Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

На правах рукописи

Абрамова Таисия Вячеславовна

ОБНАРУЖЕНИЕ АНОМАЛИЙ И НЕЙТРАЛИЗАЦИЯ УГРОЗ В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ НА ОСНОВЕ МОНИТОРИНГА СЕТЕВЫХ ИНФОРМАЦИОННЫХ ПОТОКОВ

Специальность 2.3.6. Методы и системы защиты информации,
информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук, профессор
Аралбаев Ташбулат Захарович

Оренбург – 2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы. Одним из основных факторов повышения эффективности производства является обеспечение работоспособности и оптимальных технологических режимов работы промышленных объектов информатизации (ОИ), в частности, автоматизированных систем управления технологическими процессами (АСУ ТП). Качество функционирования АСУ ТП в условиях роста числа вредоносных воздействий и атак определяется эффективностью систем защиты информации (СЗИ). Специфика топологии распределенных АСУ, динамика изменения их состояний, условия их эксплуатации создают сложность организации СЗИ.

Согласно данным сайта RISI Online Incident Database и статистики «Лаборатория Касперского» в 2015 - 2023 гг наблюдается рост числа инцидентов информационной безопасности (ИБ) в промышленных автоматизированных системах (АС). Примечательно, что более 80% ущерба наносят инциденты, связанные с вредоносными программами, нерегламентированными действиями персонала системы, потерей связи между подсистемами АСУ. Рост числа инцидентов ИБ и появление новых требований к СЗИ обуславливают необходимость совершенствования существующих средств защиты информации в АСУ, обеспечивающих своевременное обнаружение аномалий и нейтрализацию угроз безопасности информации (БИ). Особую актуальность на современном этапе приобретает проблема разработки методов и средств защиты информации в компьютерных сетях (КС) АСУ ТП транспортировки нефтегазового сырья, являющихся одним из лидеров по числу инцидентов ИБ и относящихся к объектам критической информационной инфраструктуры (КИИ).

Степень проработанности темы. Вопросы построения систем обеспечения безопасного функционирования распределенных объектов информатизации широко освещены в современной нормативной, научной, технической и патентной литературе. Среди работ по данной тематике следует отметить труды Ажмухамедова И.М., Аралбаева Т.З., Васильева В.И., Вульфина А.М., Гетьмана А.И., Котенко И.В., Маркина Ю.В., Машкиной И.В., Остапенко А.Г., Саенко И.Б.., Соко-

лова А.Н., Тимофеева А.В., Фрида А.И., Чечулина А.А., Knapp E.D., Langill J.T.. Вопросам защиты информации в КС объектов КИИ посвящены стандарты ГОСТ Р серии 27000, ГОСТ Р серии 62443, Приказы ФСТЭК России №№ 31, 235, 239.

Анализ публикаций и решений задачи исследования показал, что, несмотря на значительные достижения в области обеспечения ИБ в промышленных АС, существующие методы и средства обнаружения аномалий и нейтрализации угроз недостаточно полно учитывают специфику КС АСУ ТП: их территориальную распределенность; переменный в пространстве и времени характер угроз; необходимость анализа значительного объема сетевого трафика (СТ) как корпоративного сегмента, так и сегмента промышленной сети, использующего специализированные программное обеспечение и сетевые протоколы; повышенные требования к оперативности и достоверности средств защиты в условиях ограниченных вычислительных ресурсов.

В частности, поведенческие методы обладают высокой адаптивностью к новым видам атак, однако недостаточно достоверны при обнаружении распределенной в пространстве и времени аномалии. Методы на основе знаний характеризуются высокой достоверностью, но сложны в реализации и неэффективны при обнаружении неизвестных видов атак. Методы интеллектуального анализа данных и машинного обучения, обладают высокой точностью и позволяют оперативно выявлять неизвестные виды атак, но требуют больших объемов размеченных данных для обучения. Необходимость своевременного обнаружения аномалий и достоверной идентификации соответствующих угроз БИ, как проявлений инцидентов ИБ, обуславливает актуальность совершенствования существующих СЗИ и разработки новых высокопроизводительных и достоверных средств защиты, с учетом современных требований.

Объект исследования – системы защиты информации в распределенных промышленных сетях на примере компьютерных сетей АСУ ТП транспортировки нефтегазового сырья.

Предмет исследования – методы и средства обнаружения аномалий и нейтрализации угроз в КС распределенных АСУ промышленными объектами.

Цель работы – снижение рисков ИБ в КС распределенных АС на основе повышения достоверности и производительности методов и средств обнаружения аномалий и нейтрализации угроз безопасности информации.

Задачи исследования:

1. Анализ современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой на примере КС АСУ ТП транспортировки нефтегазового сырья.

2. Разработка метода кластеризации угроз и моделей угроз БИ для подсистем распределенных объектов КИИ на примере АСУ ТП транспортировки нефтегазового сырья.

3. Разработка метода построения математических и имитационных моделей для обнаружения аномалий и нейтрализации угроз БИ на основе данных мониторинга сетевого трафика распределенных автоматизированных систем.

4. Разработка алгоритмов, методик и программной реализации методов и средств обнаружения аномалий и нейтрализации угроз в КС распределенных автоматизированных систем.

5. Экспериментальная оценка эффективности результатов исследований и разработка рекомендаций их практического применения в распределенных АС на примере АСУ ТП транспортировки нефтегазового сырья.

Научную новизну работы составляют:

1. Метод матричной кластеризации угроз и моделей угроз (МУ) на основе статистической обработки значений рисков, отличающийся тем, что в качестве исходных данных для кластеризации используются ортогональные средние значения рисков по угрозам и МУ, формализующий описание угроз и МУ в виде вектора бинарных классификационных кодов, что позволяет оценивать степени актуальности угроз, приоритетности их нейтрализации и определять характер изменения угрозы на последовательности подсистем распределенной АСУ ТП, а также применять принципы типового проектирования при построении СЗИ для АСУ с распределенной топологией.

2. Метод построения математических и имитационных моделей для обна-

ружения аномалий и распознавания состояния КС АСУ на основе данных мониторинга сетевого трафика, отличающийся использованием дихотомического принципа разделения исследуемого множества состояний сетевого трафика на нормальные и аномальные на основе разделяющей функции мажоритарного вида, аргументами которой являются бинаризированные амплитудные оценки информативных гармоник спектров временных рядов сетевого трафика, позволяющий повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз в КС АС.

3. Алгоритмы, методики и программная реализация методов и средств идентификации источников и маршрутов распространения вредоносного кода, определения резервных маршрутов передачи данных в промышленной КС, мониторинга действий персонала АС, отличающиеся тем, что в основу работы средств защиты положены принципы построения ассоциативных процессоров, в которых адресная часть запоминающих блоков соответствует контролируемым признакам аномалий, информационная часть – характеристикам исследуемых образов, а структура и архитектура арифметико-логических блоков определяется назначением этих средств, в частности, для принятия решения по мажоритарному принципу, что позволяет повысить производительность, достоверность, универсальность средств и снизить риски от угроз БИ. Новизна ассоциативного устройства мониторинга действий персонала АС подтверждена патентом на изобретение.

Теоретическая значимость. Предложенные результаты расширяют методологию построения СЗИ КС распределенных АСУ с использованием усовершенствованных моделей и алгоритмов кластерного описания угроз и развития методов защиты информации на основе дихотомического и ассоциативно-мажоритарного подходов с применением интеллектуальной обработки данных сетевого трафика.

Практическая значимость и реализация результатов работы заключается в разработке научно обоснованных методов и средств, позволяющих снизить риски от угроз БИ в распределенных АС, в частности: от угрозы распространения вредоносного кода в КС; от угрозы несанкционированных действий персонала

АСУ не менее чем в 2 раза; риск потери информации о состоянии объекта защиты не менее чем на 14%. Разработанное программное обеспечение передано для внедрения в ООО «Уральский центр систем безопасности», ООО «Газпромнефть-Оренбург», используется в учебном процессе ФГБОУ ВО «Оренбургский государственный университет», АНО ДО «Просвещение» (г. Оренбург).

Методы исследования. Использованы методы теории информационной безопасности, теории вероятности, теории принятия решений, теории распознавания образов, теории графов, методы математического, имитационного моделирования.

Положения, выносимые на защиту:

1. Метод матричной кластеризации угроз и моделей угроз распределенной АС на основе ортогональных средних значений рисков по угрозам и МУ для сопоставления актуальных угроз, приоритетности их нейтрализации и определения характера изменения актуальности угроз на последовательности подсистем распределенной АСУ ТП.

2. Метод построения математических и имитационных моделей для обнаружения аномалий, распознавания состояний КС АСУ на основе дихотомического принципа и разделяющей функции мажоритарного вида с бинарными амплитудными оценками информативных гармоник спектров временных рядов сетевого трафика.

3. Алгоритмы, методики и программная реализация методов и средств обнаружения аномалий и нейтрализации угроз по данным сетевого трафика на основе принципов построения ассоциативных процессоров в подсистемах сетевой защиты, учета действий персонала и защиты доступности технологической информации.

4. Результаты оценки эффективности диссертационных исследований и рекомендации по их практическому применению в распределенных АС.

Достоверность результатов исследований подтверждена их апробацией в процессе проведения экспериментов с использованием разработанных программных средств, программного комплекса SCADA TRACE MODE и эмуляторов про-

мышленного сетевого протокола ModBus TCP, апробацией на научных конференциях, публикацией результатов в ведущих рецензируемых научных изданиях.

Апробация результатов. Основные положения и результаты работы докладывались и обсуждались на международных и всероссийских научно-практических конференциях «Информационное противодействие угрозам терроризма» (г. Таганрог, 2015), «Компьютерная интеграция производства и ИПИ-технологии» (г. Оренбург, 2015), «Безопасность: Информация, Техника, Управление» и «Вопросы развития современной науки и практики в период становления цифровой экономики» (г. Санкт-Петербург, 2018), «Инновационные, информационные и коммуникационные технологии» (г. Сочи, 2018-2020), «Science in the modern information society XIX» (г. Моррисвиль, 2019), « «Технологические инновации и научные открытия», «Fundamental science and technology» (г. Уфа, 2023).

Научные результаты получены при проведении работ в рамках гранта РФФИ и правительства Оренбургской области № 18-47-560012.

Соответствие паспорту специальности. Результаты диссертационной работы соответствуют следующим пунктам паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»: п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»; п. 5 «Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет»; п. 6 «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях»; п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Личный вклад автора. Все основные результаты – методы, модели, алгоритмы и методики, представленные в работе, разработаны автором лично в процессе научной деятельности. Монография, программные продукты и устройство

разработаны в соавторстве при проведении научных работ в рамках гранта РФФИ.

Публикации. По материалам исследования опубликовано 43 работы, в том числе 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 1 научная работа в издании, включенном в базу Scopus, 26 статей в других изданиях, 1 коллективная монография, 1 учебно-методическое пособие. Получен 1 патент и 9 свидетельств о регистрации программ.

Структура и объем диссертации. Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованных источников и приложений. Работа изложена на 235 страницах, в том числе: основной текст на 195 страницах, 32 таблицы, 73 рисунка, список использованных источников из 205 наименований, 8 приложений на 40 страницах.

Первая глава посвящена анализу современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой на примере КС АСУ ТП транспортировки нефтегазового сырья. Вторая глава посвящена вопросам разработки метода кластеризации угроз и моделей угроз БИ для подсистем распределенных объектов КИИ, метода построения математических и имитационных моделей и модельного базиса задачи обнаружения аномалий и нейтрализации угроз БИ на основе данных сетевого трафика распределенных АС. В третьей главе представлены результаты разработки алгоритмов, методик и программной реализации методов и средств обнаружения аномалий и нейтрализации угроз в КС распределенных автоматизированных систем. Четвертая глава посвящена экспериментальной оценке эффективности результатов исследований и разработке рекомендаций их практического применения в распределенных АС на примере АСУ ТП транспортировки нефтегазового сырья. В заключении приведены основные результаты и выводы по работе.

Приложения содержат акты о внедрении результатов работы, результаты вычислительных и натурных экспериментов, многоаспектного анализа предложенных в работе решений, фрагменты листингов программных средств, справку о получении грантов.

ГЛАВА 1. АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ОБНАРУЖЕНИЯ АНОМАЛИЙ И НЕЙТРАЛИЗАЦИИ УГРОЗ БИ НА ОБЪЕКТАХ КИИ С РАСПРЕДЕЛЕННОЙ АРХИТЕКТУРОЙ

1.1 Актуальность задачи обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой

В условиях цифрового развития экономики и увеличения числа атак на промышленные объекты информатизации вопросы защиты информации в промышленных АС требуют повышенного внимания. Особую актуальность на современном этапе приобретает проблема разработки методов и средств защиты информации в КС автоматизированных систем сложных промышленных объектов. К данному классу объектов относятся, в частности, АСУ ТП транспортировки нефтегазового сырья.

Объектом исследования в работе являются системы защиты информации в распределенных промышленных сетях на примере КС АСУ ТП транспортировки нефтегазового сырья. Согласно Федеральному закону [127] и нормативным документам ФСТЭК РФ [149, 151, 156], рассматриваемые в работе АСУ относятся к объектам критической информационной инфраструктуры (КИИ) и имеют особое значение для экономики и национальной безопасности Российской Федерации.

Согласно данным статистики [157] в 2015-2023 гг. инциденты информационной безопасности составили более 65% от всех инцидентов в нефтегазовой отрасли, являющейся лидером по числу критических уязвимостей в АСУ. Статистика инцидентов ИБ по данным сайта базы RISI - The Repository of Industrial Security Incidents [157] и Федеральной службы по экологическому, технологическому и атомному надзору [71] представлена на рисунке 1.1.

Оренбургская область является одним из ведущих нефтегазоносных регионов России. Общая протяженность транспортных трубопроводов Оренбуржья со-

ставляет более 9000 км. По данным Ростехнадзора в 2020 - 2022 гг отмечался повышенный уровень аварийности на объектах нефтегазового комплекса Оренбургской области.

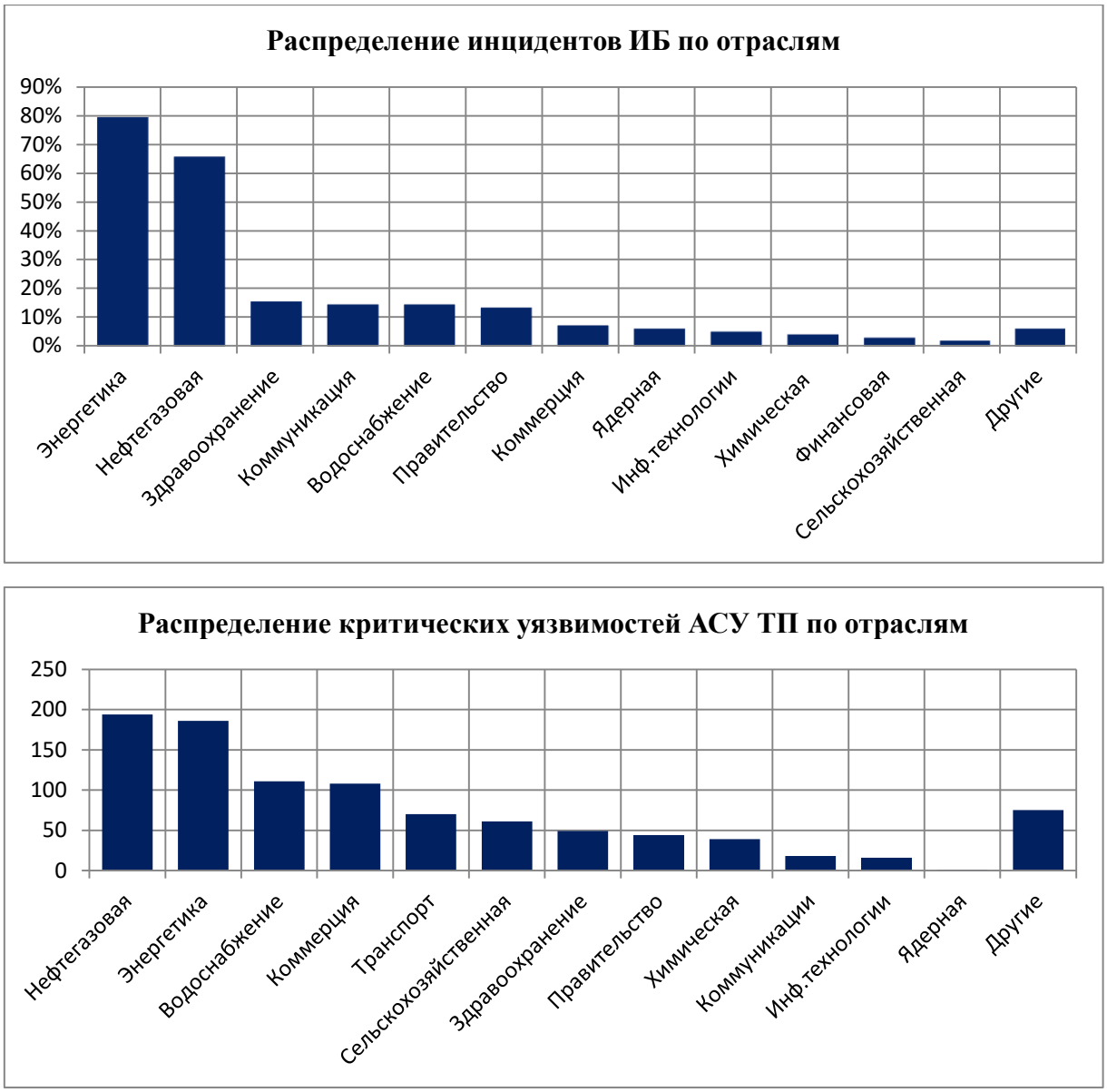


Рисунок 1.1 – Статистика инцидентов информационной безопасности на промышленных объектах за 2015 - 2023 гг.

Согласно исследованиям, проведенным лабораторией Касперского [115], АО «InfoWatch» [166] и компанией и «ООО «Атом Безопасность» [205], основными причинами инцидентов ИБ в АСУ являются атаки на сетевую инфраструктуру системы и вредоносное программное обеспечение - более 50% от всех инцидентов ИБ. Вторыми по значимости остаются ошибки и нерегламентированные

действия персонала системы - около 30%. Значительный ущерб наносят инциденты, связанные с потерей связи между территориально распределенными узлами АСУ - около 19%.

Особенностью построения СЗИ в АСУ является тот факт, что угрозы информационным ресурсам при их реализации непосредственно связаны с нарушениями в режимах работы систем, приводящими к аномалиям. Согласно источнику [30], «аномалия - отклонение от нормы, от общей закономерности». Аномалии в АСУ – это нерегламентированные отклонения режимов ее работы, которые проявляются в показателях технологического процесса и, как следствие, в информационных потоках между элементами системы [45, 64]. Примером аномалии в работе АСУ может быть повышенная сетевая активность, являющаяся результатом протекающей вирусной атаки, попыток несанкционированного управления элементами системы, потери связи между узлами. Ряд авторов придерживаются мнения, что разработка методов, направленных на анализ и выявление возможных инцидентов ИБ в АС, должна быть реализована на основе подхода с выявлением аномалий.

В соответствии с Федеральным законом [127] в целях обеспечения безопасности объекта КИИ необходимо создание надежной системы защиты информации в АСУ, обеспечивающей своевременное обнаружение аномалий в системе и нейтрализацию связанных с ними угроз безопасности информации. Таким образом, задача обнаружения аномалий и нейтрализации соответствующих им угроз в КС АСУ транспортировкой нефтегазового сырья остается актуальной.

1.2 Определение целевой функции и выбор критериев оценки результатов исследования

Разработка СЗИ в АС сопряжена с определением соответствующих критериев оценки эффективности их работы в системе. В работах [45, 96, 193] приводится обобщенный критерий оценки риска для СЗИ, определяемый как произве-

дение вероятности реализации угрозы и ущерба от ее реализации. К основным видам рисков в АСУ ТП относятся риски от:

- дестабилизации производственных процессов;
- ущерба здоровью людей;
- разглашения и утраты конфиденциальной информации;
- финансовых убытков;
- ущерба репутации.

Исследуемая в работе АСУ участком транспортного трубопровода, топологическая схема которого представлена на рисунке 1.2, относится к категории территориально-распределенных промышленных объектов и разделена на подсистемы по функционально-топологическому принципу на этапе ее разработки. Каждая из подсистем характеризуется индивидуальной моделью угроз, специфика которой определяется удаленностью от пунктов операторского и диспетчерского управления, рельефом местности, метеорологическими условиями и другими факторами.

На рисунке оси координат *NLat* и *ELong* показывают координаты северной широты и восточной долготы соответственно, *SubS1 – SubS10* – исследуемые подсистемы АСУ.

