфере компьютерной информации, позволяющая исследовать различные сценарии его совершения, выявлять закономерности между элементами его криминалистической характеристики, формировать алгоритм расследования преступного деяния, выдавать вероятность его раскрытия).

Подробно представлена эмпирическая база исследования, описаны исходные данные для построения модели в виде массива сведений из материалов уголовных дел, а также данных судебно-следственной практики, перечислены используемые для обучения системы переменные.

На основе сформированной модели разработано интеллектуальное программное технико-криминалистическое средство «Cybercrime DT Model (AI) – [Цифровой двойник киберпреступления]»[13], 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 раскрытия преступлений, среди которых способы сокрытия следов, предполагающие использование различных анонимизирующих средств и технологий, например, таких как «VPN», маскирующее программное обеспечение «Tor», SIP-телефония и пр., оказывали 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). Значимый вклад в прогноз вероятности раскрытия показал признак серийности, что особенно важно в связке с датой и временем совершения преступления (как положительный фактор), тогда как лишь наличие цифровых следов совершения преступного деяния и ряд сопутствующих признаков внесли сравнительно небольшой вклад. При этом была отмечена важность типа цифровых следов в виде уникальных идентификаторов, таких как MAC-адрес, IMEI-код и пр., наличие которых повышает вероятность раскрытия.

Проведенное исследование также показало, 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 оказалась вполне интерпретируема и согласована с экспертными и научными представлениями о преступлениях в сфере компьютерной информации.

Для выявления корреляционных зависимостей между переменными (элементами криминалистической характеристики преступления) сформированного набора данных были построены корреляционные матрицы, которые наглядно показали сильные и умеренные корреляции между переменными.

Таким образом, было доказано, что корреляционная матрица может использоваться для отбора значимых признаков и выявления скрытых закономерностей между данными.

---

[13] 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.

Графическое представление связей между преступными деяниями обеспечило использование графовых сетей, так, были выявлены признаки, объединяющие раскрытые преступления в том или ином отдельном кластере, а также показано, что определенные виды преступлений (преимущественно высокотехнологичные) труднее раскрывать или необходимо их расследовать с задействованием уникальных методик.

Кроме того, аналитическая интерпретация графа раскрываемости преступлений позволила также интерпретировать подходы к раскрытию преступлений.

Анализ данных показал, что 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 иных дел.

Таким образом, графовая криминалистическая модель позволила не только визуализировать структуру преступлений, но и выявить закономерности, связанные с их раскрытием. Сделан вывод о том, что 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.

В заключении формулируются основные выводы и обобщения по итогам диссертационного исследования, отмечается теоретическое и прикладное значение полученных сведений.

В приложениях представлены дополняющие текст диссертации данные, демонстрирующие ход исследования и подтверждающие основные положения и выводы, а также аналитические сведения, полученные в ходе проведенной работы.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ АВТОРА

Статьи, опубликованные в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации

1. Харисова, З. И. Криминалистическая модель нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей / З. И. Харисова // Философия права. – 2025. – № 2 (113). – С. 180–187.

2. 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.

3. 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.

4. 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.

5. 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. – С. 116–125.

6. 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.

7. 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(26). – С. 205–221.

8. 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.

9. 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.

10. Харисова, З. И. Информационно-компьютерная криминалистическая модель преступления в сфере компьютерной информации на примере неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / З. И. Харисова // Право и государство: теория и практика. – 2025. – № 9. – С. 509–512.

11. 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.

12. 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.

13. Харисова, З. И. Криминалистическая кодификация преступлений в сфере компьютерной информации и ее роль в унификации процесса расследования / З. И. Харисова // Вестник Санкт-Петербургского университета МВД России. – 2025. – № 4 (108). – С. 164–172.

14. Харисова, З. И. О структурных элементах криминалистической характеристики преступлений в сфере компьютерной информации / З. И. Харисова // Журнал прикладных исследований. – 2025. – № 9. – С. 199–203.

15. 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.

16. Харисова, З. И. Обеспечение прав и свобод гражданина в области использования цифровых финансовых активов / З. И. Харисова, А. Р. Лонщакова // Евразийский юридический журнал. – 2020. – № 3(142). – С. 167–168.

17. 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.

18. Харисова, З. И. Обеспечение достоверности и информационной безопасности проведения психофизиологических исследований в рамках уголовного судопроизводства в Российской Федерации и за рубежом / А. Р. Лонщакова, З. И. Харисова, В. В. Антонов // Евразийский юридический журнал. – 2019. – № 9(136). – С. 240–242.

Статьи, опубликованные в рецензируемых научных изданиях и журналах, включенных в индексируемой базе данных Web of Science

19. Model of a domain-specific profiling system based on Explainable AI technologies / V. V. Antonov, Z. I. Kharisova, L. E. Rodionova, G. G. Kulikov // IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1069. – № 12001. – P. 1–10.