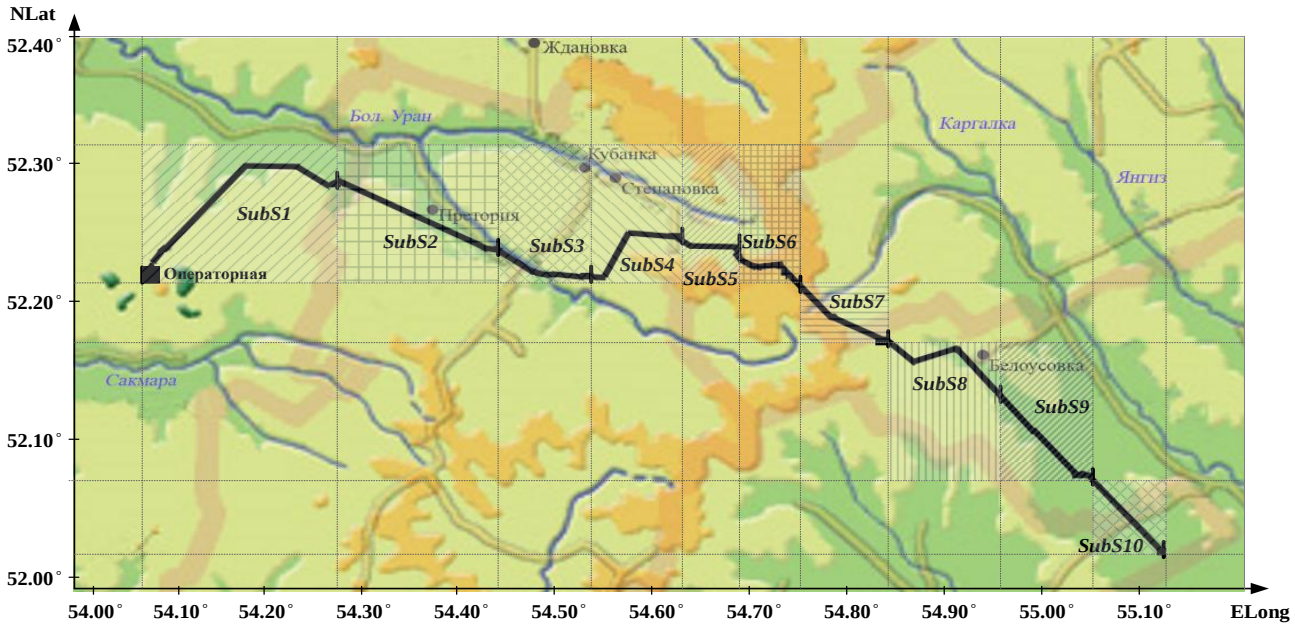


Рисунок 1.2 - Топологическая схема участка транспортного трубопровода

Значение риска от угроз для распределенной АСУ складывается из значений рисков от каждой угрозы на каждом из участков системы. Это обусловливает исследование угроз безопасности информации (БИ) как на основе общей модели угроз, так и для каждой из подсистем АСУ. Общий вид целевой функции задачи защиты информации в АСУ представлен в выражении (1.1).

$$R = \sum_{j=1}^{N}\sum_{i=1}^{L} p_{ij} * U_{ij},\ R \rightarrow min,\quad R \leq R_{доп}, T_{реал} \leq T_{доп};\ Z_{реал} \leq Z_{доп}; \qquad (1.1)$$

где R – значение риска от потенциальной реализации угроз БИ; $R_{доп}$ – допустимый остаточный риск; p_{ij} – вероятность успешной реализации угрозы i-го типа в j-й подсистеме; U_{ij} - ущерб от реализации угрозы; L – число видов угроз, создающих опасность нарушения ИБ в течение некоторого отрезка времени, определяемое моделью угроз; N – число подсистем распределенной АСУ; $T_{реал}, T_{доп}$ – реальное и допустимое время обнаружения аномалии в системе и нейтрализации связанной с ней угрозы, $Z_{реал}, Z_{доп}$ – реальные и допустимые затраты на СЗИ.

Для представления конкретных технико-экономических показателей эффективности методов и средств обнаружения аномалий и нейтрализации угроз представим задачу обнаружения аномалии, как задачу распознавания состояния АС, решением которой является определение принадлежности идентифицируемого состояния к одному из двух классов: классу аномальных (с точки зрения характера протекания технологического процесса) состояний A или классу нормальных состояний B.

Формула (1.1) характеризует статический риск, гарантированный на некоторый срок эксплуатации СЗИ при условии неизменности параметра U. Для рассматриваемого класса АС характерно функционирование в условиях изменения риска и роста ущерба от атак за период времени, требующийся для обнаружения и достоверного распознавания аномалии. Под достоверностью распознавания D в данном случае понимается вероятность правильного распознавания аномального состояния системы. Распознавание сопряжено с ошибками 1-го и 2-го рода, оцениваемыми вероятностями их возникновения α и β соответственно.

В работе [47] приводится формула оценки эффективности систем мониторинга и диагностирования сложных промышленных объектов. Формула применима и для расчета эффективности обнаружения аномалий в распределенных АСУ. Эффективность в данном случае определяется как сумма эффектов от правильного распознавания нормального и аномального состояний системы на каждом из ее участков с учетом экономии при верном распознавании, затрат при ошибочной идентификации и вероятностей ошибок 1-го и 2-го рода. Оценка достоверности распознавания аномалии D зависит от параметров α и β.

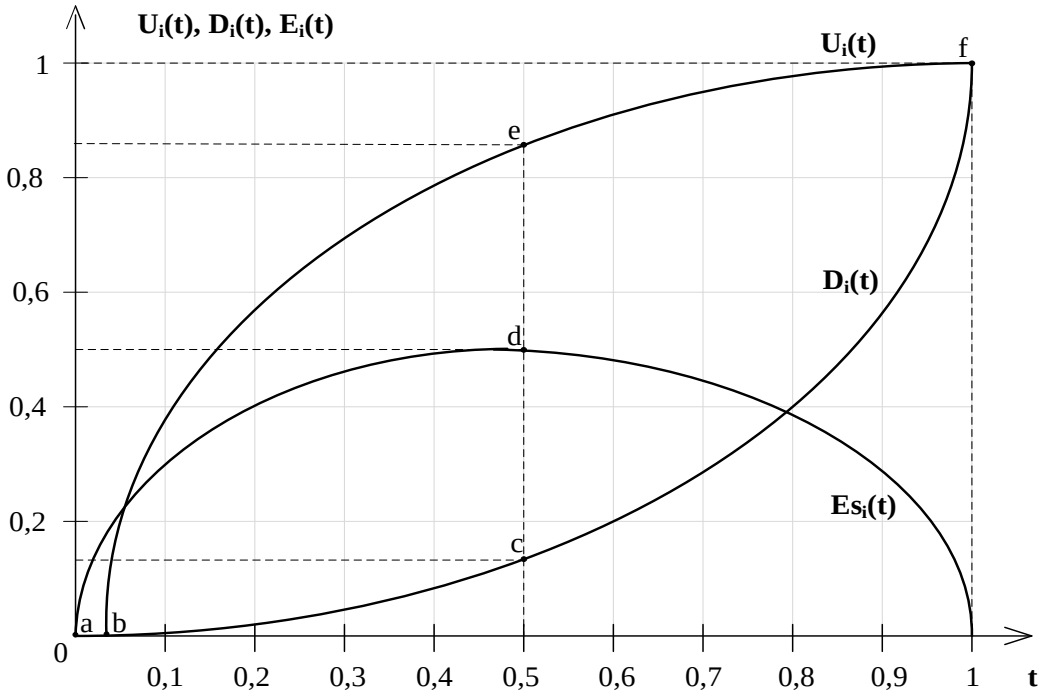


Рисунок 1.3 – Графики зависимости величин $U_i(t)$ - ущерба от реализации i-ой угрозы, $D_i(t)$ - достоверности распознавания состояния АС и $Es_i(t)$ - эффективности от принятия решения по нейтрализации угрозы от времени t

На рисунке 1.3 представлены графики зависимости ущерба от реализации угрозы, достоверности распознавания аномального состояния АС и эффективности от принятия решения по нейтрализации угрозы от времени, построенные на основе математической модели оценки эффективности систем мониторинга и диагностирования сложных промышленных объектов, представленной в работе [47].

Получение новых сведений об аномалии со временем существенно повышает достоверность распознавания состояния системы. Однако при развитии аномалии наносится все больший урон, эффект от распознавания со временем начинает снижаться. Чем дольше длится процесс распознавания аномалии и принятия решения по нейтрализации соответствующей ей угрозы, тем больше величина ущерба. Конечная стадия приводит к аварии на объекте, либо к катастрофическому ущербу. Обнаружение аномалии и принятие мер по нейтрализации угрозы должно быть осуществлено до того, как будет нанесен значительный ущерб.

В качестве примера аномального процесса, описываемого графиками на рисунке 1.3, рассмотрим процесс развития вирусной атаки в АСУ. Примером графика достоверности распознавания атаки является график, построенный на основе данных об ошибках ее распознавания 1-го и 2-го рода, полученных из журналов средств антивирусной и сетевой защиты. График ущерба в данном случае может характеризовать финансовые потери, вызванные дестабилизацией производственного процесса в результате отказа оборудования. Система мониторинга является эффективной тогда, когда обеспечивается оперативное и достоверное обнаружение аномального состояния и принятие решения по нейтрализации атаки при допустимом уровне ущерба.

Исследование целевой функции позволило определить основные критерии оценки результатов исследований: стремление к снижению риска обуславливает решение задач минимизации параметра p за счет повышения достоверности распознавания аномалии (в частности, снижения вероятностей ошибок 1-го и 2-го рода) и параметра U за счет повышения производительности (оперативности работы) методов и средств защиты при допустимых параметрах затрат для их достижения.

1.3 Анализ структурно-функциональной организации распределенной АСУ ТП как объекта защиты

1.3.1 Особенности функционирования распределенных управляющих систем в условиях угроз безопасности информации

Построение системы защиты информации для распределенной АСУ невозможно без детального анализа ее структуры и функций и исследования АСУ как объекта защиты. В качестве объекта исследования в настоящей работе выбраны СЗИ в распределенных промышленных сетях на примере КС АСУ ТП транспортировки нефтегазового сырья одного из месторождений Оренбургской области.

В работах [68, 146] рассматриваются структурные и функциональные особенности АСУ ТП с точки зрения обеспечения ИБ в системе. Однако в рассмотренных работах недостаточно внимания уделено вопросам исследования АСУ как распределенного в пространстве объекта защиты.

Согласно стандарту [74] распределённая система управления (РСУ) – это комплекс технических и программных решений для построения АСУ ТП, характерной чертой которой является децентрализованная обработка данных и наличие распределенных в пространстве управляющих устройств, систем ввода и вывода информации. Организация СЗИ для исследуемой в настоящей работе АСУ имеет свою специфику, связанную с климатическими и географическими особенностями Оренбургской области. В частности, для построения системы защиты необходим анализ уязвимостей и угроз для множества подсистем протяженной в пространстве АСУ, расположенной на территории с большим разнообразием рельефа, резкоконтинентальными климатическими условиями, близким расположением населенных пунктов.

Целью настоящего раздела является определение структурных и функциональных особенностей исследуемой АСУ как объекта защиты. Для достижения данной цели были разработаны: классификация АСУ ТП транспортировки нефтегазового сырья с учетом особенностей функционирования распределенных систем

управления; структурная модель распределенной АСУ, позволяющая определить основные уязвимости, угрозы и перечень защищаемой информации в системе; функциональная модель процесса автоматизированного управления транспортировкой нефтегазового сырья, позволяющая определить место и требования к подсистеме мониторинга аномалий в АСУ.

Особенности функционирования РСУ в условиях воздействия угроз БИ оказывают значительное влияние на эффективность работы методов и средств защиты информации. Для определения особенностей исследуемого класса АСУ разработана классификация, представленная на рисунке 1.4.

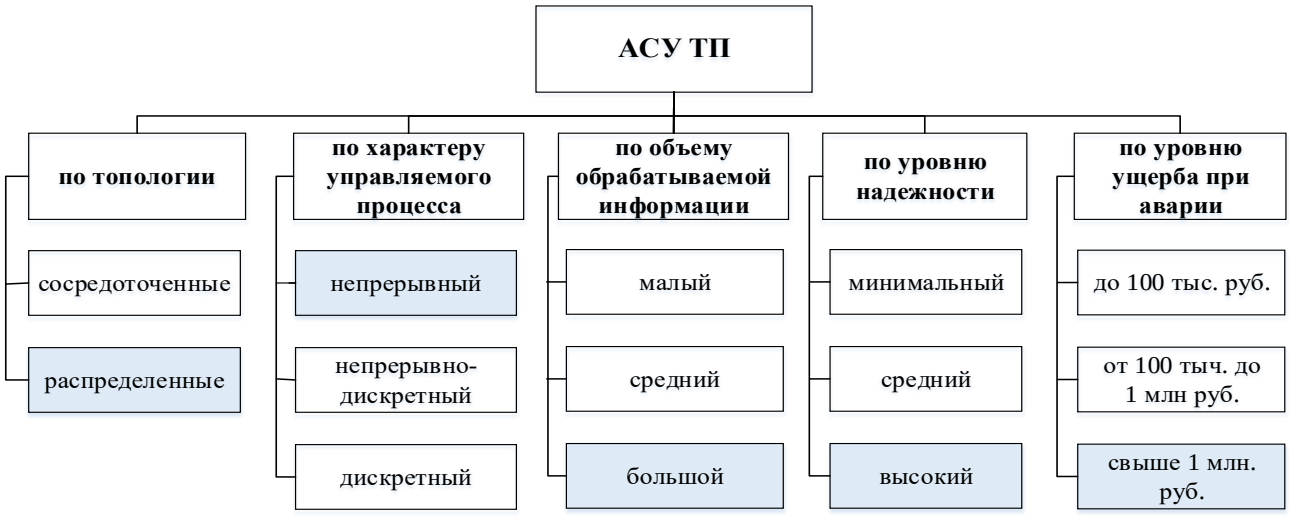


Рисунок 1.4 – Классификация АСУ ТП

Анализ разработанной классификации и материалов источников [62, 68, 69, 80, 86, 166] позволил определить особенности АСУ ТП транспортировки нефтегазового сырья как объекта защиты:

- протяженность промышленного объекта и распределенность в пространстве подсистем АСУ (протяженность рассматриваемого в работе участка трубопровода – более 130 км);

- необходимость обеспечения непрерывности технологического процесса;

- переменный во времени и в пространстве характер угроз объектам информатизации АСУ, обусловленный географическими и климатическими особенностями Оренбургской области (резкими перепадами температур, сезонными павод-

ками, особенностями рельефа), определяющими различные параметры периодичности, сезонности и стохастичности проявления угроз БИ;

- увеличение объемов обрабатываемой информации о состоянии системы, обусловленное усложнением решаемых задач и повышением требований к защите информации в АСУ, в условиях ограниченных вычислительных ресурсов;

- использование промышленного Ethernet, для которого характерно наличие как протоколов корпоративных сетей, так и промышленных протоколов и средств связи, обнаружение и устранение уязвимостей в которых затруднительно с использованием традиционных СЗИ;

- высокий уровень потенциального ущерба вследствие реализации угроз безопасности информации.

Перечисленные особенности увеличивают время анализа данных средствами защиты и снижают оперативность достоверного распознавания аномальных состояний АС, влекущих за собой сбои в работе системы управления, обеспечивающей поддержание заданных технологических параметров. В результате повышается риск возникновения аварийной ситуации или нарушения выполняемых системой функций управления со значительными негативными последствиями для технологического процесса, оборудования, экологии.

1.3.2 Структурная модель распределенной АСУ транспортировкой нефтегазового сырья

Рассматриваемая в работе АСУ ТП представляет собой совокупность программно-технических средств (ЭВМ, средств связи, устройств отображения информации, передачи данных и т.д.), моделей, методов, алгоритмов, организационных комплексов и персонала, обеспечивающих рациональное управление технологическим процессом транспортировки нефтегазового сырья.

Анализ типовых структур и перечня выполняемых функций распределенных АСУ, проведенный на основе работ [162, 168, 170], позволил представить структурную модель исследуемой системы в виде совокупности подсистем (1)–(3), изображенных на рисунке 1.5.

Объектом управления является распределенный в пространстве технологический комплекс. Органом управления – распределенная АСУ, осуществляющая автоматизацию процессов сбора и обработки информации о состоянии объекта со всех его участков и оперативного контроля и управления ТП.

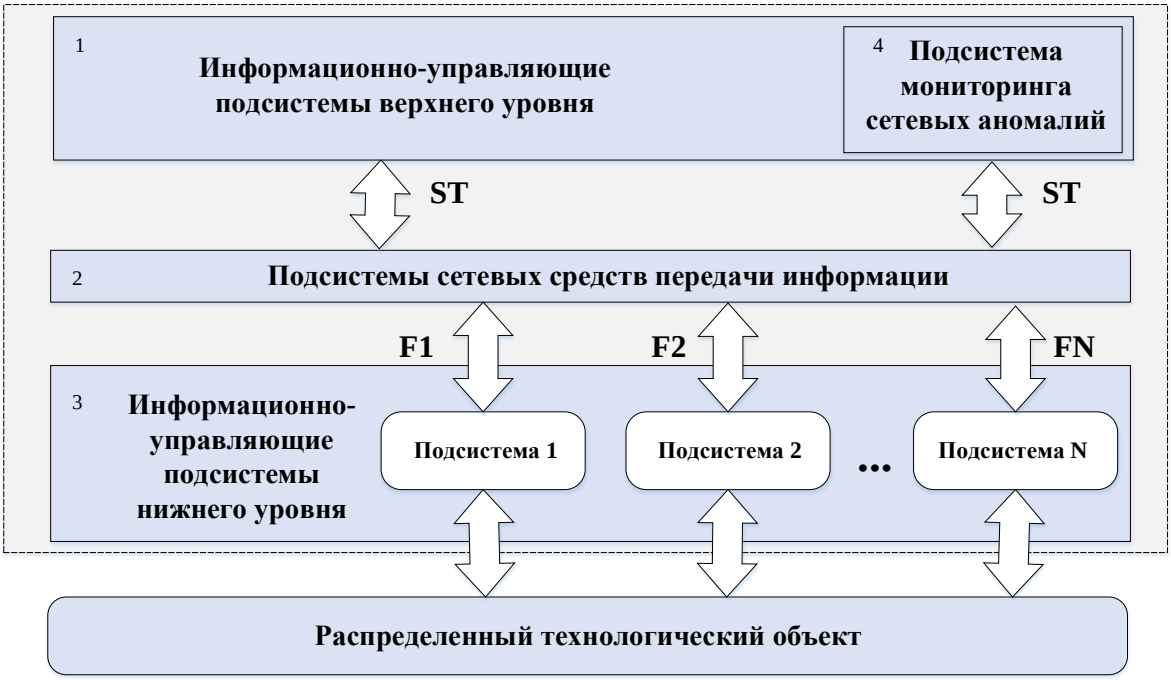


Рисунок 1.5 – Структурная модель распределенной АСУ транспортировкой нефтегазового сырья

Исследуемая АС разделена на подсистемы по функционально-топологическому принципу на этапе ее разработки. К основным подсистемам относятся: информационно-управляющие подсистемы нижнего уровня - подсистемы блочно-комплектных электростанций (БКЭС), включающие оборудование связи, контроллеры, датчики, исполнительные механизмы; информационно-управляющие подсистемы верхнего уровня – подсистемы установки подготовки нефти и газа, линейно-производственного управления, управления по эксплуатации соединительных продуктов, административного здания, включающие оборудование связи, сервера и автоматизированные рабочие места (АРМ) телемеханизации и системы обнаружения утечек, служб мониторинга состояния АСУ, АРМы операторов и диспетчеров.

Информационно-управляющие подсистемы нижнего уровня АСУ напрямую связанны с объектом управления и обеспечивают сбор данных о параметрах технологического процесса и состояния оборудования, реализуют управляющие воздействия. Информационно-управляющие подсистемы верхнего уровня контролируют ход технологического процесса, формируют управляющие воздействия на объект и контролируют их исполнение.

Связь между подсистемами осуществляется через комплекс сетевых средств передачи информации. Через сетевые интерфейсы компоненты АСУ взаимодействуют по каналам связи, представляющим собой совокупность сред распространения сигнала, а также транзитных сетевых устройств. Информационный поток в подсистеме средств связи представляет собой сетевой трафик, описываемый сетевыми протоколами стека TCP/IP. На рисунке 1.5 представлены следующе информационные потоки: *F1-FN* – потоки измерительной и управляющей информации в подсистемах нижнего уровня; *ST* – информационные потоки сетевого трафика в подсистеме сетевых средств передачи информации.

Особое место в типовой структуре АСУ занимает подсистема мониторинга сетевых аномалий (4), осуществляющая обнаружение нерегламентированных состояний АСУ по данным сетевого трафика и поддержку принятия решений по их нейтрализации. Подсистема мониторинга реализуется на верхнем уровне управления и непосредственно связана с подсистемой сетевых средств передачи информации.

Разработанная структурная модель и положения ГОСТ [78] позволили выявить основные уязвимости, характерные для исследуемого класса АСУ. Классификация уязвимостей представлена на рисунке 1.6. Анализ публикаций [78, 157] показал, что наибольшее число уязвимостей (более 80%) приходится на элементы информационно-управляющей подсистемы верхнего уровня и подсистему сетевых средств передачи информации, в частности большинство уязвимостей обнаружены в устройствах с функциями управления, диспетчеризации и мониторинга, в сетевых устройствах и инженерном программном обеспечении. Около 12% уязвимостей приходятся на информационно-управляющие подсистемы нижнего

уровня. Специальное прикладное ПО, использующееся на нижних уровнях, содержит меньше уязвимостей, но является значимой целью атак, реализуемых на верхнем уровне, так как задает логику управления.

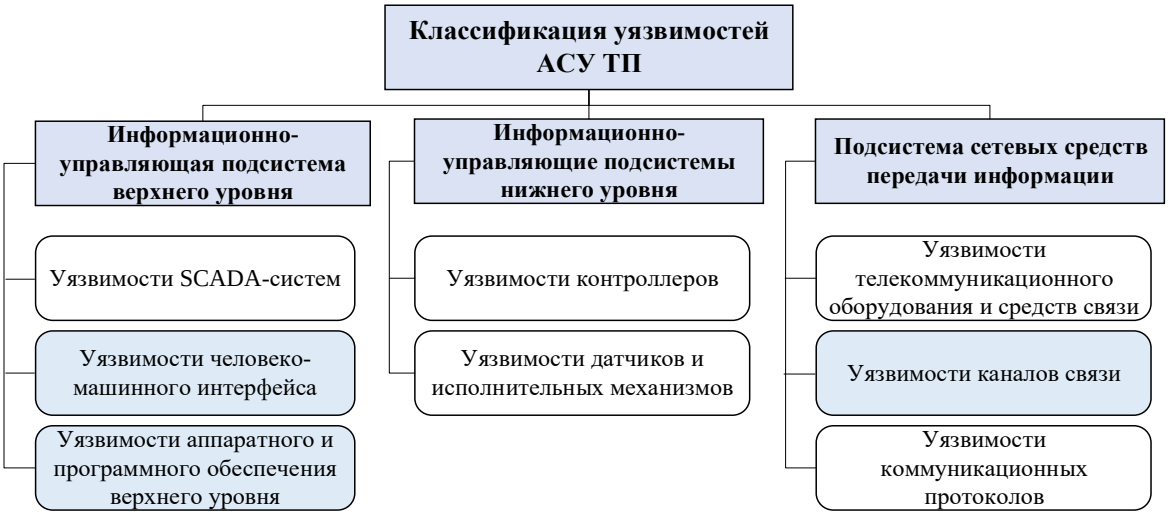


Рисунок 1.6 – Классификация уязвимостей элементов АСУ ТП

Особенностью подсистемы сетевых средств передачи информации является ее большая протяженность в пространстве, что повышает вероятность несанкционированного доступа к коммутационному оборудованию, повреждения каналов связи при наступлении неблагоприятных климатических условий или неправильном монтаже. Дополнительные уязвимости создаются за счет использования незащищенных протоколов стека TCP/IP и особенностей промышленных протоколов (например, антивирусы часто игнорируют промышленные протоколы).

Перечисленные уязвимости обуславливают появление угроз БИ для информационных и программно-аппаратных ресурсов АСУ. В частности:

- использование сетей общего пользования для передачи информации на верхнем и среднем уровнях повышают вероятность реализации сетевых атак и несанкционированного удаленного доступа к узлам АСУ;

- сложность управления доступом ведет к повышению пользовательских привилегий (в том числе, в управлении АСУ), а в ряде случаев позволяет полностью обойти механизмы аутентификации и авторизации;

- большая пространственная распределенность подсистем АСУ и сезонные изменения климата увеличивают риск нарушения целостности линий связи и потери критически важной информации о состоянии системы при ее передаче оператору и диспетчеру.

В нормативных документах [127, 156] в качестве основных защищаемых от угроз ресурсов в АСУ ТП транспортировки нефтегазового сырья выделяют:

- технологическую информацию, включающую управляющую и контрольно-измерительную информацию;
- производственную тайну, циркулирующую на всех уровнях АСУ и включающую чертежи и геологические карты, сведения об инфраструктуре системы, данные о производственных и технологических процессах, физико-химические характеристики продукции, данные об исследованиях и испытаниях;
- коммерческую тайну, включающую результаты тендерной деятельности, данные договоров с партнерами и подрядчиками, данные о запасах нефти и газа;
- программно-технический комплекс, включающий технические средства, программное обеспечение (ПО) и средства защиты информации (СЗИ);
- персонал АСУ.

В рамках настоящей работы рассмотрены вопросы защиты технологической и конфиденциальной информации, а так же программно-технического комплекса АСУ от угроз сетевых вирусных атак, нерегламентированных действий пользователей, потери информации при передаче по каналам связи.

1.3.3 Функциональная модель процесса автоматизированного управления транспортировкой нефтегазового сырья

Анализ структурной модели позволил выявить функциональные особенности АСУ. На рисунке 7 представлена функциональная модель процесса автоматизированного управления транспортировкой нефтегазового сырья. Для организации управления технологическим процессом используются руководящие документы и требования (федеральные законы, государственные стандарты и стандарты организаций), предъявляемые к исследуемому классу промышленных систем,

в частности [81-84, 127, 153, 156]. Основными «механизмами управления» в вопросах, связанных с защитой информации в АСУ, являются оператор (*О*), диспетчер (*Д*) и специалист по информационной безопасности.

Рисунок 1.7 – Контекстная функциональная модель процесса автоматизированного управления транспортировкой нефтегазового сырья

Для декомпозиции и детализированного описания представленной функциональной модели разработана классификация подсистем АСУ ТП, приведенная на рисунке 1.8.

Рисунок 1.8 – Классификация подсистем АСУ ТП

Декомпозиция контекстной модели на функциональные блоки, позволяющая детализировать процесс автоматизированного управления транспортировкой нефтегазового сырья, представлена на рисунке 1.9.

К информационно-управляющим подсистемам верхнего уровня относятся подсистемы *A3, A4, A5, A7* и *A9*. Сбор информации и управление технологическим процессом на нижнем уровне осуществляется подсистемами *A1, A6* на каждом из *N* участков трубопровода. К подсистемам сетевых средств передачи информации относятся подсистемы *A2* и *A8*.

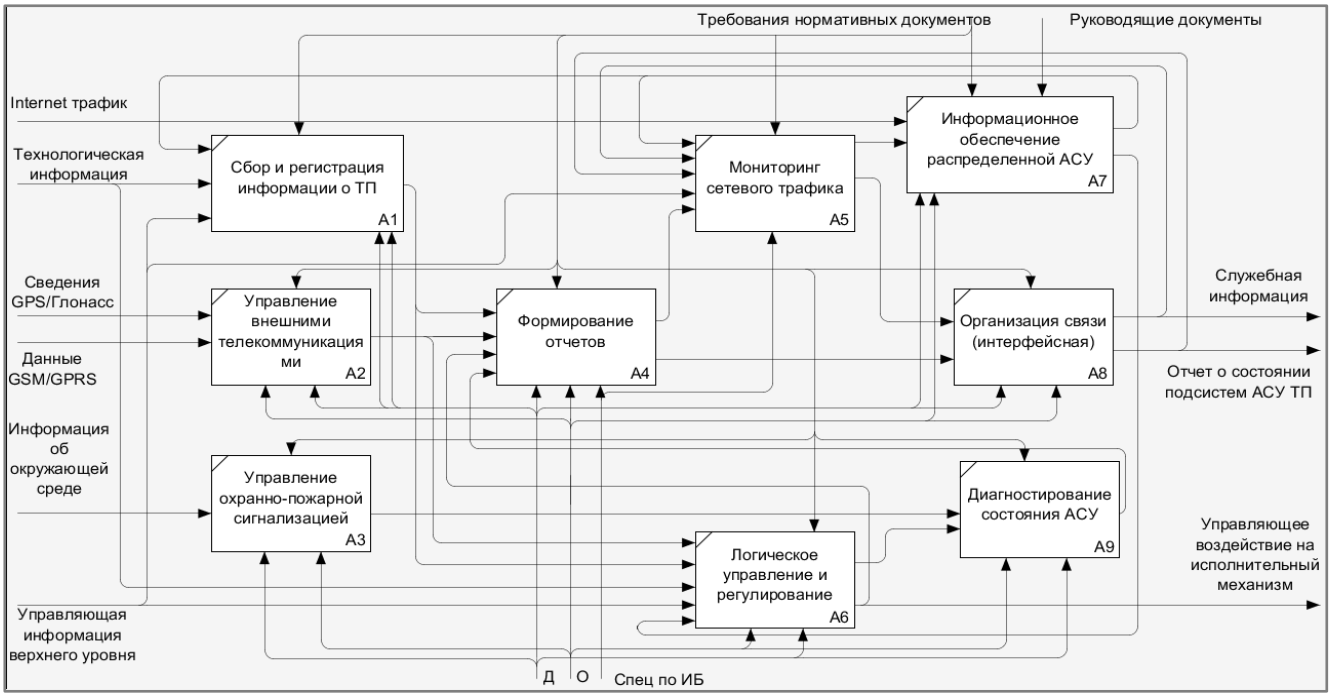


Рисунок 1.9 – Декомпозиция контекстной модели процесса автоматизированного управления транспортировкой нефтегазового сырья

С точки зрения источника информации о состоянии АСУ как объекта защиты особый интерес представляет подсистема организации внутренней связи *A8*, являющаяся частью компьютерной сети АСУ и включающая:

- сеть нижнего уровня (полевую шину), обеспечивающую сетевое взаимодействие между контроллерами и удаленной периферией по промышленным протоколам;

- сеть верхнего уровня АСУ ТП, предназначенную для передачи данных между контроллерами, серверами, диспетчерскими и операторскими рабочими станциями по сетям Ethernet.

Выбор сетевого трафика, циркулирующего в подсистеме *A8*, в качестве основного источника информации для подсистемы *A5* обусловлен следующими факторами:

- совокупность сведений, полученных путем обработки данных сетевого трафика в некоторый интервал времени, позволяет проследить динамику изменения состояния АСУ (например, изменение параметров технологического процесса, маршруты распространения вируса в системе);

- сетевой трафик, циркулирующий в подсистеме *A8*, содержит данные, передаваемые из сетей нижнего уровня (например, по протоколу Modbus TCP) и позволяет получить сведения об информационных процессах на всех уровнях системы;

- мониторинг аномалий по данным сетевого трафика позволяет регистрировать признаки потенциального инцидента безопасности до его возникновения и прогнозировать варианты его развития (например, обнаруживать нерегламентированные команды оператора до их передачи на контроллер).

Особое место в функциональной модели АСУ занимает подсистема защиты информации, расположенная на всех ее уровнях и функционально связанная с каждым из блоков представленной модели. Подсистема мониторинга сетевых аномалий является частью подсистемы защиты информации и устанавливается на функциональный узел, через который проходит большинство информационных потоков о состоянии АСУ. К таким потокам относятся: потоки технологической, управляющей, служебной информации, отчеты о состоянии АСУ, сведения подсистемы информационного обеспечения.

Анализ функциональной модели позволил выбрать подсистему *A5* в качестве основной для реализации разрабатываемых методов обнаружения аномалий и нейтрализации угроз. Подсистема мониторинга сетевого трафика непосредственно взаимодействует с подсистемой организации связи *A8* и имеет доступ к

данным сетевых потоков информации на верхнем и нижнем уровнях. На вход подсистемы подаются управляющая информация верхнего уровня, отчеты о состоянии АСУ, служебная информация и сведения подсистемы информационного обеспечения. На выходе формируются сведения об аномалиях и рекомендации по их нейтрализации.

Важной особенностью подсистемы *A5* является то, что она может быть установлена как на нижнем, так и на верхнем уровнях АСУ. В первом случае средства мониторинга подключаются к каналу связи определенного участка N и контролируют внутренний трафик, во втором – к общему каналу связи и контролируют трафик всей системы управления. Модели и алгоритмы обнаружения аномалии при этом будут идентичными. Особенности поиска в каждом из случаев будут определяться особенностями сетевого взаимодействия.

Требования к подсистеме мониторинга сетевого трафика, как к составляющей системы ИБ, определяются в зависимости от класса защищенности АСУ, в соответствии с нормативными документами ФСТЭК [127, 151], ГОСТом [81] и политикой безопасности предприятия. В соответствии с положениями приказа ФСТЭК России № 31 от 14.03.2014 г. исследуемая АСУ имеет класс защищённости «К3». Базовый набор требований защиты информации для АСУ ТП с учётом присвоенного класса защищённости включает:

- обеспечение конфиденциальности, целостности и доступности информационных и программно-аппаратных ресурсов АСУ, анализ защищенности ресурсов;
- контроль и разграничение доступа к элементам АСУ;
- антивирусная защита информации;
- контроль управляющих воздействий на технологический объект;
- обеспечение своевременности поступления информации о технологическом объекте;
- обеспечение оперативной реакции на инциденты безопасности;
- регистрация и протоколирование событий безопасности для восстановления хода нерегламентированной или аварийной ситуации.

В соответствии со стандартом [81] система мониторинга аномалий по данным сетевого трафика должна обеспечивать:

- получение и обработку данных от множества, в том числе разнородных, источников данных мониторинга:
- представление результатов анализа данных мониторинга в режиме времени, близком к реальному;
- возможность анализа событий безопасности и иных данных мониторинга на основе различных правил (сигнатур);
- централизованное хранение данных мониторинга (для всех объектов мониторинга или в рамках каждого объекта мониторинга);
- возможность формирования различных отчетов по результатам мониторинга ИБ.

Анализ структурно-функциональной организации распределенной АСУ как объекта защиты позволил подвести задачу обнаружения аномалий к задаче совершенствования методов и средств распознавания и идентификации аномальных состояний КС АСУ на основе исследования и интеллектуальной обработки сетевых информационных потоков, передающихся между ее узлами. Для определения признаков и правил распознавания необходима классификация и характеристика аномалий, возникающих в системе.

1.4 Классификация и характеристика основных аномалий в распределенных управляющих системах

Под аномалиями в АСУ понимаются нерегламентированные отклонения режимов ее работы, которые могут возникать случайно, либо быть результатом намеренного деструктивного воздействия. Важнейшим аспектом решения задачи распознавания аномалий является их классификация, позволяющая: построить эталонное множество образов нормального состояния АСУ в условиях неопределенности воздействий внешней и внутренней среды; выявить необходимые и до-

статочные информативные признаки аномальных состояний АСУ; построить правила их распознавания и идентификации.

С целью упорядочивания аномалий на основе материалов публикаций [56, 78, 122] разработана классификация, представленная на рисунке 1.10. В классификации приведены основные аномалии, характерные для рассматриваемой в работе АСУ ТП транспортировки нефтегазового сырья.

В качестве основных классификационных признаков выбраны вид аномалии, причина возникновения, особенности проявления, место возникновения, источник аномалии и источник информации об аномалии, распределенность аномалии в системе. Выбор признаков обусловлен спецификой функционирования исследуемой АСУ и особенностями поиска аномалий в сетевом трафике.

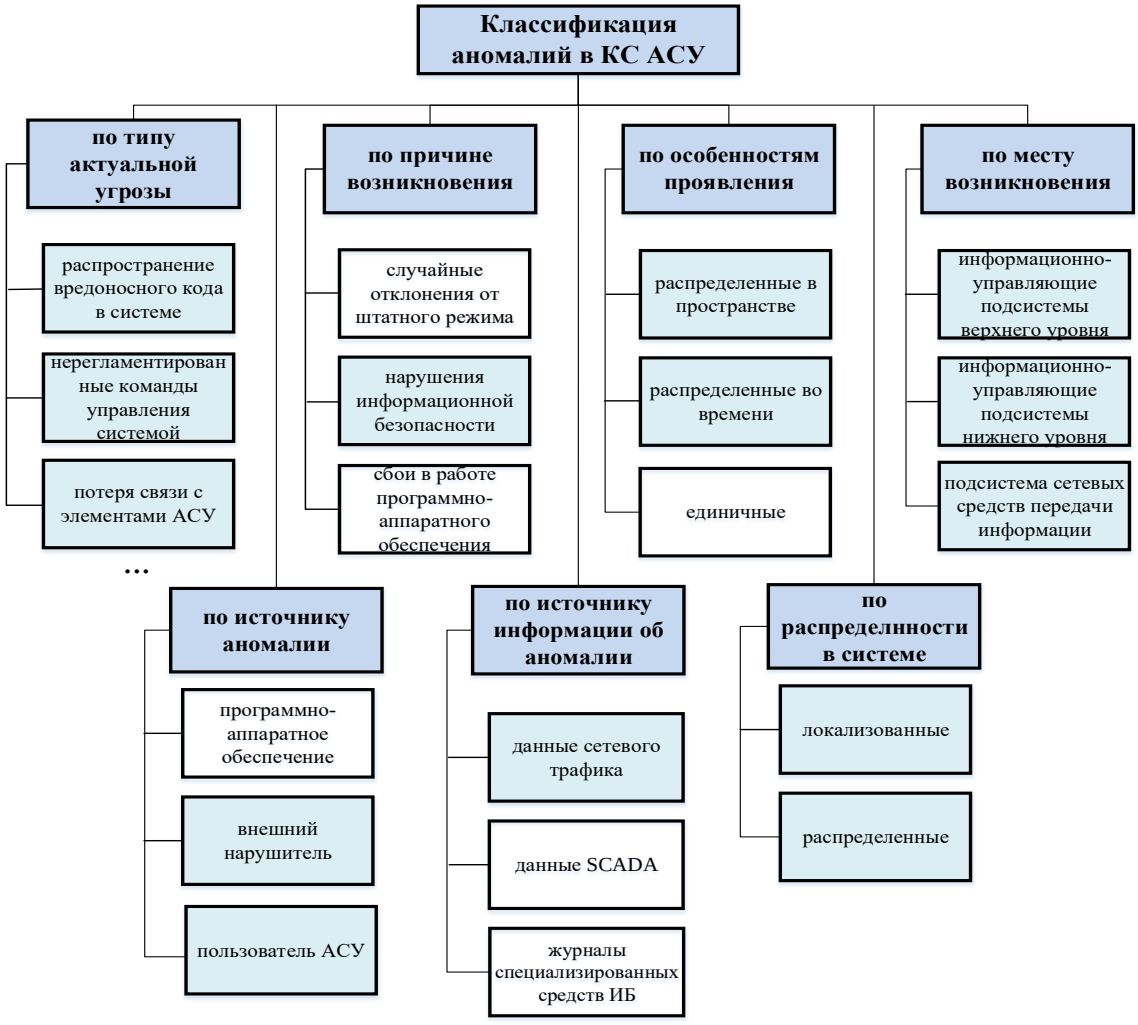


Рисунок 1.10 – Классификация аномалий в распределенных управляющих системах транспортировки нефтегазового сырья

Исследование статистики инцидентов информационной безопасности и моделей угроз для исследуемого класса АСУ показало, что наиболее опасными видами аномалий являются отклонения, возникающие вследствие:

- сетевых вирусных атак на IT-компоненты АСУ, приводящих к распространению вредоносного кода в системе (вируса, спама и т.д.);
- сбоя, отказа технических, программных средств связи, физическое выведение из строя средств передачи информации;
- ошибочных, либо злоумышленных действий персонала системы, ведущих к появлению нерегламентированных команд управления.

Аномалии, возникающие в исследуемой системе, могут проявляться на всех ее уровнях, быть локализованы в конкретном сегменте сети, либо распределены по всей системе и вызваны действиями внешних нарушителей и внутренних пользователей, в частности, операторов и диспетчеров АСУ. В качестве основного источника исходной информации об аномалиях определен сетевой трафик.

1.5 Характеристика сетевого трафика АСУ ТП как источника сведений об аномалиях

Решению задачи распознавания состояния КС посвящен представительный ряд публикаций, в которых в качестве источника исходных данных для анализа состояний используется сетевой трафик (СТ) [70, 124, 132, 179 - 182, 59]. В перечисленных работах определяются требования к анализу, рассматриваются основные классы существующих систем анализа с учетом особенностей подключения сетевых узлов к сетям обмена данными и используемой программно-аппаратной базы.

Целью настоящего раздела является определение особенностей сетевого трафика как источника информации об аномалиях в АСУ. Для достижения цели были определены особенности сетевого трафика АСУ ТП, признаки и источники признаковой информации об аномалиях в сетевых информационных потоках, построена обобщенная сигнатура распознавания аномалии.

Под сетевыми информационными потоками данных в АСУ понимается совокупность сведений о работе системы в виде некоторого количества пакетов определенного типа. Совокупность данных сетевого трафика, зарегистрированных в конкретный момент времени, характеризует текущее состояние системы. В общем случае множество состояний системы можно разделить на два класса: класс регламентированных (нормальных) состояний QN и класс аномальных состояний QA. Классы QN и QA содержат некоторые множества образов состояний, определяемых значениями параметров СТ.

Временные ряды параметров СТ позволяют получать информацию о динамике изменения состояний АСУ и об аномалиях в системе управления. Под аномалией в сетевом трафике понимается регистрация количественного, либо качественного изменения потока информации в КС АСУ, не связанного с регламентированными режимами ее работы. Аномалии в сетевом трафике сигнализируют об отклонениях в функционировании промышленного объекта или отклонениях, связанных с нарушением взаимодействия устройств при обмене данными в его составе [64, 95]. Обнаружение аномалий – это поиск отклонений параметров СТ от регламентированных значений, «нормального» профиля.

В работе авторского коллектива [70] определяется обобщённая схема анализа сетевого трафика с целью обнаружения аномалий, частным случаем которой является анализ аномалий в два этапа:

1. Обнаружение аномальных состояний АСУ, как проявлений инцидентов ИБ, на основе агрегирования и классификации сетевых информационных потоков системы на «нормальный» и «аномальный» трафик. Для определения аномальности состояния, в частности, детектируются отклонения от «нормальной» картины на основе статистической информации об активности некоторых хостов в сети. Подобная активность, зачастую, хорошо различима в промышленной КС.

2. В случае обнаружения аномальных состояний проводится дальнейшая уточняющая классификация «аномального» сетевого трафика и идентификация состояния системы по данным протоколов или конкретных сетевых приложений, например, программе мониторинга состояния. Одним из подходов к классифика-

ции является анализ сигнатур – характерных признаков состояния системы. Классификация может выполняться как на уровне пакета, так и на уровне потока.

Одной из основных задач идентификации является определение параметров трафика, отражающих различные состояния системы. В качестве общего набора данных для обнаружения аномальных состояний КС АСУ в работах [27, 58, 124, 131, 179 - 182] выделяют некоторые наборы счетчиков, характеризующих сетевые сессии, например, количество переданных пакетов и байт, время создания и завершения потока; для распознавания состояния - сведения об адресах сетевых узлов ***IP,*** протоколах связи ***O***, номерах портов ***P***, данных пакета ***D***. Для контроля управляющих воздействий на систему особое значение имеют сведения о командах управления ***K***. Время регистрации аномалии *T* необходимо для определения выборки событий, удовлетворяющих интервалу анализа. Анализ потоков сетевого трафика позволил представить его составляющие в виде формулы (1.2):

$$ST=\{T, IP, O, P, D, K\}. \quad (1.2)$$

Признаки распознавания аномальных состояний АСУ, связанных с актуальными угрозами [115, 205] распространения вредоносного кода в КС, нерегламентированных действий персонала системы, сбоя, отказа технических, программных средств связи, физического выведение из строя средств передачи информации, представлены в таблице 1.1.