20. Modeling problems legal regulation of the field of artificial intelligence / V. V. Antonov, Z. I. Kharisova, N. R. Kalimullin, A. I. Abdulnagimov // IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1069. – № 12002. – P. 1–7.

Учебные издания и иные пособия

21. Харисова, З. И. Международно-правовые аспекты обеспечения информационной безопасности в сети интернет : учебное пособие / В. В. Антонов, З. И. Харисова, В. А. Колесников. – Уфа : Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2021. – 48 с.

22. Харисова, З. И. Особенности информационного обеспечения профессиональной деятельности в органах внутренних дел : учебное пособие / В. В. Антонов, З. И. Харисова, В. Р. Гурьянова [и др.]. – Уфа : Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2022. – 48 с.

23. Харисова, З. И. Информационные технологии в управлении органами внутренних дел / В. В. Антонов, З. И. Харисова, Н. Р. Калимуллин [и др.] : учебное пособие. – Уфа : Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2022. – 48 с.

24. Харисова, З. И. Противодействие преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий: отдельные аспекты : учебное пособие / В. Р. Гурьянова, Г. А. Тугузбаев, З. И. Харисова [и др.]. – Уфа : Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2023. – 48 с.

25. Харисова, З. И. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, В. Р. Гайнельзянова, З. И. Харисова [и др.]. – Уфа : Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2023. – 96 с.

26. Харисова, З. И. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, В. Р. Гайнельзянова, З. И. Харисова [и др.]. – 2-е изд., перераб. и доп. – М. : – ГУРЛС МВД России, 2024. – 112 с.

27. Харисова, З. И. Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : практикум / Э. Д. Нугаева, З. И. Харисова, В. А. Суворова [и др.]. Уфимск. гос. авиац. техн. ун-т. – Уфа : УГАТУ, 2022. – 56 с.

28. Харисова, З. И. Тактика производства отдельных следственных действий по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : научно-практическое пособие / Э. Д. Нугаева, З. И. Харисова, А. Л. Арипов. − Уфа : Уфимский ЮИ МВД России, 2023. – 96 с.

29. Харисова, З. И. Тактика применения средств видеофиксации при производстве следственных действий : учебно-методическое пособие / Э. Д. Нугаева, З. И. Харисова, С. А. Рябчиков [и др.]. – Уфа : Уфимский ЮИ МВД России, 2024. – 80 с.

30. Харисова, З. И. Тактика производства отдельных видов осмотра при расследовании преступлений, совершенных с использованием информационных технологий : мультимедийное учебное издание / Э. Д. Нугаева, З. И. Харисова, А. Ю. Самойлов. − Уфа : Уфимский ЮИ МВД России, 2024. 700 мБ.

31. Харисова, З. И. Производство осмотра компьютерной техники и мобильных устройств при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий : мультимедийное учебное издание / Э. Д. Нугаева, З. И. Харисова. − Уфа : Уфимский ЮИ МВД России, 2025. 700 мБ.

Статьи, опубликованные в иных научных журналах и изданиях

32. Харисова, З. И. Международно-правовые основы информационной безопасности в целях устойчивого развития / З. И. Харисова // Правовое обеспечение развития социального государства в свете целей устойчивого развития : материалы Международной научно-практической конференции. Ч. 2. – Уфа : Башкирский государственный университет, 2018. – С. 103–106.

33. 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.

34. 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.

35. Харисова, З. И. Взаимодействие информационных потоков с наукой, бизнесом и технологиями как основной фактор анагенеза / З. И. Харисова, Д. И. Дорошенко // Социальные технологии работы с молодежью в условиях становления цифрового общества : материалы IV Международной научно-практической конференции. – Уфа: Башкирский государственный университет, 2019. – С. 305–308.

36. 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 : материалы Международной научно-практической конференции. – Уфа: Башкирский государственный университет, 2019. – С. 256–263.

37. Харисова, З. И. О перспективах перехода органов внутренних дел на отечественное программное обеспечение в рамках импортозамещения / З. И. Харисова, А. А. Катьянова // Организация Объединенных Наций и глобальные проблемы человечества в XXI веке : материалы Международной научно-практической конференции. – Уфа: Башкирский государственный университет, 2019. – С. 250–256.

38. Харисова, З. И. Право международной безопасности: современное состояние и тенденции развития / О. А. Филиппов, З. И. Харисова // Вестник Института права Башкирского государственного университета. – 2020. – № 1(5). – С. 46–50.

39. Харисова, З. И. Верификация информации при управлении социальными системами / Н. Р. Калимуллин, З. И. Харисова// Общественная безопасность, законность и правопорядок в III тысячелетии. – 2020. – № 6-2. – С. 169–173.