Признаки содержатся как в заголовке сетевого пакета (тип протокола, адреса, номера портов, время), так и в информационной части (директивные команды управления). Для решения задач обнаружения и распознавания состояний АС в контексте инцидентов информационной безопасности необходим глубокий анализ пакетов по различным протоколам на нескольких уровнях модели OSI, чаще всего протоколов прикладного, транспортного и сетевого уровней, в частности, IP, TCP, Modbus TCP и ARP. Таблица распределения протоколов связи в промышленных АСУ по уровням модели OSI представлена в приложении Б.

Таблица 1.1 – Признаки распознавания аномальных состояний АСУ по данным сетевого трафика

Угрозы	**Основные объекты воздействия**	**Аномалии в КС АСУ**	**Уровни модели OSI**	**Основные параметры распознавания аномалии в СТ**
Распространение вредоносного кода в КС	Аппаратно-программное обеспечение на верхнем и среднем уровнях АСУ (в частности, инженерные рабочие станции SCADA серверы, ПЛК, операционные системы, базы данных и спец. ПО)	- увеличение интенсивности пакетов от определенных IP-адресов, связанных с распространением вредоносного кода; - быстрое распространение вредоносного ПО в системе, нарушение доступности данных и сервисов на узлах АСУ.	Сетевой, транспортный, сеансовый, уровень представления, прикладной	- IP-адреса *(IP)* зараженных узлов; - время регистрации пакетов *(t)*, период времени распространения вируса *(T)*; -данные сетевых пакетов *(D);* - порты (*P*).
Нерегламентированные действия персонала	Аппаратно-программное обеспечение на верхнем и среднем уровнях АСУ (в частности, ПЛК, SCADA-системы)	- нерегламентированные управляющие операции и транзакции в СТ; - резкие изменения значений технологических параметров в системе; - увеличение интенсивности пакетов СТ, связанных с тревожными сообщениями от SCADA-систем.	Сетевой, прикладной	- IP-адреса *(IP)* управляющих узлов; - управляющие команды *(K)*, передаваемые в данных *(D)* пакетов протокола *(O)* Modbus TCP.
Сбой, отказ технических, программных и средств связи, физическое выведение из строя средств передачи информации	Технические и программные средства связи, каналы связи на сетевом уровне АСУ	- увеличение интенсивности пакетов-запросов на соединение; - отсутствие связи с элементами системы.	Сетевой	- IP-адреса (*IP*) недоступных узлов; - время отсутствия ответа от недоступного узла (Δt), регистрируемое по данным пакетов протокола *(O)* ARP.

Анализ таблицы 1.1 позволил представить обобщенную сигнатуру состояния АСУ по данным сетевого трафика в виде формулы (1.3):

$$S(t) = <T, IP, O, P, D, K>. \quad (1.3)$$

Каждый из перечисленных параметров, регистрируемый в дискретный момент времени ***t***, имеет свою природу, диапазон изменения значений и значитель-

ное количество возможных значений в этом диапазоне. Так как состояние системы, определяется несколькими параметрами одновременно и анализируется в течение некоторого интервала времени, число возможных состояний системы является очень большим и определяется по формуле (1.4):

$$N\text{сост} = \prod_{i=1}^{N} DP_i \ , \qquad (1.4)$$

где DP_i – количество возможных значений $\boldsymbol{i}$ – го параметра в диапазоне его изменения, $\boldsymbol{N}$ – число параметров. Авторские исследования, проведенные в работах [14, 23, 41, 45, 46] показали, что сетевой трафик распределенной АСУ характеризуется большими объемами информации.

Перечисленные выше особенности создают повышенные требования к производительности и достоверности работы средств мониторинга и анализа сетевого трафика и приводят к необходимости разработки новых моделей и методов обнаружения аномальных состояний КС, позволяющих компактно хранить и оперативно анализировать данные сетевого трафика.

Для определения концепции задачи исследования и требований к разрабатываемым методам был проведен анализ современных решений задачи обнаружения аномалий и нейтрализации угроз в распределенных АСУ ТП.

1.6 Анализ современных решений задачи обнаружения аномалий и нейтрализации угроз БИ в распределенных АСУ ТП

1.6.1 Анализ теоретических и прикладных работ по теме исследования

Для представления сущности и особенностей задачи мониторинга аномалий в распределенных АСУ был проведен анализ теоретических и прикладных работ по нескольким направлениям. Целью анализа является определение концепции решения задачи обнаружения аномалий и нейтрализации угроз для рассматриваемого класса промышленных объектов.

К первому направлению отнесены публикации, содержащие сведения о современном уровне развития систем мониторинга состояния безопасности АСУ, нефтегазового оборудования и транспортных трубопроводов. В частности, работы Аралбаева Т.З. [47, 49], Воронцова А. [68], Гаспарянца Р.С. [69], научные исследования Веревкина А.П. [66], Савиной А.В. [160], Knapp E. D., Langill J. T. [188]. Анализ данных работ выявил динамику развития методов и средств мониторинга и позволил определить особенности построения рассматриваемых систем для различных объектов автоматизации: распределенность, многофункциональность, повышенные требования к безопасности АСУ.

Ко второму направлению отнесены публикации, посвященные вопросам повышения технико-экономических характеристик методов и средств обнаружения аномалий, прогнозирования состояний и принятия решений при возникновении инцидентов ИБ в АСУ ТП. К ним отнесены: труды ученых академических организаций и ВУЗов, в частности, Васильева В.И., Вульфина А.М., Картака В.М., Фрида А.И., [55, 61 - 65, 130, 185], Котенко И.В., Остапенко А.Г., Саенко И.Б., Чечулина А.А. [26, 109, 133, 174, 194], Соколова А.Н. [52, 60], Тимофеева А.В. [167]; исследования сотрудников ряда организаций, занимающихся обеспечением информационной безопасности АСУ, в частности, АО «Лаборатория Касперского» [115, 136], АО «Positive Technologes», ООО «УЦСБ» [144, 187], ООО «Атом Безопасность» [205]. Анализ данных публикаций позволил определить направленность научных и практических исследований по теме работы. В рассмотренных работах отмечается увеличение потока информации в распределенных АСУ и делается прогноз на развитие средств мониторинга их состояния по данным сетевого трафика.

К третьему направлению отнесены публикации Арояна З.А. [50], Белова Е.Б. [54], Гетьмана А.В., Евстропова Е.Ф., Зегжды Д.П., [96, 97], Маркина Ю.В. [70], Машкиной И.В. [120], Луценко Е.В [162], Симанкова В.С., Суханова А.В. [165], содержащие сведения концептуального характера, определяющие стратегию, тактику и перспективы исследований по теме диссертации.

Сведения, представленные в Федеральном законе [127], ГОСТах [75 - 86] и нормативных документах ФСТЭК [122, 128, 129, 149, 151, 156], позволили определить методическую направленность исследований и законодательные требования к разрабатываемым методам.

Анализ теоретических и прикладных работ по теме исследования показал следующее:

- задаче обнаружения аномалий и нейтрализации угроз в АСУ промышленными объектами уделяется большое внимание со стороны научно-исследовательских и производственных организаций в России и за рубежом, однако большинство существующих методов ее решения не учитывают ряд особенностей, связанных с распределенностью автоматизированных систем и изменением характера угроз на всей протяженности объекта;

- в настоящее время наметилась тенденция контроля за состоянием ИБ территориально-распределенного технологического объекта посредством мониторинга сетевого трафика, как наиболее полного источника данных о состоянии распределенной автоматизированной системы;

- задача обнаружения аномалий в КС промышленных АСУ имеет свою специфику, связанную с необходимостью анализа больших объемов данных сетевого трафика и специализированных промышленных протоколов, таких как Modbus, Modbus TCP, CAN, HART, PROFIBUS, разрабатываемых с учетом особенностей производства.

К особенностям, определяющим эффективность решения задачи поиска аномалий в сетевом трафике, относятся:

- необходимость анализа больших объемов информации в режиме реального времени, передаваемой между подсистемами АСУ;
- различные форматы информации и сложность формализации запросов на поиск совокупности аномальных признаков в слабоструктурированных данных сетевого трафика;
- необходимость определения граничных значений ключевых признаков аномалии в сетевом трафике для снижения вероятности ошибок распознавания.

1.6.2 Обзор методов и средств мониторинга и анализа аномалий в АСУ ТП по данным сетевого трафика

Анализ структурно-функциональной организации и классификация основных аномалий в распределенной АСУ позволили выявить характерные особенности КС промышленных объектов, определяющих специфичность подхода к построению СЗИ:

- используемые средства защиты информации должны быть ориентированы на работу в территориально распределенных сетях;

- необходимо оперативное обнаружение аномалий, как проявлений инцидентов ИБ, и достоверная идентификация соответствующих им угроз БИ, приводящих к аварийным ситуациям на объекте;

- для выявления инцидентов ИБ необходимо обеспечение анализа значительного объема сетевого трафика как корпоративного сегмента, так и сегмента промышленной сети, содержащего специализированные протоколы и данные средств промышленной автоматизации;

- для передачи данных между сегментами АСУ используются сети общего пользования (Internet), что повышает вероятность реализации сетевых атак и несанкционированного удаленного доступа к узлам АСУ;

- для контроля и управления технологическим процессом необходимо обеспечение непрерывной работы КС АСУ, задержки в работе КС критичны;

- необходим контроль выполнения процедур обеспечения безопасности в действиях пользователей, попыток неавторизованных взаимодействий по промышленным протоколам, а также корректности (полномочности) использования предоставленных в доступ информационных ресурсов АСУ.

В научных публикациях по исследуемой тематике [58, 98, 179, 180] среди основных методов *обнаружения* аномалий в сетевом трафике КС выделяют:

- поведенческие методы на основе вейвлет-анализа, статистического, спектрального, кластерного, фрактального анализа, анализа энтропии;

- методы вычислительного интеллекта и машинного обучения на основе нейронных сетей, нечеткой логики, иммунных систем, опорных векторов, Байесовских сетей, деревьев решений, Мар-сплайнов, алгоритмов кластеризации, алгоритмов регрессии;

- методы на основе экспертных систем.

В таблице 1.2 и приложении В представлены результаты сравнительного анализа методов обнаружения аномалий в сетевом трафике АСУ.

Таблица 1.2 – Сравнительный анализ методов обнаружения аномалий в СТ

Методы обнаружения аномалий в сетевом трафике АСУ	**Достоинства**	**Недостатки**
Поведенческие методы на основе: - вейвлет-анализа, - статистического анализа, - спектрального анализа, - кластерного анализа, - фрактального анализа, - анализа энтропии.	- простота применения; - возможность обнаружения широкого спектра аномалий; - высокая оперативность; - высокая адаптивность к новым видам аномалий; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- наличие ложноположительных срабатываний из-за сложности построения профилей нормальной работы системы; - чувствительность к изменениям статистических характеристик трафика; - необходимость постоянной корректировки параметров обнаружения; - сложность обнаружения распределенной в пространстве и времени аномалии; - недостаточно достоверны в условиях изменения риска от угроз на последовательности подсистем распределенной АСУ.
Методы вычислительного интеллекта и машинного обучения на основе: - нейронных сетей, - нечеткой логики, - иммунных систем, - опорных векторов; - Байесовских сетей, - деревьев решений, - Мар-сплайнов, - алгоритмов кластеризации, - алгоритмов регрессии.	- высокая достоверность; - адаптивность; - способность обнаруживать новые виды аномалий; - способность автоматически обучаться на новых данных и выявлять сложные аномалии; **- эффективны для анализа аномалий в СТ АСУ ТП.**	- сложность построения; - высокие вычислительные затраты; - требуется большое количество размеченных данных для обучения; - сложности в интерпретации результатов.
Методы на основе экспертных систем	- высокая точность распознавания аномалии.	- низкая оперативность; - сложность построения нормального профиля работы АС; - потребность в больших объёмах знаний; - неэффективны при обнаружении неизвестных видов атак; **- неэффективны при обнаружении аномалий в СТ АСУ ТП.**

Анализ основных методов *обнаружения* аномалий в сетевом трафике АС показал, что **поведенческие методы** обладают высокой оперативностью и адаптивностью к новым видам аномалий, однако чувствительны к изменениям статистических характеристик трафика и недостаточно достоверны при обнаружении сложных аномалий в условиях изменения риска от угроз на последовательности подсистем распределенной АСУ. **Методы интеллектуального анализа данных и машинного обучения**, обладают высокой точностью и позволяют оперативно выявлять новые виды аномалии, но для обучения им требуются большие объемы размеченных данных, которые на практике бывает сложно получить. **Методы на основе экспертных систем** характеризуются низкой оперативностью, сложны в реализации и являются неэффективными при обнаружении аномалий в сетевом трафике АСУ ТП.

Методы на основе знаний (в частности, сигнатурный метод, методы на основе конечных автоматов, сетей Петри, экспертных систем), используемые для *распознавания* вида аномалии, являются эффективными для выявления известных типов атак, но их применимость по отношению к новым, а также к модификациям известных атак является безрезультативной.

Анализ публикаций показал, что для реализации методов обнаружения и распознавания аномалий необходим комбинированный подход, сочетающий различные методы. Перспективными являются решения, направленные на обнаружение аномалий на основе интеллектуального, статистического и спектрального анализа, и распознавание вида аномалии на основе сигнатурного подхода.

Программные и программно-аппаратные средства, реализующие перечисленные методы и представленные на российском рынке СЗИ, от компаний «InfoWatch», «Positive Technologes», «Лаборатория Касперского», «Уральский центр систем безопасности» [187, 190, 191, 201], позволяют решать задачи мониторинга аномалий и нейтрализации угроз в КС АСУ в соответствии с требованиями нормативных документов ФСТЭК. В таблице 1.3 представлены результаты анализа функциональности наиболее популярных средств, согласно требованиям приказа ФСТЭК [129], критериям, наиболее значимым с точки зрения экспертов

центров защиты АСУ ТП и объектов КИИ [164], с учетом характерных особенностей КС промышленных АСУ.

Таблица 1.3 – Анализ функциональности средств мониторинга и анализа аномалий в АСУ ТП по данным сетевого трафика

Средство мониторинга и анализа / **Функциональные критерии**	**KICS for Networks** (*Лаборатория Касперского)*	**ISIM** *(Positive Technologies)*	**DATAPK** *(УЦСБ)*
Мониторинг сетевого трафика без влияния на технологический процесс	+	+	+
Выявление аномалий на основе функции контроля изменения технологических параметров	+	+	-
Добавление пользовательских сигнатур в интерфейсе программы	-	+	+
Передача зарегистрированных событий в сторонние системы мониторинга (SIEM)	+	+	+
Интеграция с промышленными системами управления (SCADA)	+	+	+
Моделирование аномального промышленного СТ	-	-	-
Формирование отчётов	+	+	+
Построение маршрутов распространения атаки	+	+	+
Определение источников атаки	-	-	-
Контроль управляющих операций пользователей	+	+	+
Контроль управляющих транзакций пользователей	-	-	-
Маршрутизация технологического трафика при решении задач резервирования	-	-	-

Анализ статистики инцидентов ИБ и нормативных документов ФСТЭК показал, что наиболее серьезные требования по защите информации в КС АСУ ТП предъявляются в задачах сетевой и антивирусной защиты, регистрации и контроля действий пользователя системы, обеспечения непрерывности ТП и целостности технологической информации.

Обзор наиболее популярных решений, в частности, KICS for Networks (Лаборатория Касперского), Datapk (УЦСБ), ISIM (Positive Technologies) показал, что существующие решения акцентируют внимание на вопросах, связанных с предотвращением вторжений, и не обеспечивают необходимую производительность в отдельных задачах ИБ, в частности:

– при реализации мер, связанных *с обнаружением и предотвращением компьютерных атак*, присутствует функция построения маршрутов сетевых взаимодействий, однако отсутствует возможность анализа маршрутов развития атак и выявления источников распространения вредоносной информации, что необходимо для быстрой нейтрализации угрозы дальнейшего распространения вредоносного кода (УБИ.1 [53]);

– при реализации мер, связанных *с аудитом безопасности*, присутствуют функции контроля отдельных команд пользователей АСУ, однако отсутствует возможность их анализа как последовательности логически связанных операций (транзакций), что может привести к реализации угроз нерегламентированных управляющих действий персонала системы (УБИ. 061, УБИ. 063);

– при реализации мер, связанных *с защитой автоматизированной системы и обеспечением действий в нештатных ситуациях* отсутствуют функции быстрой маршрутизации сетевого трафика при переключении на резервные каналы связи, что может привести к потере технологической информации (УБИ. 136) и возможности возникновения аварии в результате несвоевременного выявления и реагирования на изменение параметров технологического процесса (УБИ. 214);

– при реализации мер, связанных *с аудитом безопасности и реагированием на компьютерные инциденты,* наблюдается снижение производительности средств защиты в случае необходимости анализа больших объемов СТ;

– отсутствуют функции кластеризации угроз и моделей угроз подсистем распределенной АСУ.

Результат сравнительного анализа средств обнаружения аномалий и нейтрализации угроз по данным сетевого трафика, проведенный в работах [23, 164, 177, 182, 1], показал, что, несмотря на значительные достижения в области обеспечения ИБ в промышленных АС, существующие методы и средства защиты недостаточно полно учитывают специфику распределенных систем управления, большие объемы информации, обрабатываемые СЗИ, переменный в пространстве и времени характер угроз. Исследования, проведенные в работах [45, 58], показали воз-

можность их совершенствования в части повышения производительности и достоверности работы.

Перечисленные факторы создают необходимость расширения функциональной полноты существующих решений и разработку новых высокопроизводительных методов и средств обнаружения аномалий и нейтрализации угроз БИ.

Анализ публикаций специалистов в исследуемой области, требований соответствующей нормативно-правовой базы и современных решений задачи исследования показал возможности повышения оперативности и достоверности методов и средств обнаружения, распознавания аномальных состояний АС на основе исследования и интеллектуальной обработки сетевых информационных потоков и позволил разработать концепцию снижения рисков ИБ на объектах КИИ.

1.7 Концепция исследования

Основная концепция диссертационной работы разработана на основе анализа публикаций специалистов в исследуемой области, с учетом требований соответствующей нормативно-правовой базы, критериев оценки качества защиты информации на объектах КИИ, направлена на снижение рисков ИБ за счет высокопроизводительных методов и средств оперативного и достоверного обнаружения, распознавания аномальных состояний АС, как проявлений инцидентов ИБ, нейтрализации связанных с ними угроз на основе исследования и интеллектуальной обработки сетевых информационных потоков. Концепция определена следующими аспектами.

1. Разработка метода кластерного анализа угроз и МУ БИ для подсистем распределенных объектов КИИ на основе ортогональных средних значений рисков для определения характера изменения актуальности угроз на последовательности подсистем распределенной АСУ ТП и приоритетности их нейтрализации.

2. Разработка метода построения математических и имитационных моделей для обнаружения аномалий, идентификации аномальных состояний КС АСУ, как проявлений инцидентов ИБ вследствие реализации угроз. Для решения задачи об-

наружения аномалий выбран дихотомический подход с использованием разделяющей функции мажоритарного вида, позволяющий путем деления интервала неопределенности пополам оперативно и достоверно определять нормальное, либо аномальное состояния АСУ. Идентификация вида аномалии осуществляется на основе ассоциативно-мажоритарного подхода за счет поиска ассоциативных связей между признаками и образами аномальных состояний и процессов, что позволяет повысить производительность, достоверность, универсальность средств обнаружения аномалий и нейтрализации угроз.

4. Разработка алгоритмов, методик и программной реализации методов и средств обнаружения аномалий и нейтрализации угроз в задачах: идентификации источников и маршрутов распространения вредоносного кода, определения резервных маршрутов передачи данных в промышленной КС, мониторинга действий персонала автоматизированных систем - на основе ассоциативного подхода и мажоритарного принципа принятия решений.

5. Экспериментальная оценка эффективности результатов исследований и разработка рекомендаций по их практическому применению в распределенных АС на примере системы управления процессом транспортировки нефтегазового сырья.

Определенная выше стратегия наряду с результатами исследований, представленными в работах [23, 45, 70], позволила определить особенности решения задачи диссертационного исследования:

- принятие решений по выбору оптимальной стратегии обнаружения аномалий и нейтрализации угроз осуществляется на основе системного подхода, предполагающего анализ всех актуальных угроз для объекта информатизации, выбор и обоснование целевой функции и критериев оценки результатов исследований;

- решение задачи идентификации аномальных состояний распределенных автоматизированных систем производится на основе модели угроз, разработанной с учетом требований соответствующей нормативно-правовой базы ФСТЭК РФ;

- в качестве источника исходной информации для обнаружения и идентификации аномалий используется сетевой трафик, как доступный поток информации обо всех подсистемах АСУ;

- в качестве инструментального аппарата использованы математические и имитационные модели, построенные на основе теории информационной безопасности, теории вероятности, теории принятия решений, теории распознавания образов, теории графов;

- основными результатами исследования являются методы, алгоритмы, методики и программная реализация средств обнаружения аномалий и нейтрализации угроз по данным сетевого трафика в задачах идентификации источников и маршрутов распространения вредоносного кода, определения резервных маршрутов передачи данных в промышленной КС, мониторинга действий персонала автоматизированных систем, отвечающие требованиям высокой достоверности и производительности и позволяющие снизить риски ИБ в системах защиты распределенных объектов информатизации.

Разработанные методы и методики должны отвечать следующим требованиям:

- выполнение требований руководящих документов ФСТЭК РФ и нормативных документов к СЗИ в АСУ объектов КИИ, в частности, транспортировкой нефтегазового сырья;

- высокая производительность, в частности, оперативность и достоверность распознавания аномалии по данным сетевого трафика и принятия решения по нейтрализации соответствующей ей угрозе;

- адекватные затраты на систему мониторинга сетевого трафика, не превышающие ущерб от реализации угроз БИ;

- возможность интеграции разработанных методов и средств в существующую систему защиты информации распределенной АСУ;

- разрабатываемые методы и средства должны обеспечивать надежное и безопасное функционирование распределенной АСУ с учетом ее особенностей во всех предусмотренных режимах работы оборудования.

1.8 Выводы по первой главе

Анализ современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой на примере КС АСУ ТП транспортировки нефтегазового сырья выявил необходимость разработки новых методов и средств, обеспечивающих решение задач оперативного поиска данных о состоянии системы, достоверной идентификации, оценки состояния и принятия решения по нейтрализации соответствующей угрозы безопасности информации.

Анализ целевой функции позволил определить в качестве основных требований к разрабатываемым методам оперативность и достоверность обнаружения, идентификации аномалии и нейтрализации угрозы БИ, при допустимых параметрах производительности и затрат для их достижения.

Анализ структурно-функциональной организации распределенной АСУ ТП как объекта защиты позволил подвести задачу обнаружения аномалий к задаче разработки методов и средств распознавания состояний КС АСУ на основе исследования и интеллектуальной обработки потоков сетевого трафика, циркулирующего между узлами системы.

На основе анализа публикаций специалистов в исследуемой области, с учетом требований соответствующей нормативно-правовой базы, критериев оценки качества защиты информации на объектах с КИИ, разработана основная концепция диссертационной работы: снижение риска ИБ за счет высокопроизводительных методов и средств оперативного и достоверного обнаружения, распознавания аномальных состояний АС, как проявлений инцидентов ИБ, нейтрализации связанных с ними угроз на основе исследования и интеллектуальной обработки сетевых информационных потоков.

Выбранная стратегия определила необходимость разработки метода построения математических и имитационных моделей и модельного базиса задачи оперативного обнаружения аномалий и нейтрализации угроз в распределенных системах управления на основе мониторинга сетевых информационных потоков.

ГЛАВА 2. РАЗРАБОТКА МЕТОДА ПОСТРОЕНИЯ МАТЕМАТИЧЕСКИХ И ИМИТАЦИОННЫХ МОДЕЛЕЙ И МОДЕЛЬНОГО БАЗИСА ЗАДАЧИ ОБНАРУЖЕНИЯ АНОМАЛИЙ И НЕЙТРАЛИЗАЦИИ УГРОЗ БИ НА ОСНОВЕ ДАННЫХ МОНИТОРИНГА СЕТЕВОГО ТРАФИКА

2.1 Классификация моделей задачи обнаружения аномалий и нейтрализации угроз в распределенных автоматизированных системах

Разработка методов и средств мониторинга и анализа сетевого трафика должна опираться на адекватные модели и инструменты моделирования процессов защиты информации. К настоящему времени разработано и апробировано на практике множество моделей, позволяющих эффективно решать задачи мониторинга состояния АСУ различной природы и архитектуры [73, 87, 93, 97, 113, 114]. Однако существующие модели не полностью учитывают специфику распределенных систем управления (РСУ), работающих в условиях пространственных и временных возмущений.

Целью настоящего раздела является определение перечня моделей для решения задачи обнаружения аномалий и нейтрализации угроз в распределенных системах управления.

Анализ задачи исследования, проведенный в первой главе, и положения ГОСТ [60] предопределили разбиение множества разрабатываемых моделей на 4 класса по этапам исследования: модели для определения требований к техническим решениям, модели для определения системных решений, модели для определения частных (подсистемных) решений, модели для исследования эффективности разработок. Модельный базис задачи обнаружения аномалий и нейтрализации угроз в распределенных АСУ представлен на рисунке 2.1.

Первая группа моделей предназначена для описания АСУ как объекта защиты и определения требований к разрабатываемым методам.

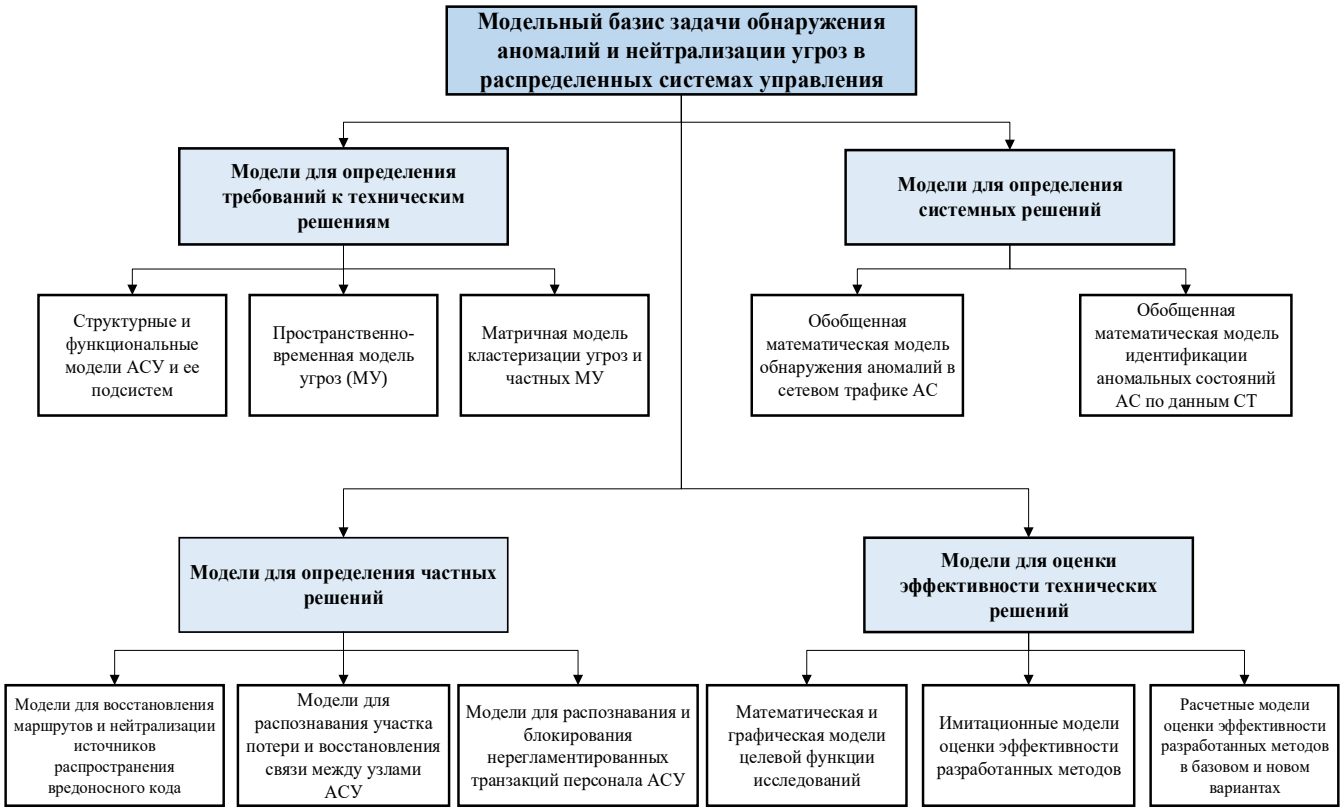


Рисунок 2.1 – Модельный базис задачи обнаружения аномалий и нейтрализации угроз в распределенных АСУ

Структурные и функциональные модели распределенной АСУ транспортировкой нефтегазового сырья предназначены для представления ее структуры, функциональных подсистем, информационных потоков и позволяют определить качественный состав сетевого трафика, как предмета исследования. Модели представлены в разделе 1.3.

П*ространственно-временная модель угроз (МУ) и модель кластеризации угроз и частных МУ для АСУ транспортировкой нефтегазового сырья* позволяют определить основную концепцию исследования и стратегию защиты информации для исследуемого класса промышленных объектов. Модели представлены в разделах 2.2 – 2.3.

Разработка моделей первой группы позволяет выявить особенности функционирования АСУ в условиях воздействия пространственно-временных угроз, определить концепцию защиты информации в системе и требования к разрабатываемым техническим решениям.

Вторая группа моделей предназначена для определения системных решений, позволяющих усовершенствовать методы обнаружения аномалий и нейтрализации угроз на всех этапах: поиска сведений об аномалии, выбора наиболее достоверного результата, принятия решения по нейтрализации угрозы.

Обобщенные математические модели для обнаружения аномалий и идентификации аномального состояния КС, представленные в разделах 2.4 - 2.5, предназначены для оперативного обнаружения и распознавания аномальных состояний КС АСУ и достоверного принятия решений по их нейтрализации. Концепция построения моделей основана на использовании дихотомического и ассоциативно-мажоритарного подходов, обеспечивающих максимально возможную производительность средств мониторинга и высокую достоверность принятия решений на основе принципов мажоритарности.

Модели для определения частных решений необходимы для разработки методик и методов обнаружения аномалий, связанных с наиболее актуальными угрозами: распространения вредоносного кода в системе, потери связи между подсистемами АСУ, нерегламентированных действий пользователей.

Графо-аналитическая модель восстановления маршрутов распространения вредоносного кода по фрагментам данных сетевого трафика предназначена для идентификации источников и нейтрализации вредоносного воздействия зараженных узлов.

С целью минимизации потерь информации при ее передачи между подсистемами АСУ разработаны *графовая модель переключения потоков сетевого трафика* и *имитационная модель маршрутизации сетевых потоков в режимах переключения на резервные каналы связи.* Данные модели необходимы для определения оптимального маршрута передачи данных при использовании методов горячего резервирования.

Графовая модель контроля управляющих транзакций персонала АС предназначена для анализа и контроля управляющих воздействий на объект в режиме реального времени. Модели третьей группы представлены в разделах 3.1.1, 3.2.1 и 3.3.1 соответственно.

Группа моделей для оценки эффективности технических решений включает: *математическую и графическую модели целевой функции исследований*, представленную в разделе 1.2; *расчетные модели оценки эффективности* разработанных методов, представленные в разделах 4.1 – 4.2. Данная группа моделей позволяет выявить особенности работы методов и средств обнаружения аномалий и нейтрализации угроз и определить границы их эффективности.

Перечисленные модели отличаются следующими особенностями [17]:

- модели позволяют в динамике исследовать процессы функционирования сложных систем управления;
- охватывают основные вопросы построения систем защиты, осуществляющих мониторинг и диагностирование состояния распределенных АСУ;
- ориентированы на конкретный технологический объект - системы транспортировки нефтегазового сырья.

Обзор существующих моделей обнаружения аномалий по данным сетевого трафика [97, 126, 175, 203, 204] показал, что для получения полной информации о состоянии КС АСУ невозможно использовать ограниченный класс моделей. Это приводит к необходимости разработки обобщенных моделей для обнаружения и распознавания аномального состояния КС и моделей для определения частных решений, необходимых для разработки методик и методов защиты от наиболее актуальных угроз.

Для анализа актуальных угроз, определяющих аномальные состояния сетевого трафика, и определения приоритетности их нейтрализации проведено исследование базовой модели угроз (МУ) для распределенной АСУ процессом транспортировки нефтегазового сырья.

2.2 Характеристика базовой модели угроз для распределенной АСУ процессом транспортировки нефтегазового сырья

Под угрозой безопасности информации в АСУ понимается совокупность условий и факторов, создающих потенциальную или реальную существующую опасность несанкционированных и (или) непреднамеренных воздействий на информацию, обрабатываемую в системе, и способных привести к возникновению чрезвычайных ситуаций или к нарушению выполняемых системой функций со значительными негативными последствиями. Согласно приказам ФСТЭК России [127, 151] анализ угроз безопасности информации в отношении объекта КИИ является одной из обязательных мер защиты.

Вопросы разработки и анализа моделей угроз (МУ) для АСУ рассматриваются в научно-технической литературе, нормативных документах и рекомендациях ФСТЭК [53, 90, 120, 122, 55]. Однако в доступных источниках недостаточно внимания уделено вопросам исследования МУ для сложных систем управления, для которых характерны различия в характеристиках антропогенных, техногенных и природных угроз между подсистемами, топологически распределенными в заданном географическом регионе.

Объектом исследования в настоящем разделе является базовая МУ для КС АСУ транспортировкой нефтегазового сырья одного из месторождений Оренбургской области. Выбор этой системы обусловлен ее техническими и эксплуатационными характеристиками, присущими большинству распределенных АСУ транспортировкой нефтегазового сырья.

Целью характеристики базовой МУ для исследуемой АСУ является определение системы требований к СЗИ, учитывающей особенности распределенного объекта информатизации.

Анализ базовой МУ проводился на основе реальных характеристик объектов нефтегазовой отрасли Оренбургской области, результатов экспертного опроса сотрудников ООО «УЦСБ» и положений следующих методических документов ФСТЭК России:

− «Методика оценки угроз безопасности информации» [122];

− «Банк данных угроз безопасности информации» [53];

− «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [151];

− «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» [156].

Контекстная диаграмма процесса разработки модели угроз для распределенной АСУ ТП, построенная на основе методологии IDEF0 [6, 123], представлена на рисунке 2.2.

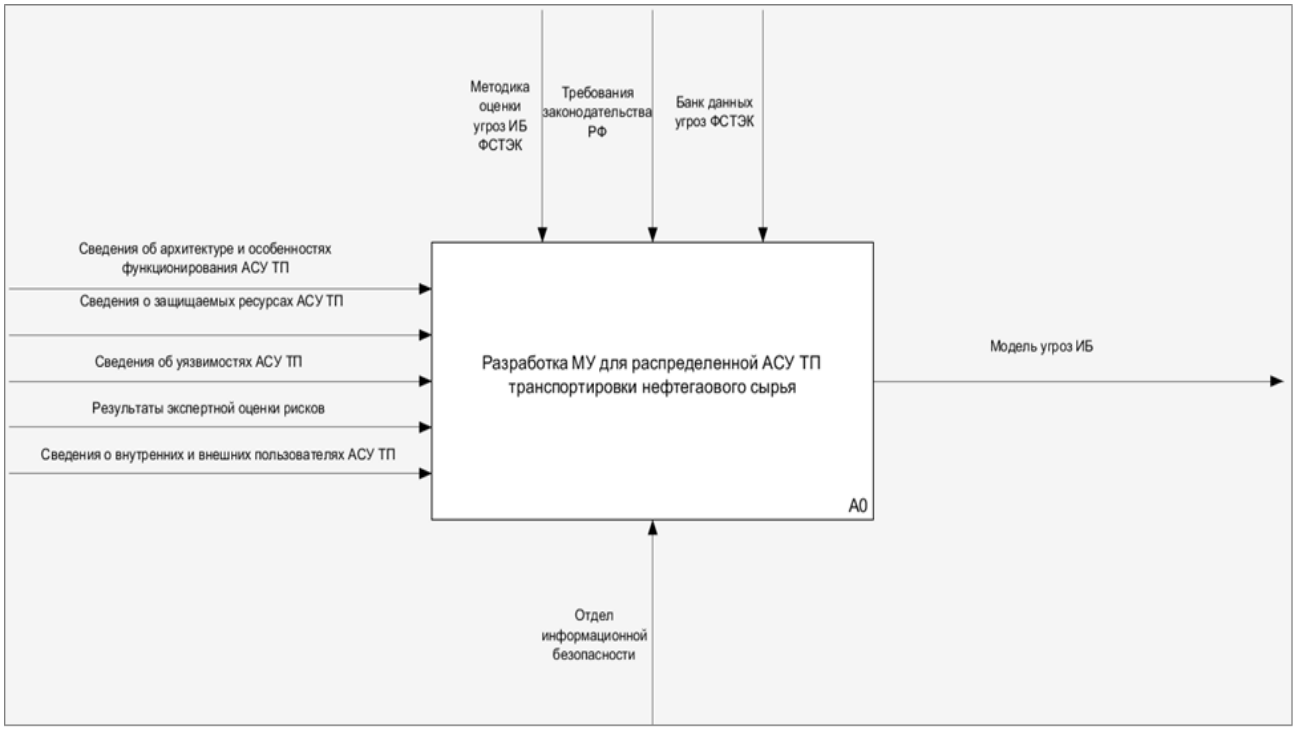


Рисунок 2.2 – Контекстная диаграмма процесса разработки модели угроз для распределенной АСУ ТП

Декомпозиция контекстной диаграммы, представленная на рисунке 2.3, отражает основные этапы разработки МУ для исследуемого объекта, согласно «Методике…» [122] ФСТЭК.

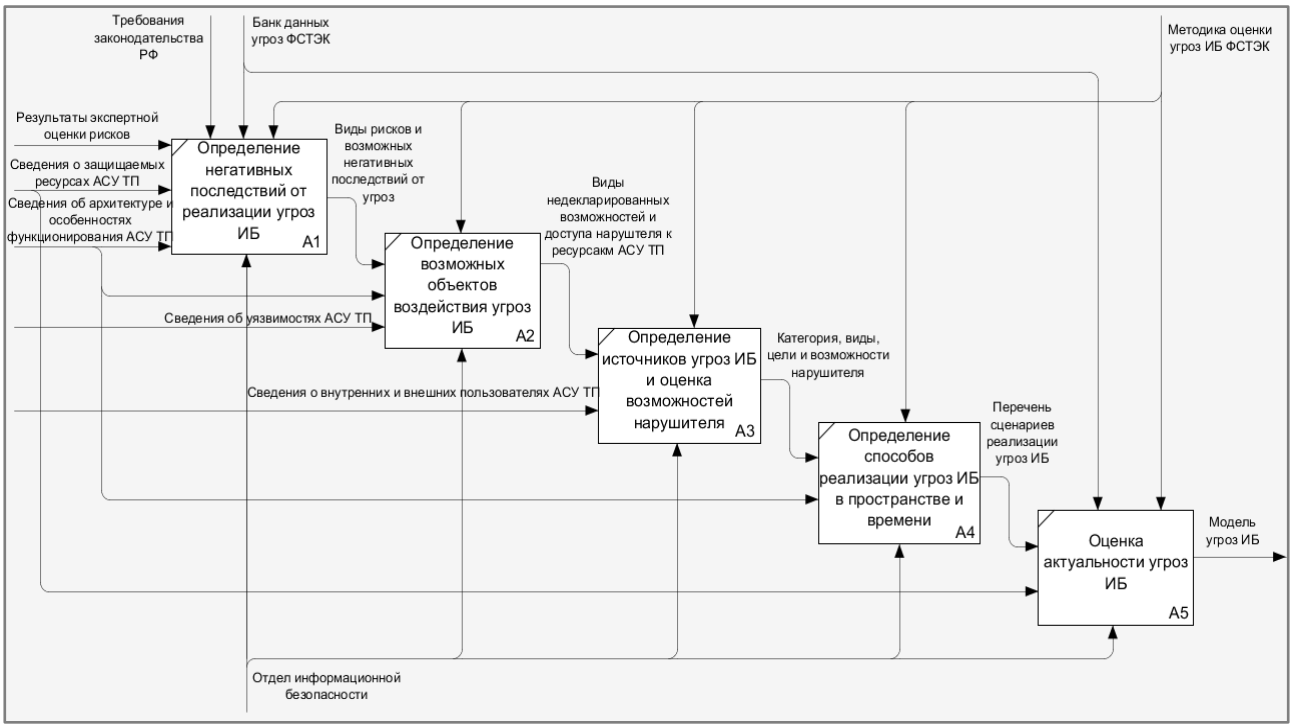


Рисунок 2.3 – Декомпозиция контекстной диаграммы

К негативным последствиям от реализации угроз в базовой МУ отнесены следующие виды риска (ущерба):

– ущерб физическому лицу - угроза жизни и здоровью людей;

– риски юридическому лицу: недополучение ожидаемой прибыли, причинение имущественного ущерба и необходимость дополнительных затрат на восстановление деятельности, нарушение штатного режима функционирования АСУ и снижение эффективности ее работы, утечка конфиденциальной информации и нарушение деловой репутации;

– ущерб государству: прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, возникновение ущерба бюджетам Российской Федерации, вредные воздействия на окружающую среду.

В качестве основных объектов воздействия угроз выделены:

- АРМы АСУ ТП;
- серверы АСУ ТП;
- специальное ПО (SCADA-систем, СУБД) серверов и АРМов;
- программируемые контроллеры;

- датчики и исполнительные механизмы;
- телекоммуникационное оборудование и средства связи;
- каналы связи;
- технологическая и конфиденциальная информация;
- персонал АСУ.

В отношении перечисленных объектов возможны следующие виды деструктивных воздействий:

- копирование, уничтожение, модификация, блокирование, перехват, разглашение и хищение конфиденциальной информации;

- блокировка и несанкционированное управление технологическим процессом (ТП), приводящие к потере управления ТП оператором;

- фальсификация и модификация параметров ТП, приводящие к потере видимости информации о процессе;

- модификация параметров ТП, приводящая к останову и аварии на объекте;

- деградация вычислительных ресурсов, приводящая к отказу в обслуживании;

- сокрытие следов преступлений.

В качестве потенциальных нарушителей информационной безопасности определены:

– криминальные структуры;

– представители конкурирующих фирм и организаций, иностранных экономических структур, деятельность которых направлена против интересов государственных структур Российской Федерации, крупных компаний, организаций и предприятий;

– отдельные посторонние лица или группы лиц с корыстными или иными интересами (хакеры и т.п.);

– пользователи АСУ ТП (оператор, диспетчер, работники, осуществляющие планирование переключений);

– персонал, обеспечивающий поддержку и сопровождение (администраторы АСУ ТП, СУБД, АРМ);

– лица, имеющие доступ в помещения, где располагаются АСУ ТП, но не имеющие легитимных прав доступа к системе (технический персонал, работники фирм-подрядчиков, посетители).