40. 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 в XXI веке. – 2020. – Т. 12, № 1. – С. 282–287.

41. Харисова, З. И. Искусственный интеллект в государственном управлении / З. И. Харисова, О. А. Филиппов, Д. А. Федоров // Информационные технологии интеллектуальной поддержки принятия решений (ITTDS'2020) : материалы VIII Всероссийской научной конференции. – Уфа: ФГБОУ ВО УГАТУ, 2020. – С. 26–29.

42. Харисова, З. И. 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.

43. Харисова, З. И. Проблемы правового регулирования сферы искусственного интеллекта / В. В. Антонов, Н. Р. Калимуллин, З. И. Харисова [и др.] // Информационные технологии интеллектуальной поддержки принятия решений (ITTDS'2020) : материалы VIII Всероссийской научной конференции (с приглашением зарубежных ученых). В 2-х томах, Уфа. Том 1. – Уфа: ФГБОУ ВО УГАТУ, 2020. – С. 10–14.

44. Харисова, З. И. Особенности обеспечения прав и свобод гражданина в области использования цифровых финансовых активов / З. И. Харисова, А. Р. Лонщакова // Современные проблемы уголовного процесса: пути решения : материалы Международной научно-практической конференции. – Уфа : Уфимский ЮИ МВД России, 2020. – С. 201–204.

45. Харисова, З. И. Отдельные проблемы процессуальных решений и тактические ошибки при осуществлении мер безопасности (на примере раскрытия и расследования насильственных преступлений) / А. Р. Лонщакова, З. И. Харисова // Актуальные проблемы деятельности органов внутренних дел по обеспечению безопасности лиц, подлежащих государственной защите. – Уфа: Уфимский ЮИ МВД России, 2020. – С. 94–97.

46. Харисова, З. И. Модель предметно-ориентированной системы профайлинга на основе объяснимого искусственного интеллекта / В. В. Антонов, Л. Е. Родионова, З. И. Харисова [и др.] // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации : материалы II Всероссийской научной конференции. – Ставрополь: Северо-Кавказский федеральный университет, 2020. – С. 84–91.

47. Харисова, З. И. Защита электронных ресурсов от несанкционированного доступа в информационных системах образовательных учреждений / З. И. Харисова, А. Ф. Острякова // Современные цифровые технологии в деятельности образовательных организаций силовых ведомств: концепция, практика, инновации : материалы Международной научно-практической конференции. – Уфа: Уфимский ЮИ МВД России, 2020. – С. 79–81.

48. Харисова, З. И. Отдельные инструменты работы с криминалистически значимой информацией / А. Р. Лонщакова, З. И. Харисова // Теория и практика расследования преступлений : материалы VIII Международной научно-практической конференции, Краснодар. – Краснодар: Краснодарский университет МВД России, 2020. – С. 236–240.

49. Харисова, З. И. Особенности обеспечения прав и свобод гражданина в области использования цифровых финансовых активов / З. И. Харисова, А. Р. Лонщакова // Современные проблемы уголовного процесса: пути решения : материалы Международной научно-практической конференции. – Уфа: Уфимский ЮИ МВД России, 2020. – С. 201–204.

50. 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 : материалы Всероссийской научной конференции. – Москва: МОСУ МВД России им. В.Я. Кикотя, 2020. – С. 163–165.

51. Харисова, З. И. Моделирование проблем правового регулирования сферы искусственного интеллекта / В. В. Антонов, З. И. Харисова, Н. Р. Калимуллин // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации : материалы II Всероссийской научной конференции (с приглашением зарубежных ученых), Ставрополь. – Ставрополь: Северо-Кавказский федеральный университет, 2020. – С. 100–104.

52. 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. – Краснодар: Краснодарский университет МВД России, 2022. – С. 548–552.

53. Харисова, З. И. Изъятие криминалистически важной информации с мобильных средств связи в рамках расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий / З. И. Харисова, О. А. Филиппов, Э. Д. Нугаева // Вестник Института права Башкирского государственного университета. – 2023. – № 1(17). – С. 57–64.

54. Харисова, З. И. Возможности применения средств видеофиксации с обработкой данных на основе искусственного интеллекта при производстве следственных действий / 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.

55. Харисова, З. И. Возможности применения средств видеофиксации с обработкой данных на основе искусственного интеллекта при производстве следственных действий / Д. С. Алексеева, В. В. Антонов, З. И. Харисова // материалы IV Международной научной конференции. – Екатеринбург: Институт цифровой экономики и права, 2023. – С. 374–380.