Анализ возможностей нарушителей показал, что наибольшую опасность представляют хакеры, организующие атаки на АСУ, а также пользователи и персонал системы. Данные категории нарушителей имеют профессиональную подготовку в сфере информационных технологий и могут получить доступ на объект в ходе выполнения профессиональных обязанностей, либо в результате удаленной атаки на компоненты системы.

Для определения возможных сценариев атак были использованы приведенные в «Методике…» [122] тактики и техники (в частности, T_1: $T_{1.3}$ - $T_{1.6}$, $T_{1.8}$, $T_{1.9}$, $T_{1.11}$, $T_{1.12}$, $T_{1.13}$, $T_{1.16}$ - $T_{1.20}$; T_2: $T_{2.1}$ – $T_{2.13}$; T_3: $T_{3.1}$ – $T_{3.3}$, $T_{3.5}$, $T_{3.8}$, $T_{3.9}$, $T_{3.14}$, $T_{3.16}$; T_4: $T_{4.1}$ – $T_{4.7}$; T_5: $T_{5.1}$ – $T_{5.11}$; T_6: $T_{6.1}$ – $T_{6.8}$; T_7: $T_{7.1}$ – $T_{7.8}$, $T_{7.10}$ – $T_{7.25}$; T_8: $T_{8.1}$ – $T_{8.8}$; T_9: $T_{9.1}$ – $T_{9.13}$; T_{10}: $T_{10.1}$ - $T_{10.3}$, $T_{10.7}$ - $T_{10.15}$), а также информация из банка данных угроз ФСТЭК.

Проведенный анализ статистических данных научных публикаций, материалов Интернет-источников, моделей угроз промышленных объектов АСУ транспортировкой нефтегазового сырья позволил определить перечень актуальных угроз с высоким и очень высоким коэффициентом опасности, характерных для рассматриваемого класса АСУ, и степень их опасности.

Соответствующий перечень представлен в таблице 2.1. Порядок представления угроз в таблице имеет регистрационный характер, не связанный со степенью их актуальности.

Анализ результатов исследования показал, что угрозы, источники и характер реализации которых связаны с сетевыми каналами передачи информации, составляют более 50 % из перечня актуальных угроз.

Таблица 2.1 – Актуальные угрозы для распределенной АСУ ТП транспортировки нефтегазового сырья с высоким коэффициентом опасности

Наименование угрозы	Вероятность реализации угрозы	Коэффициент опасности угрозы	Актуальность угрозы
Инсталляция и запуска вируса	Средняя	Очень высокая	Актуальная
Определение типа ОС маршрутизатора	Высокая	Высокая	Актуальная
Выявление маршрутов прохождения пакетов информации	Высокая	Высокая	Актуальная
Получение доступа к программам удалённого администрирования посредством ввода имени и пароля, заданных по умолчанию для используемой ОС	Высокая	Высокая	Актуальная
Внедрение ложного доверенного объекта (ARP-spoofing, IP-spoofing, DNS-spoofing)	Высокая	Высокая	Актуальная
Переполнение буфера с запуском исполняемого кода	Высокая	Высокая	Актуальная
Инсталляция программного обеспечения «шпион клавиатуры»	Средняя	Очень высокая	Актуальная
Инсталляция программного обеспечения, разрушающего аппаратное обеспечение компьютера	Средняя	Очень высокая	Актуальная
Инсталляция программ удалённого управления	Средняя	Очень высокая	Актуальная
Перехват трафика маршрутизатора	Высокая	Очень высокая	Актуальная
Посылки скрытых вредоносных программ	Высокая	Очень высокая	Актуальная
Запуск программ с удалённого узла	Высокая	Очень высокая	Актуальная
Атаки, основанные на уязвимостях Web-серверов	Высокая	Очень высокая	Актуальная
Использование ошибок в сценариях автоматизации	Высокая	Очень высокая	Актуальная
Обход межсетевого экрана	Высокая	Очень высокая	Актуальная
Нерегламентированные действия пользователей, ошибки при эксплуатации технических средств	Средняя	Очень высокая	Актуальная
Сбой, отказ технических средств	Средняя	Очень высокая	Актуальная
Отказ оборудования связи	Средняя	Очень высокая	Актуальная
Угроза физического выведения из строя средств передачи информации	Высокая	Очень высокая	Актуальная
Сбой, отказ программных средств	Средняя	Очень высокая	Актуальная

Особенностью построения СЗИ для исследуемого объекта является необходимость учета условий и факторов, зависящих от места и времени их проявления и влияющих на работу каждой из подсистем АСУ. Анализ значений рисков от актуальных угроз для различных подсистем территориально распределенной АСУ позволил выявить следующие особенности:

- построение МУ для распределенного объекта защиты сопряжено с такими сложностями, как разнообразный характер угроз антропогенного, техногенного и природного типа на различных его участках;
- значения рисков от угроз меняется для каждой из подсистем;
- СЗИ, построенная на основе базовой МУ для всей АСУ, может быть адекватной для одних участков, но избыточной, либо недостаточной для других.

Особенности топологического расположения распределенных АСУ ТП (протяженность в пространстве, удаленность компонентов АСУ от пунктов операторского и диспетчерского управления, рельеф местности, метеорологические условия) и различие факторов, влияющих на значения рисков ИБ, обуславливают исследование угроз безопасности информации для каждой из ее подсистем. Перечисленные особенности создают необходимость анализа базовой модели угроз в виде множества частных МУ для каждой из подсистем и оценку рисков от каждой угрозы для каждой подсистемы. С целью выявления приоритетных угроз для каждой подсистемы и снижения временных и стоимостных затрат на создание и модернизацию СЗИ разработан метод кластеризации угроз и моделей угроз для подсистем распределенной АС.

2.3 Метод кластеризации угроз и моделей угроз БИ для подсистем распределенных объектов КИИ на основе ортогональных средних значений рисков

Одним из факторов эффективной защиты АСУ является построение адекватной модели угроз безопасности информации (БИ). Вопросы построения и анализа МУ для АСУ подробно рассмотрены в современной литературе, в частности,

в работах [90, 120, 205]. Однако в доступной литературе недостаточно внимания уделено вопросам построения и исследования моделей угроз для распределенных управляющих систем, в частности, не рассматриваются вопросы систематизации и анализа МУ для подсистем распределенных АСУ. Индивидуальный подход к исследованию МУ для каждой из подсистем АСУ позволит устранить избыточность СЗИ на одних участках и усилить защиту на других.

Целью настоящего раздела является исследование частных МУ для различных подсистем распределенных АСУ в условиях воздействия угроз различного типа. Целью исследования является построение адекватной системы защиты информации на каждом участке АСУ на основе дифференцированного подхода, позволяющего снизить временные и стоимостные затраты на создание и модернизацию СЗИ.

Для достижения цели были решены следующие задачи:

- выявлены особенности построения пространственно-временной модели угроз (ПВМУ) для распределенной управляющей системы транспортировки нефтегазового сырья;

- обоснована целесообразность применения кластерного анализа при исследовании ПВМУ в виде частных моделей угроз;

- разработана математическая модель кластеризации угроз и частных моделей угроз для подсистем распределенных АСУ;

- разработаны алгоритм, программное средство и метод кластеризации угроз и частных моделей угроз для подсистем распределенных АСУ;

- проведен кластерный анализ угроз и моделей угроз для подсистем распределенной АСУ процессом транспортировки нефтегазового сырья;

- даны рекомендации по совершенствованию существующей СЗИ в АСУ.

Кластерный анализ угроз и моделей угроз проводился с учетом реальных характеристик АСУ транспортировкой нефтегазового сырья, топологическая схема участка которой представлена на рисунке 1.2. Исследуемая АСУ ТП разделена на подсистемы по функционально-топологическому принципу на этапе ее разработки (как показано на рисунке 1.2). На рисунке оси координат *NLat* и *ELong* по-

казывают координаты северной широты и восточной долготы соответственно, *SubS1 – SubS10* – исследуемые подсистемы АСУ.

Исследование влияния угроз БИ на каждую из подсистем АСУ показало переменный в пространстве и времени характер угроз на всей протяженности объекта. Пространственные угрозы обусловлены распределенной топологией систем управления, характеризуемой изменчивостью рельефа местности, близостью дорог и населенных пунктов. Временные угрозы обусловлены климатическими условиями (например, весенними паводками вблизи рек), режимами эксплуатации системы, а также характеристиками износа оборудования.

Риск информационной безопасности для *i*-ой угрозы вычисляется по формуле $R_i = P_i * U_i$, где P_i – вероятность реализации *i*-ой угрозы; U_i –ущерб от реализации *i*-ой угрозы. Общее значение риска $R_{общ}$ для распределенной системы складывается из значений рисков от каждой угрозы для каждой из подсистем и вычисляется по формуле (1.1), приведенной в разделе 1.2.

Каждая подсистема характеризуется особенностями ее эксплуатации, расположения ее узлов, их функционирования в течение года. Эти особенности напрямую влияют на содержание частных МУ каждой подсистемы. Пространственные координаты (x_j, y_j) определяют границы подсистем. Они влияют на вероятность реализации угроз, связанных с особенностями рельефа местности и расположением вблизи объекта автомобильных дорог, городов, поселков. Временные характеристики работы системы *t* определяют периодичность и сезонность проявления угроз.

Переменный в пространстве и времени характер угроз для каждой из подсистем АСУ привел к необходимости дифференцированного подхода к построению СЗИ и анализа базовой модели в виде частных МУ в частности, а в целом – общей пространственно-временной модели угроз (ПВМУ) [25].

Для решения задачи анализа ПВМУ целесообразно все множество угроз и частных МУ сгруппировать в кластеры по определенному признаку (например, по ортогональным средним значениям рисков). Для решения задачи кластеризации частных МУ используется модифицированный метод k-средних, отличающийся

оперативностью работы и простотой реализации. При решении задачи исследования ПВМУ распределенных АСУ кластерный анализ позволяет:

- систематизировать множество угроз и частных моделей угроз;

- уменьшать вычислительную сложность задачи анализа большого числа частных МУ;

- выявлять наиболее значимые угрозы и группы подсистем с недостаточным, либо избыточным уровнем защищенности в зависимости от условий их работы.

Задача кластерного анализа частных МУ представляется следующим образом. Пусть дано:

- $M = \{M_1, M_2, ..., M_N\}$ - множество частных МУ, каждая из которых содержит конечный перечень угроз БИ;

- N – общее число частных МУ для N подсистем;

- $U = \{U_1, U_2, ..., U_L\}$ – множество угроз БИ;

- L – общее число угроз БИ.

Задача кластерного анализа заключается в построении множества кластеров. Каждый кластер включает перечень угроз из множества U при кластеризации угроз, либо частных МУ из множества M при кластеризации МУ. Значения рисков R_{ij} одних и тех же угроз близки для всех угроз или частных МУ, входящих в один кластер.

Математическое описание процедуры кластерного анализа ПВМУ по угрозам представлено в выражениях (2.1) - (2.3), по моделям угроз - (2.4) – (2.6).

$$K_l = k_{l1}, k_{l2}, \dots k_{ln}, \dots, k_{lN}; \quad (2.1)$$

$$k_{ln} = \begin{cases} 1, \text{если } R_{ln} \geq s_l; \\ 0, \text{если } R_{ln} < s_l; \end{cases} \quad (2.2)$$

$$s_l = \frac{\sum_{n=1}^{N} R_{ln}}{N}, l = 1, L; \quad (2.3)$$

$$K_n = k_{1n}, k_{2n}, \dots, k_{ln}, \dots, k_{Ln}; \quad (2.4)$$

$$k_{ln} = \begin{cases} 1, \text{если } R_{ln} \geq s_n; \\ 0, \text{если } R_{ln} < s_n; \end{cases} \quad (2.5)$$

$$s_n = \frac{\sum_{l=1}^{L} R_{ln}}{L}, n = 1, N, \quad (2.6)$$

где R_{ln} – значение риска l-ой угрозы n-ой модели, s_l – среднее значение риска по угрозе, s_n – среднее значение риска по модели угроз. Число угроз L одинаково для

каждой из частных МУ и определяется количеством угроз в модели угроз для АСУ.

Математическая модель кластеризации угроз и частных МУ может быть представлена в виде двумерной матрицы, изображенной на рисунке 2.4. По строкам матрицы располагаются наименования угроз, по столбцам – идентификаторы частных МУ.

Частные МУ / Угрозы	***МУ1***	***МУ2***	***МУ3***	**…**	***МУ$_N$***	**Совокупный классификационный код угрозы**
У1	$k^h_{1.1}$ / $k^v_{1.1}$	$k^h_{1.2}$ / $k^v_{1.2}$	$k^h_{1.2}$ / $k^v_{1.2}$	…	$k^h_{1.N}$ / $k^v_{1.N}$	$k^h_{1.1}, k^h_{1.2\ \ldots}\ k^h_{1.N}$
У2	$k^h_{2.1}$ / $k^v_{2.1}$	$k^h_{2.2}$ / $k^v_{2.2}$	$k^h_{2.2}$ / $k^v_{2.2}$	…	$k^h_{2.N}$ / $k^v_{2.N}$	$k^h_{2.1}, k^h_{2.2\ \ldots}\ k^h_{2.N}$
…	…	…	…	…	…	…
У$_L$	$k^h_{L.1}$ / $k^v_{L.1}$	$k^h_{L.2}$ / $k^v_{L.1}$	$k^h_{L.2}$ / $k^v_{L.1}$	…	$k^h_{L.N}$ / $k^v_{L.N}$	$k^h_{L.1}, k^h_{L.2\ \ldots}\ k^h_{L.N}$
Совокупный классификационный код модели угроз	$k^v_{1.1}, k^v_{2.1\ \ldots}$ $k^v_{L.1}$	$k^v_{1.2}, k^v_{2.2\ \ldots}$ $k^v_{L.2}$	$k^v_{1.2}, k^v_{2.2\ \ldots}$ $k^v_{L.2}$	…	$k^v_{1.N}, k^v_{2.N\ \ldots}$ $k^v_{L.N}$	Пример классификационного кода: 1011100

Рисунок 2.4 - Матрица кластеризации угроз и частных моделей угроз для подсистем АСУ

Мера сходства при объединении в кластеры определяется по бинарным классификационным кодам (КД)**.** Составляющие КД k_{ln} рассчитываются на основе средних значений рисков по угрозам (горизонтальная кластеризация - ГК) и по моделям угроз (вертикальная кластеризация - ВК), где единицы характеризуют превышение конкретной оценки риска над средним значением ее по горизонтали или вертикали. Количество единиц в КД МУ позволяет выявить наиболее значимые угрозы для конкретной подсистемы АСУ (либо временного периода при анализе изменения характера угроз во времени). Количество единиц в КД угрозы позволяет судить о степени ее актуальности и приоритетности нейтрализации данной угрозы для распределенной АСУ.

Кластеризация угроз ***У*** проводится по совокупным КД, формируемым по строкам таблицы, что позволяет выявить значимые для каждой из подсистем (либо периода времени) угрозы и определить приоритетные направления для разработки СЗИ. Кластеризация моделей угроз *МУ* проводится по классификационным

кодам, формируемым по столбцам таблицы, и позволяет сделать вывод о значимости каждой угрозы для каждой подсистемы, выявить группы подсистем с недостаточным, либо избыточным уровнем защиты и уменьшить вычислительную сложность задачи анализа большого числа МУ. Особенностью метода кластеризации является представление и анализ рисков в процентном соотношении от общего риска модели угроз (начального или остаточного), что позволяет проводить исследование на основе системного подхода.

Схема алгоритма кластеризации угроз и частных МУ представлена на рисунке 2.5.

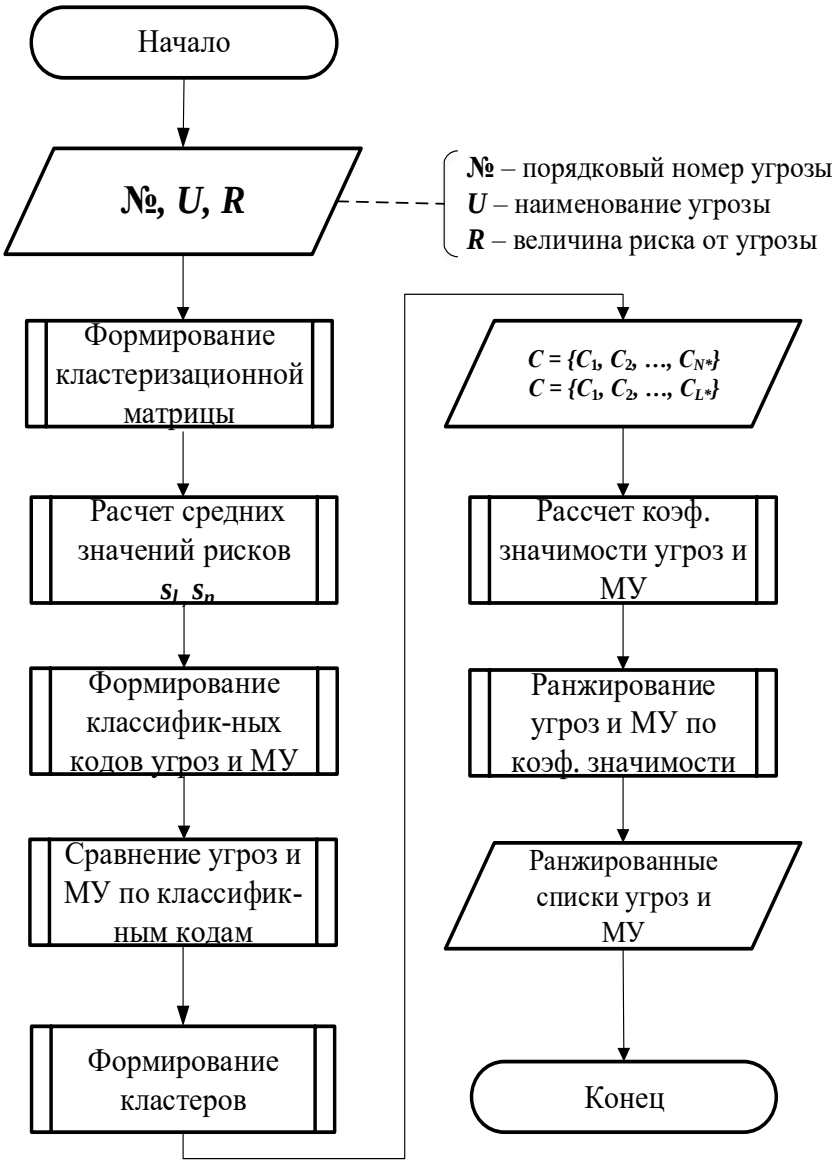


Рисунок 2.5 - Схема алгоритма кластеризации угроз и частных МУ

В качестве исходных данных для анализа выступает множество угроз и частных моделей угроз. Частные МУ представлены в виде матриц, в строках которых содержатся порядковые номера угроз, а в столбцах - данные о наименовании угрозы и значении риска от угрозы (в числовом или процентном формате). В результате анализа исходное множество угроз и частных МУ, объединяется в множество кластеров, содержащее L^* (при вертикальной кластеризации) и N^* (при горизонтальной кластеризации) элементов соответственно. На завершающем этапе проводится ранжирование угроз и моделей угроз по классификационным кодам.

Для исследования ПВМУ было разработано программное средство [8], реализующее представленные модель и алгоритм. Листинг программного средства представлен в приложении Ж. Экранная форма работы программы представлена на рисунке 2.6. Разработанные модель, алгоритм и программа положены в основу метода матричной кластеризации угроз и моделей угроз (МУ) на основе статистической обработки значений рисков.

На основе статистических данных научных публикаций, материалов Интернет-источников, моделей угроз промышленных объектов АСУ транспортировкой нефтегазового сырья - с использованием разработанного метода кластеризации и реестра угроз ФСТЭК - проведена оценка актуальности угроз для каждой из десяти подсистем исследуемой АСУ.

При построении частных МУ были выбраны основные группы актуальных угроз, характерные для исследуемого класса АСУ: *У1* – вирусные атаки через корпоративную сеть передачи данных на традиционные IT-компоненты, применяемые в АСУ; *У2* – получение удаленного доступа к элементам управления АСУ; *У3* - перехват, искажение и передача информации, циркулирующей в сети; *У4* – нерегламентированные действия персонала; *У5* – потеря связи с элементами АСУ. Значения рисков получены с использованием генератора случайных чисел в диапазонах, учитывающих реальные характеристики объектов нефтегазовой отрасли Оренбургской области и исследований, представленных в разделе 2.2.

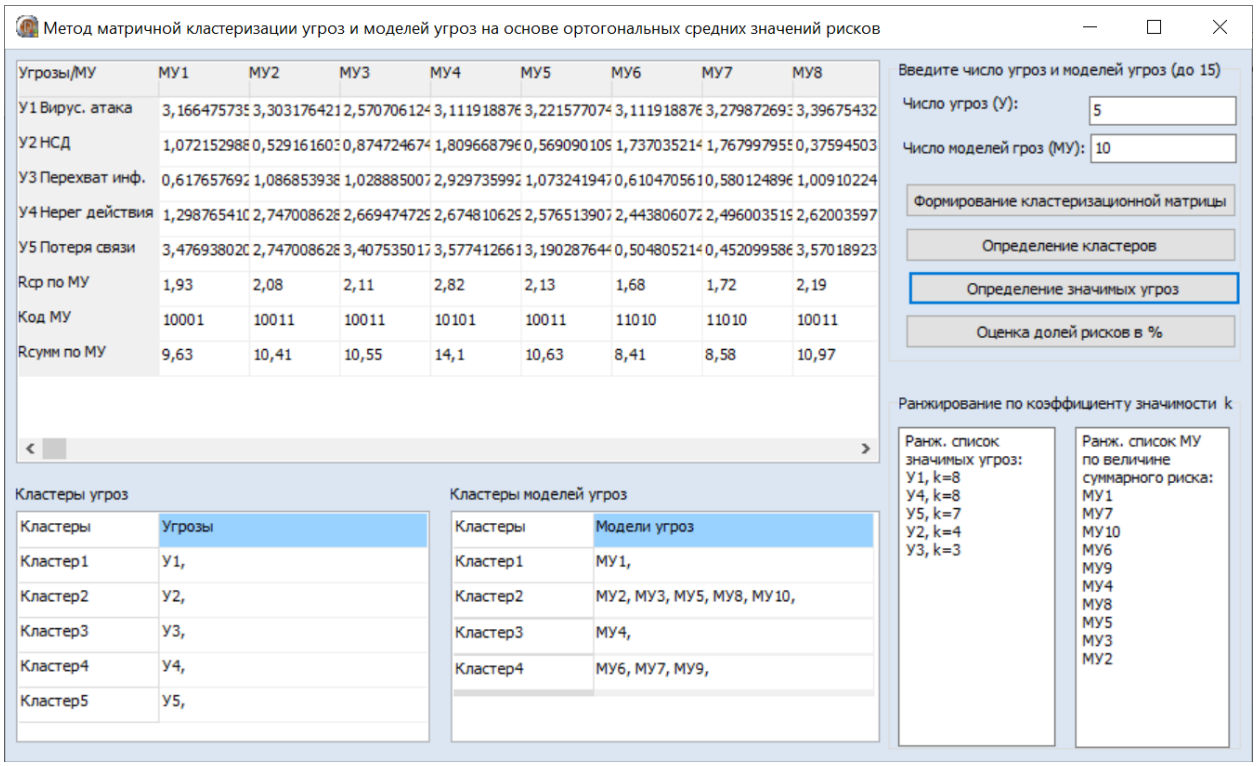


Рисунок 2.6 – Экранная форма матричной кластеризации угроз и моделей угроз на основе ортогональных средних значений рисков

На рисунке 2.6 видно, что все частные МУ, входящие в один кластер, характеризуются близкими значениями рисков для одних и тех же угроз. Например, частные модели угроз для подсистем АСУ кластера 2 содержат высокие значения риска от угрозы потери связи с элементами АСУ, так как соответствующие подсистемы находятся вблизи рек, дорог и населенных пунктов. Эти факторы создают опасность обрыва линий связи в результате размыва почв, либо прохождения тяжелой техники в районе прокладки кабеля. Угроза несанкционированного использования технологий удаленного доступа на этих участках, напротив, невелика. Таким образом, для разработки СЗИ для рассматриваемой АСУ, состоящей из 10 подсистем, достаточно исследование 4 частных МУ.

Ранжированный список угроз, полученный в результате кластеризации угроз, показал, что наиболее значимыми для большинства подсистем являются угрозы сетевых вирусных атак, потери связи с элементами АСУ и нерегламентированных действий пользователей.

При исследовании временных особенностей проявления угроз условия работы каждой из подсистем АСУ были исследованы в конкретный период времени. В результате было выявлено, что угроза обрыва линии связи наиболее актуальна в сезон весеннего половодья, когда происходит размыв почв. Для угроз, связанных с нерегламентированными действиями пользователей рассматривались суточные изменения значений рисков. Данные угрозы наиболее актуальны днем, когда большая часть персонала системы находится на работе. Колебаний значений рисков вирусных атак во времени выявлено не было.

Достоинствами представленного метода являются:

– простота и наглядность анализа МУ распределенных систем управления;

– учет условий эксплуатации каждой из подсистем распределенной АСУ;

– снижение временных и финансовых затрат на создание и модернизацию СЗИ при сохранении основных требований по защите информации;

– представление и анализ рисков в процентном соотношении от общего риска модели угроз (начального или остаточного), что позволяет проводить исследование на основе системного подхода.

Проведенный анализ подтвердил необходимость совершенствования существующей СЗИ в направлении оперативного обнаружения, идентификации аномальных состояний КС АСУ и нейтрализации связанных с ними актуальных угроз сетевых вирусных атак, потери информации вследствие блокирования канала связи между сетевыми узлами АС, нерегламентированных действий персонала системы.

Для обнаружения аномалий и распознавания состояния КС АСУ, как проявлений инцидентов ИБ вследствие реализации угроз, разработан метод построения математических и имитационных моделей, представленный ниже.

2.4 Метод построения математических и имитационных моделей для обнаружения аномалий и распознавания состояния КС АСУ на основе данных мониторинга сетевого трафика

2.4.1 Математическая модель и метод обнаружения аномалий в сетевом трафике АС на основе дихотомического подхода

Актуальность задачи мониторинга состояния компьютерных систем (КС) по данным сетевого трафика (СТ) обусловлена доступностью и высокой информативностью сведений сетевых потоков, и как следствие, необходимостью обеспечения высокой производительности и достоверности используемых методов и средств обнаружения и реагирования на прецеденты, связанные с защитой информации.

Под аномалиями в компьютерных сетях понимаются состояния КС, отраженные в СТ, соответствующие нерегламентированным режимам работы сетевых узлов, режимам обмена информацией между узлами и режимам передачи данных с нарушением сетевых протоколов и заданных ограничений по защите информации. Характерным признаком проявления аномалий является нерегламентированные отклонения параметров сетевого трафика от «нормального» профиля. Примером аномалии в сетевом трафике, может быть повышенная интенсивность сетевых пакетов, являющаяся результатом протекающей вирусной атаки, попыток несанкционированного управления элементами системы, потери связи между узлами сети.

Широко используемы в настоящее время методы интеллектуального анализа данных и машинного обучения, обладают высокой достоверностью и универсальностью. Эффективность их использования во многом определяется наличием представительной выборки исходных данных и значительными временными затратами на обучение и распознавание ситуаций.

Целью раздела является повышение оперативности и достоверности выявления аномального состояния компьютерной сети по характеристикам интенсив-

ности пакетов сетевого трафика на основе поиска и совершенствования эффективных методов и средств обработки и анализа информации.

Для достижения цели решены следующие задачи:

1. На основе анализа требований и характеристик используемых методов интеллектуальной обработки данных СТ обоснована применимость дихотомического подхода в задаче обнаружения аномального состояния компьютерной сети.

2. Разработана модель дихотомического разделения состояний СТ с выделением аномального состояния на основе спектральных характеристик временных рядов и применения мажоритарного разделяющего правила.

3. На основе модели разработан алгоритм и компьютерная программа обнаружения сетевых аномалий на основе дихотомической модели распознавания образов.

4. Проведена апробация результатов распознавания аномальных ситуаций на экспериментальных данных и данных сетевого трафика, полученных при регистрации инцидентов информационной безопасности в КС вуза.

Под дихотомическим распознаванием аномалий в работе понимается процедура выбора одного из двух состояний объекта по информативным признакам, определенным на стадии обучения распознающей модели [4]. Применимость дихотомического подхода обусловлена необходимостью оперативного выделения состояния КС, отличного от нормального профиля для последующего углубленного анализа и принятия управляющих решений.

В научной литературе решению аналогичной задачи посвящен представительный ряд публикаций. В частности, в работах профессора Загоруйко Н.Г., представлены результаты оценок возможностей распознающих средств, методы выбора информативной системы признаков и определения правил принятия решений [94]. В исследованиях профессора Ивахненко А.Г. [98] и его учеников, рассмотрены задачи разработки и исследования методов синтеза разделяющих функций для идентификации образов различной природы. Особенностью этих методов является определение оптимального пространства признаков в процессе проверки и усовершенствования распознающих моделей на обучающих и экзаме-

национных выборках исходных данных. В современных публикациях ученых и инженеров широко представлен перечень разработок по нейросетевым технологиям, некоторые из которых приведены в списке литературы [147, 111, 99, 186].

В основу модели дихотомического разделения состояний СТ положен принцип определения ранжированного по информативности перечня гармоник спектров временного ряда СТ [4]. Показатель информативности определяется по величине рассогласования (разности) оценок математического ожидания амплитудных характеристик соответствующих гармоник спектров, рассчитанных для временных рядов различных образов (ситуаций). Число используемых информативных гармоник определяется в процессе обучения модели. В качестве разделяющей функции в работе выбрана мажоритарная функция вида «*m* из *n*», в которой порог принятия решения *m* и число аргументов *n* определяются с учетом требований по достоверности и сложности реализации алгоритма распознавания на этапе обучения модели.

Вычисление оценки вероятности принадлежности значения амплитудной оценки спектра *x* информативной гармоники к одному из образов (*A* или *B*) производится с помощью формулы нормального распределения (2.7):

$$P(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad , \tag{2.7}$$

где μ и σ, соответственно, оценки математического ожидания и среднеквадратичного отклонения амплитудных спектральных оценок для информативных гармоник с одинаковыми номерами для временных рядов обучающих выборок для каждого образа *A* и *B*.

Бинаризация значений аргументов X_i (i=1, n) для разделяющей функции осуществляется по формулам (2.8) и (2.9):

$$X = 1, \text{если } P_A(x) \geq P_B(x), \tag{2.8}$$

$$X = 0, \text{если } P_A(x) < P_B(x). \tag{2.9}$$

Формулы разделяющей функции от трех аргументов и правила принятия решения относительно распознаваемого состояния q_x представлены соответственно выражениями (2.10) и (2.11).

$$F(X_1, X_2, X_3) = X_1X_2 \vee X_1X_3 \vee X_2X_3 \vee X_1X_2X_3; \quad (2.10)$$

$$q_x \in A, \text{если } F(X_1, \dots, X_n) = 1;\ q_x \in B, \text{если } F(X_1, \dots, X_n) = 0. \quad (2.11)$$

Достоинствами разработанной модели являются:

- высокая достоверность и производительность;
- возможность обучения и адаптации модели к изменениям характеристик временных рядов;
- невысокие требования к вычислительным ресурсам при ее реализации в прикладных программах.

На рисунке 2.7 представлена схема алгоритма обучения и распознавания одной из двух ситуаций (образов) КС по данным временных рядов сетевого трафика: *A* - аномальной ситуации, *B* - регламентированной ситуации.

Временные ряды, используемые в процессе исследований, получены в результате имитации различных ситуаций в СТ на базе лабораторного сетевого стенда [3] и в процессе сбора данных о работе компьютерной сети вуза по логфайлам сетевого сервера. Расчет спектральных оценок временных рядов на разных этапах экспериментов в блоке 2 проведен с использованием стандартных функций преобразования Фурье в среде программирования Python, а также средствами табличного процессора Excel.

Для исследования модели и алгоритма разработано программное средство [37] дихотомического распознавания аномалий в сетевом трафике. Программа предназначена для использования на персональных компьютерах типа IBM PC 686/Pentium/AMD, работающих под управлением операционных систем MS Windows 7/8/10/11 64 - или 86-битной архитектуры, систем Linux с использованием Windows API - Wine. Интерфейс программы представлен на рисунке 2.8.

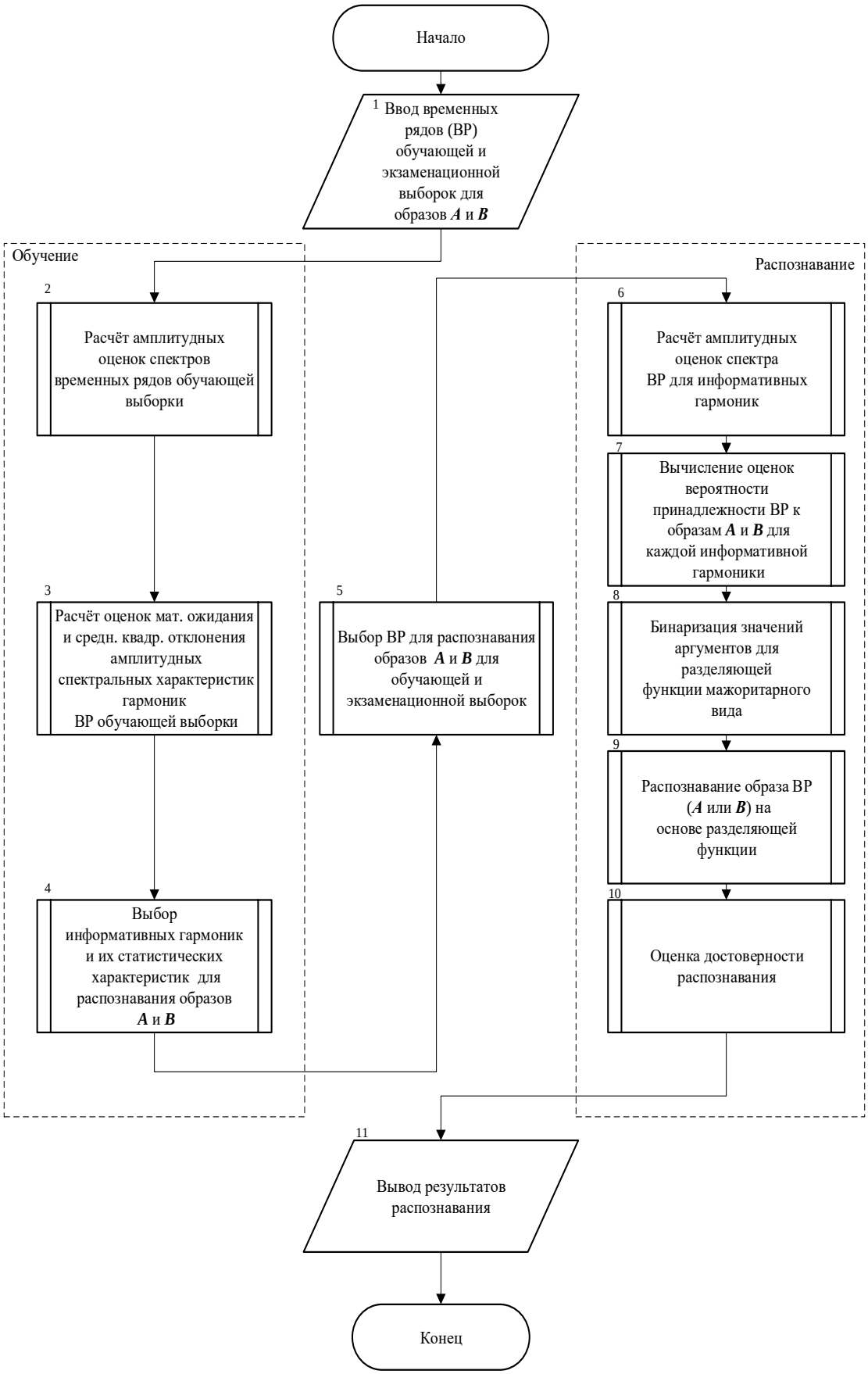


Рисунок 2.7 – Схема алгоритма обучения и распознавания состояния КС по данным временных рядов СТ на основе дихотомической модели

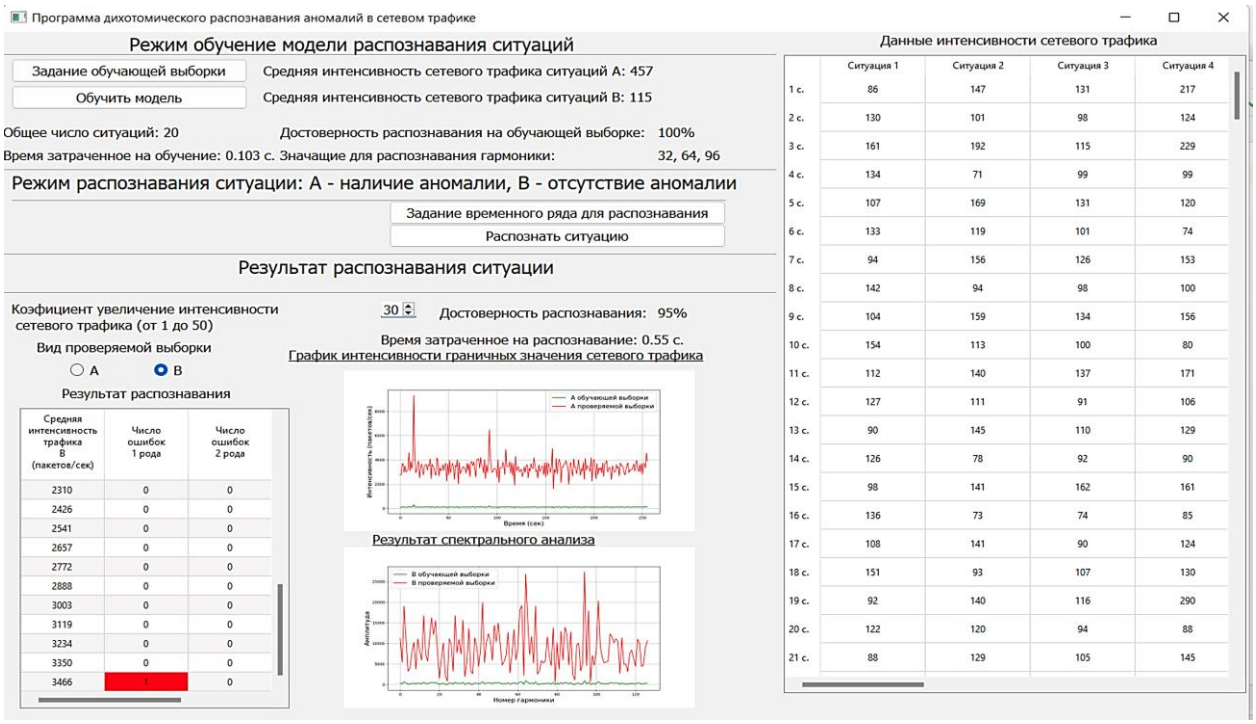


Рисунок 2.8 – Экранная форма работы программы дихотомического распознавания аномалий в сетевом трафике

В ходе натурного эксперимента была исследована работа модели с учетом разных уровней интенсивности сетевого трафика в режиме наличия и отсутствия атаки. Для моделирования аномалий было проведено 10 экспериментов, зарегистрированы временные ряды трафиков работы сети общим объемом около 700 Мбайт. На основе полученных данных сформированы обучающее и тестовое множества файлов сетевого трафика. В качестве исходного материала для экспериментального исследования моделировались и использовались временные ряды за 256-секундные интервалы со средней интенсивностью трафика, изменяемой в интервале от 100 пакетов в секунду до 3,5 тысяч пакетов в секунду. Результаты натурного эксперимента по обнаружению сетевых аномалий на основе дихотомической модели распознавания образов и представлены в разделе 4.3.1.

При распознавании ситуаций по данным СТ с интенсивностями верхнего уровня диапазона ошибки первого и второго рода не превышали 5 %.

Апробация модели и программы проведена на основе реальных данных сетевого трафика, полученных при регистрации Dos-атаки в КС Оренбургского государственного университета. Интенсивность поступления пакетов не превышала

110 пакет/сек. со средней дисперсией 93,8 в режиме атаки и 7,3 в режиме отсутствия атаки. Погрешности первого и второго рода при распознавании ситуаций на реальных данных СТ компьютерной сети вуза не превышали 3 %.

Анализ результатов натурного эксперимента показал высокую оперативность и достоверность выявления аномального состояния узлов КС по характеристикам интенсивности пакетов сетевого трафика на основе дихотомического подхода. Сопоставительный анализ методов реализации дихотомического разделения состояний сетевого трафика на основе мажоритарной и аналогичных, в частности, нейросетевой модели, представлен в разделе 4.1.

Идентификация обнаруженного аномального состояния КС и уточнение вида аномалии осуществляется с использованием обобщенной математической модели распознавания на основе ассоциативно-мажоритарного подхода.

2.4.2 Математическая модель идентификации аномального состояния АС на основе ассоциативно-мажоритарного подхода

Целью разработки модели является повышение оперативности и достоверности распознавания аномалий в больших объемах сетевого трафика АСУ. Анализ факторов, влияющих на эффективность средств распознавания, и современных тенденций развития теории и практики анализа сетевого трафика, представленный в работах [27, 70, 164, 174, 177], позволили выявить преимущества ассоциативно-мажоритарного подхода (АМП) для решения задач исследования. Ассоциативный подход позволяет установить закономерности между аномалией, признаками ее проявления и участками сетевого трафика, в котором они встречаются, и повысить оперативность поиска сведений об отклонениях в работе системы. Принцип мажоритарности позволяет повысить достоверность принятия решения по нейтрализации угрозы, соответствующей найденной аномалии.

В основу обобщенной математической модели идентификации аномальных состояний АС по данным сетевого трафика положена ассоциативно-мажоритарная модель (АММ) [45], позволяющая производить оперативный поиск

и выборку информации в сетевом трафике по сигнатуре и оперативно идентифицировать состояние АС. Исходные данные АММ описываются следующими выражениями:

- $Q=\{Q_1, Q_2, \dots, Q_N\}$ – множество классов распознаваемых состояний АС;
- q^x – состояние, подлежащее распознаванию;
- Q^* – класс образов состояний, к которому отнесен q^x;
- $P = \{p_1, p_2, \dots, p_M\}$ – множество признаков распознавания состояний в сетевом трафике;
- $<s_i>$ – зарегистрированное значение i-го признака, $i = 1, M$; $<S^x>$ – вектор зарегистрированных значений признаков q^x в потоке сетевого трафика;
- $D=\{D_1, D_2, \dots, D_N\}$ – множество диапазонов изменения признаков;
- $V\{q^x, Q_j\}$ – мера близости между q^x и j-ым образом из множества Q, $j= 1, N$;
- $v_{ij}\{<s_i>, Q_j\}$ – частный параметр ассоциативности значения $<s_i>$ признака s_i из множества S^x для образа Q_j;
- $A\{<S^x>, Q\}$ – матрица коэффициентов ассоциативности значений признаков $<S^x>$ и всех классов образов из множества Q;
- $\Phi\{<S^x>, Q_j\}$ – разделяющая функция для вычисления $V\{q^x,Q_j\}$.