56. Харисова, З. И. О мерах, направленных на противодействие преступлениям, совершаемым с использованием криптовалют, в условиях становления криптопроцессинга в Российской Федерации / Э. Д. Нугаева, З. И. Харисова // Актуальные проблемы раскрытия и расследования преступлений

: материалы Международной научно-практической конференции. – Екатеринбург : Уральский юридический институт Министерства внутренних дел Российской Федерации, 2023. – С. 54–68.

57. Харисова, З. И. Основы обеспечения информационной безопасности в глобальной сети Интернет / З. И. Харисова, А. Н. Елизарьев, А. С. Ишмеева // Инновационная экономика: информация, аналитика, прогнозы. – 2024. – № 2. – С. 177–182.

58. Харисова, З. И. Метод формализации процесса исследования взаимозаменяемости программных продуктов с применением принципов системного анализа и аппарата категорного анализа логики в рамках импортозамещения зарубежного программного обеспечения на примере систем роботизации бизнес-процессов / В. В. Антонов, Н. А. Кононов, З. И. Харисова // материалы IV Международной научной конференции. – Екатеринбург: Институт цифровой экономики и права, 2023. – С. 359–366.

59. Харисова, З. И. О некоторых особенностях проведения доследственной проверки фактов незаконного сбыта наркотических средств, психотропных веществ, совершенных дистанционным способом / Э. Д. Нугаева, З. И. Харисова // Криминалистика: актуальные вопросы теории и практики : материалы Международной научно-практической конференции. – Ростов-на-Дону : РЮИ МВД России, 2023. – С. 148–154.

60. 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 : Волгоградская академия МВД России, 2023. – С. 103–105.

61. Харисова, З. И. О возможностях анализа метаданных при расследовании киберпреступлений в программном комплексе «Metadax» / 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.

62. Харисова, З. И. О возможностях собирания и нейросетевого исследования цифровых доказательств при расследовании преступлений в сфере компьютерной информации / И. А. Макаренко, З. И. Харисова // Проблемы криминалистической науки и экспертной практики : сборник научных трудов. – Омск: Омская академия МВД России, 2025. – С. 34–36.

63. Харисова, З. И. О применении гибридных моделей анализа электронных доказательств при расследовании преступлений в сфере компьютерной информации / З. И. Харисова // Высокотехнологичное право: ожидание и реальность : материалы Международной научной конференции. – Москва : Московский институт электронной техники, 2025. – С. 196–205.

64. Харисова, З. И. Об опыте подготовки квалифицированных кадров, специализирующихся на борьбе с киберпреступностью / Э. Д. Нугаева, З. И. Харисова // Итоги учебно-методической деятельности и перспективы развития образовательной среды Уфимского ЮИ МВД России: сборник материалов учебно-методического сбора профессорско-преподавательского состава. – Уфа: Уфимский ЮИ МВД России, 2025. – С. 99–103.

65. Харисова, З. И. О практико-ориентированном подходе обучения сотрудников органов внутренних дел, специализирующихся на борьбе с киберпреступностью / Э. Д. Нугаева, З. И. Харисова // Педагогический диалог. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2025. – № 4. – 172 с. – С. 58–63.

66. Харисова, З. И. Виртуальный тренировочный комплекс «Киберполигон» / З. И. Харисова // Актуальные вопросы расследования преступлений в условиях развития цифровых технологий : материалы Всероссийской научной конференции. – Уфа: Уфимский ЮИ МВД России, 2025. – С. 181–186.

67. Харисова, З. И. О технико-криминалистических средствах, применяемых при расследовании преступлений в сфере компьютерной информации / И. А. Макаренко, З. И. Харисова // Проблемы и перспективы развития предварительного следствия в России : материалы Всероссийской научно-практической конференции. – Волгоград: Волгоградская академия Министерства внутренних дел Российской Федерации, 2025. – С. 32–35.

68. 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.

69. Харисова, З. И. Вовлечение несовершеннолетних в совершение киберпреступлений и антиобщественных действий: современные техники и тенденции / И. А. Макаренко, З. И. Харисова // Криминалистика : вчера, сегодня завтра : материалы Международной научно-практической конференции, посвященной 75-летию со дня образования кафедры криминалистики Юридического факультета МГУ имени М. В. Ломоносова. – Москва: МГУ имени М. В. Ломоносова, 2025. – С. 144–150.

70. Харисова, З. И. Программное технико-криминалистическое средство для расследования преступлений в сфере компьютерной информации на основе искусственного интеллекта / З. И. Харисова // Актуальные проблемы использования специальных знаний в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях : материалы XIV научно-практической конференции. – Уфа: АНО «Право будущего», 2025. – С. 180–184.

Свидетельства о государственной регистрации программы для ЭВМ

71. 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. Лонщакова.

72. 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.

73. 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.

74. 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.

75. 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.

76. 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.

77. 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.

78. 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.

79. 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.

80. 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.

81. 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.

82. 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.