Математическое описание АММ распознавания имеет следующий вид:

$$V\{q^x, Q_j\} = \Phi\{< S^x >, Q_j\}, j = 1, N; \tag{2.12}$$

$$\Phi\{< S^x >, Q_j\} = \sum_{i=1}^{M} v_{ij}\{< s_i{}^x >, Q_j\}, i = 1, M; \tag{2.13}$$

$$A\{<S^x, Q>\}= (v_{ij}); \tag{2.14}$$

$$v_{ij}\{< s_i{}^x >, Q_j\} = \begin{cases} 1, & \text{если} \quad < s_i{}^x > \in D_{ij}; \\ 0, & \text{если} \quad < s_i{}^x > \notin D_{ij}; \end{cases} \tag{2.15}$$

$$q^x \in Q^* \in Q: V\{q^x, Q^*\} \equiv max V\{q^x, Q_j\},\ Q_j \in Q. \tag{2.16}$$

Анализ современных подходов к распознаванию аномалий по данным сетевого трафика, позволил выбрать в качестве разделяющей функцию вида (2.13). В матрице (2.14) каждый столбец соответствует частным мерам близости v_{ij} множества $<S^x>$ для каждого класса образов по всем признакам. Выражение (2.16) представляет собой правило отнесения q^x к одному из образов множества Q по мажоритарному принципу (по максимальной величине меры близости). Достоинством АММ является высокая производительность и достоверность распознавания аномалии.

2.4.3 Обобщенный алгоритм и структурно-функциональная модель ассоциативного процессора обнаружения аномалий и нейтрализации угроз по данным сетевого трафика

В основу обобщенного алгоритма положены разработанные математические модели обнаружения и идентификации аномального состояния КС АСУ, представленные выше. Схема обобщенного алгоритма обнаружения аномалий и нейтрализации угроз по данным сетевого трафика представлена на рисунке 2.9.

Алгоритм включает несколько этапов.

1. Захват пакетов, проходящих через контролируемое сетевое соединение и запись данных сетевого трафика в базу log-файлов. В качестве общего набора данных для распознавания состояния КС выделяются IP-адреса, протоколы, номера портов, и некоторые наборы счетчиков: количество переданных пакетов и байт, время создания и завершения потока.

2. Обнаружение аномальных состояний АС, как проявлений инцидентов ИБ, на основе разделения сетевых информационных потоков системы на «нормальный» и «аномальный» трафик. Для определения аномалии, в частности, детектируются отклонения от «нормальной» картины на основе статистической информации об активности некоторых хостов в сети. Для решения задачи обнаружения аномалий в СТ, характеризующих нерегламентированные состояния АС, используется дихотомический подход, реализуемый на основе мажоритарной функции.

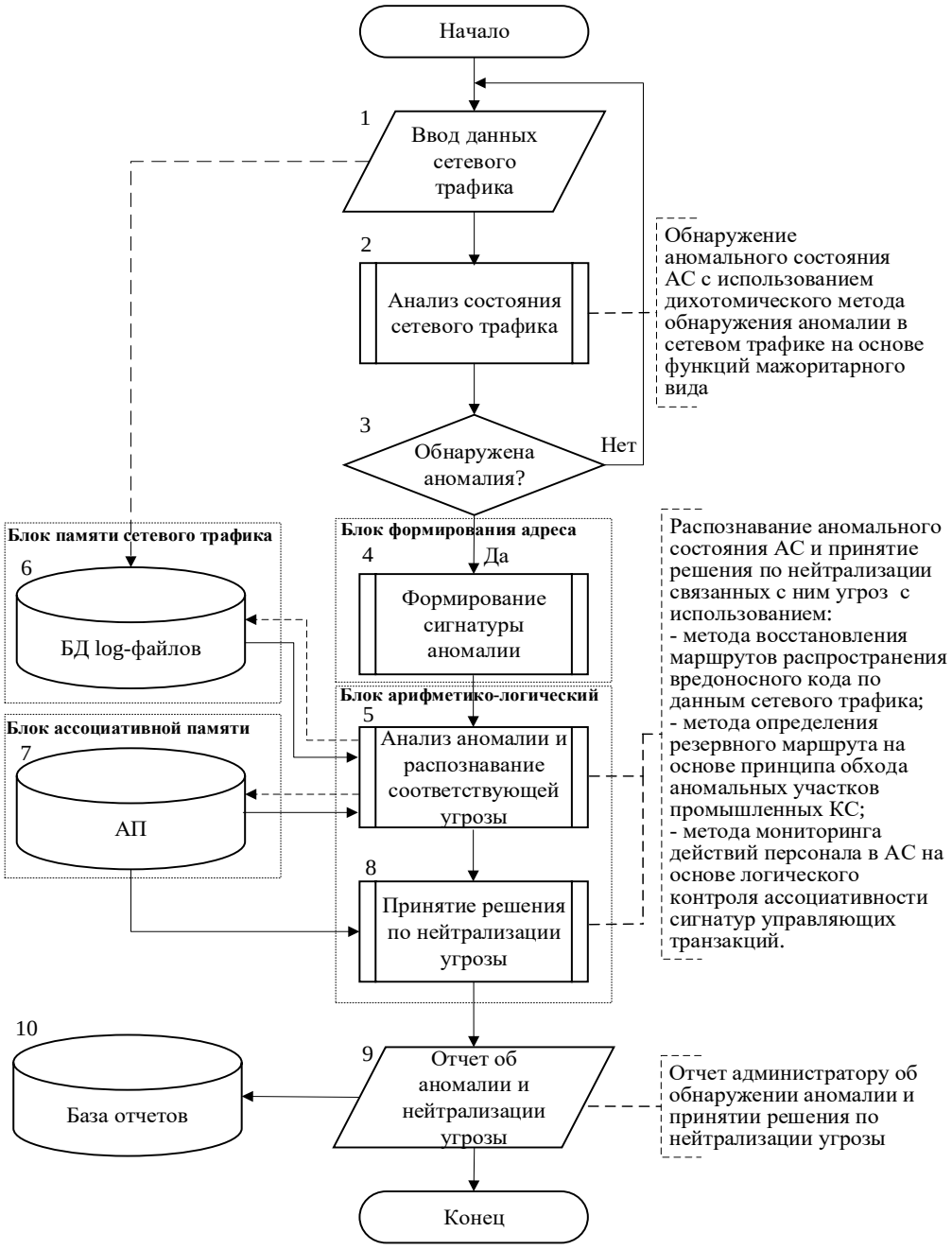


Рисунок 2.9 - Схема обобщенного алгоритма обнаружения аномалий и нейтрализации угроз по данным сетевого трафика

3. В случае обнаружения «отклонения» в сетевом трафике осуществляется идентификация аномальных состояний, заключающееся в дальнейшей уточняющей классификации «аномального» сетевого трафика на основе анализа сигнатур – характерных признаков состояния системы – и поиска информации о соответствующей аномалии в лог-файле сетевого трафика и ассоциативной памяти по адресу-сигнатуре. Для решения этой задачи предложен ассоциативно-

мажоритарный подход, обеспечивающий оперативность поиска сведений об аномалиях и достоверность их распознавания.

4. Принятие мер по нейтрализации угрозы, связанной с аномальным состоянием, с использованием выявленных сигнатур угроз, являющихся адресами памяти ассоциативного процессора защиты информации, по которым хранятся соответствующие сведения для принятия решения по нейтрализации.

Отличительной особенностью алгоритма является наличие блоков 4 – 8, осуществляющих оперативное обнаружение аномальных состояний АС на основе дихотомической модели, их распознавание на основе ассоциативно-мажоритарной модели и принятие мер по нейтрализации угрозы по данным, хранящимся в ассоциативной памяти.

На рисунке 2.10 представлена обобщенная структурно-функциональная модель ассоциативного процессора (АПр) для распознавания аномалий по данным сетевого трафика. АПр представляет собой цифровой автомат, реализующий математическую модель идентификации состояния АС, представленную в разделе 2.4.2. Процессор содержит: блок формирования адреса (БФА), блок ассоциативной памяти (БАП), блок арифметико-логический (БАЛ), блок памяти сетевого трафика БПСТ, блок управления (БУ). Символами *i* и *o* обозначены входы и выходы блока управления соответственно.

Отличительной особенностью процессора является то, что адресная часть запоминающих блоков соответствует контролируемым признакам аномалий, информационная часть – характеристикам исследуемых образов, а структура и архитектура арифметико-логических блоков определяется назначением этих средств, в частности, для контроля последовательности состояний исследуемых процессов или принятия решения по мажоритарному принципу, что позволяет повысить производительность, достоверность, универсальность средств и снизить риски от угроз БИ. Структурно-функциональные особенности БАП и БАЛ определяются спецификой решения конкретной задачи.

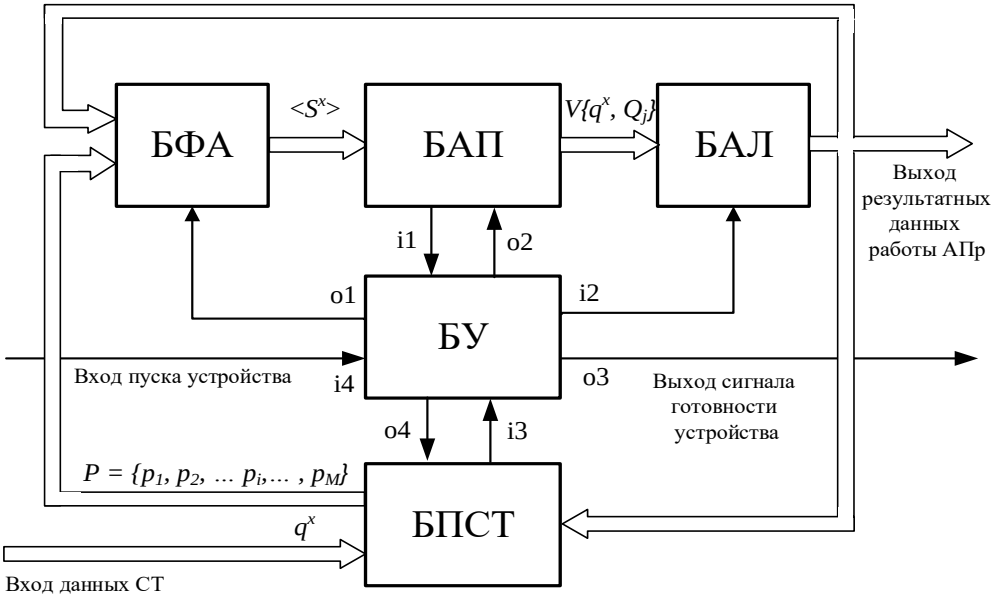


Рисунок 2.10 – Обобщенная структурно-функциональная модель ассоциативного процессора для распознавания аномалий по данным сетевого трафика

В работах [14, 23, 41, 45] в процессе исследований доказано преимущество использования АММ и ассоциативного процессора перед традиционными средствами последовательного поиска информации. В частности, результаты исследований показали увеличение производительности поисковых систем в среднем на 15%.

Исследования, проведенные в работе [41], показали, что время, затрачиваемое на поиск данных с применением ассоциативно-мажоритарного подхода, значительно меньше, чем время поиска в базовом варианте (на основе моделей и методов последовательного перебора строк в лог-файле сетевого трафика, в котором время поиска зависит числа строк). При анализе лог-файла, объемом в 0,5 Гб можно наблюдать увеличение оперативности поиска сведений об аномалии более чем в 5 раз при использовании АММ. С увеличением объема сетевого трафика эффект будет расти.

В результате исследований, можно сделать следующие выводы:

- ассоциативно-мажоритарный подход к поиску информации об аномалиях в КС позволяет повысить производительность средств мониторинга и анализа сетевого трафика, причем, чем больше объем сетевого трафика, тем больше эффект;

- применение ассоциативно-мажоритарного подхода сопряжено с дополнительными затратами на реализацию ассоциативной памяти (структурная сложность ассоциативной памяти зависит от реализации архитектуры связей множества данных об объекте и соответствующего увеличения объема памяти);

- для эффективного мониторинга состояния управляемых объектов по данным сетевого трафика необходимы предварительные исследования изменения технических характеристик подсистем поиска и анализа информации с учетом реальных характеристик объекта.

Исследование эффективности ассоциативно-мажоритарного подхода на примере задачи определения и восстановления маршрутов распространения вредоносного кода в КС АСУ транспортировкой нефтегазового сырья представлены в разделе 4.2.1.

Представленные математические модели и алгоритм универсальны, их частная реализация зависит от постановки конкретной задачи, определяемой моделью угроз. Проведенный анализ статистических данных научных публикаций, материалов Интернет-источников, моделей угроз промышленных объектов АСУ транспортировкой нефтегазового сырья выявил необходимость совершенствования существующей СЗИ и разработки новых моделей, методов, алгоритмов и методик в следующих задачах:

- задача 1 - определение маршрутов и источников распространения вредоносного кода;

- задача 2 - определение адресов заблокированных узлов и резервного маршрута передачи данных в КС;

- задача 3 - распознавание нерегламентированных управляющих операций и транзакций пользователя АС.

Математические, графовые и имитационные модели для решения перечисленных задач, положенные в основу работы методов и средств обнаружения аномалий и нейтрализации угроз, представлены в главе 3 настоящей работы.

2.5 Выводы по второй главе

Разработана классификация моделей задачи обнаружения аномалий и нейтрализации угроз, позволившая определить перечень моделей для решения задач исследования.

Разработан метод матричной кластеризации угроз и моделей угроз (МУ) на основе статистической обработки значений рисков, отличающийся тем, что в качестве исходных данных для кластеризации используются ортогональные средние значения рисков по угрозам и МУ, позволяющий формализовать описание угроз и МУ в виде вектора бинарных классификационных кодов, что позволяет оценивать степени актуальности угроз, приоритетности их нейтрализации и определять характер изменения угрозы на последовательности подсистем распределенной АСУ ТП, а также применять принципы типового проектирования при построении СЗИ для АСУ с распределенной топологией.

Разработан метод построения математических и имитационных моделей для обнаружения аномалий и распознавания состояния КС АСУ на основе данных мониторинга сетевого трафика, отличающийся использованием дихотомического принципа разделения исследуемого множества состояний сетевого трафика на нормальные и аномальные на основе разделяющей функции мажоритарного вида, аргументами которой являются бинаризированные амплитудные оценки информативных гармоник спектров временных рядов сетевого трафика, позволяющий повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз в КС АС. Предложены обобщенные математические модели:

- математическая модель для обнаружения аномалий в сетевом трафике АС *на основе дихотомического подхода*, позволяющая повысить оперативность и достоверность обнаружения нерегламентированных состояний системы по спектральным характеристикам временного ряда сетевого трафика;

- математическая модель для идентификации аномального состояния распределенных АС, построенная *на основе ассоциативно-мажоритарного подхода,*

позволяющая повысить оперативность и достоверность распознавания аномальных состояний по данным сетевого трафика.

Разработан обобщенный алгоритм обнаружения аномалий и нейтрализации угроз и структурно-функциональная модель ассоциативного процессора для распознавания аномалий по данным сетевого трафика. Отличительной особенностью ассоциативного процессора является то, что адресная часть БАП соответствует контролируемым признакам аномалий, информационная часть – характеристикам исследуемых образов, а структура и архитектура БАЛ определяется назначением этих средств, в частности, для решения задач: задача 1 - определение маршрутов и источников распространения вредоносного кода; задача 2 - определение адресов заблокированных узлов и резервного маршрута передачи данных в КС; задача 3 - распознавание нерегламентированных управляющих действий пользователя АС.

Полученные модели легли в основу разработки алгоритмов, методик и программной реализации методов и средств обнаружения аномалий и нейтрализации угроз в КС распределенных автоматизированных систем.

ГЛАВА 3. РАЗРАБОТКА АЛГОРИТМОВ, МЕТОДИК И ПРОГРАММНОЙ РЕАЛИЗАЦИИ МЕТОДОВ И СРЕДСТВ ОБНАРУЖЕНИЯ АНОМАЛИЙ И НЕЙТРАЛИЗАЦИИ УГРОЗ В КС РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

3.1 Графо-аналитическая модель и метод восстановления маршрутов распространения вредоносного кода по фрагментам данных сетевого трафика

Вопросы повышения эффективности методов и средств распознавания аномальных состояний АСУ, возникающих в результате сетевых вирусных атак на систему, входят в перечень актуальных в теории и практике управления. В современной литературе известен ряд публикаций, посвященных разработке и исследованию методов и средств интеллектуального анализа сведений о сетевых вирусных атаках, в частности [105, 135, 179, 194, 200, 109]. Однако большинство из них посвящены выявлению ситуаций, связанных с сетевыми вторжениями, и лишь вскользь затрагивают вопросы анализа фрагментированных данных об атаке и выявления зависимостей между ними.

Одной из часто встречаемых задач по нейтрализации угроз, связанных сетевыми вирусными атаками в АСУ, является восстановление маршрутов распространения вредоносного кода в системе по доступным фрагментам сведений. Такие задачи актуальны при определении факта распространения сетевой вирусной атаки, выявления источника распространения и нейтрализации вредоносного воздействия зараженных узлов [7]. Анализ исследований в данной области, представленных в научных публикациях отечественных и зарубежных ученых [131, 205], показал сложность оперативного поиска источников атаки и восстановления полной картины распространения вируса, обусловленную большими объемами и фрагментированностью данных сетевого трафика АСУ, что не позволяет своевременно реагировать на инцидент.

Целью разработки модели и метода является повышение оперативности и достоверности средств восстановления маршрутов и определения источников распространения вредоносного кода в условиях дефицита исходных данных.

Для достижения цели разработаны:

- графо-аналитическая модель и метод восстановления маршрутов распространения вредоносного кода в распределенной КС;
- алгоритм, методика и программная реализация метода и средств восстановления маршрутов распространения вредоносного кода в распределенной КС;
- проведено исследование эффективности метода на реальных данных.

Под маршрутами распространения вредоносного кода понимаются пути передачи вредоносной информации (например, вируса) в сетевой инфраструктуре АСУ. Задача восстановления маршрута заключается в оперативном поиске фрагментов данных сетевого трафика о распространении вируса в системе по некоторым известным признакам атаки и восстановлении объективных связей между ними.

В качестве исходных данных для поиска аномальных фрагментов сетевого трафика, содержащих сведения о распространении вредоносного кода, используются данные трафика за период заражения и сведения об IP-адресах зараженных узлов, полученные от антивирусных средств.

Математическое описание задачи распознавания аномальных фрагментов представляется следующим образом:

- $Q=\{q_1, q_2, \ldots, q_m\}$ – множество маршрутов распространения вредоносного кода в системе, m – число возможных маршрутов;

- $N=\{N_1, N_2, \ldots, N_j \ldots, N_n\}$ – множество IP-адресов узлов сети, n – число узлов в КС;

- $F=\{f_1, f_2, \ldots, f_b\}$ – множество аномальных фрагментов (пакетов) сетевого трафика, содержащих признаки наличия вируса в системе, b – число фрагментов; совокупность аномальных фрагментов, связанных адресами передачи вредоносной информации, формируют маршрут распространения q;

- $P = \{p_1, p_2, \ldots, p_k\}$ – множество k признаков распознавания аномального фрагмента; $D = \{d_1, d_2, \ldots, d_k\}$ – множество диапазонов изменения признаков p.

В качестве основных признаков p для распознавания аномального фрагмента сетевого трафика рассмотрены:

- IP – адрес узла сети;

- t – время регистрации фрагмента (пакета) сетевого трафика;

Дополнительно для распознавания может быть использовано множество характерных признаков атаки - Pa. Например, признаком распространения вируса-шифровальщика WannaCry, является резкое увеличение сетевых пакетов от определенных компьютеров, отправленных на 445 TCP-порт. В данном случае в качестве признаков распознавания будут использованы адреса источников и приемников пакета, число пакетов от определенного адреса, протокол и номер порта.

Перечисленные признаки формируют сигнатуру распознавания S. В простейшем случае, когда известен вид вирусной атаки, формируется сигнатура вида (3.1).

$$S = \{IP, t\}; \tag{3.1}$$

$$f_b = \begin{cases} 1, \text{ если } IP_{f_b} \in D_{IS} \wedge t_{f_b} \in D_T,\ tn \leq D_T \leq tk; \\ 0, \text{ если } IP_{f_b} \notin D_{IS} \vee t_{f_b} \notin D_T,\ tn \leq D_T \leq tk; \end{cases} \tag{3.2}$$

$$N_j \in Source:\ Sn_j \equiv \max Sn,\ Sn \geq 2. \tag{3.3}$$

Параметры IP и t свидетельствуют об аномальности фрагмента трафика, если IP-адреса источников и приемников пакета принадлежат диапазону зараженных адресов D_{IS}, а время его передачи соответствует периоду D_T распространения вируса в системе. Параметр D_T ограничивается временем первого tn и последнего tk появления признака вируса в сетевом трафике. В выражении 3.2 представлено правило распознавания аномального фрагмента.

В выражении 3.3 представлено правило распознавания источника вредоносной рассылки, где Sn – число аномальных фрагментов от узла сети. Узел N_j относится к источникам вредоносной рассылки $Source$, если является инициатором посылки большинства аномальных пакетов в маршруте. Маршрутом считается це-

почка распространения вредоносной информации, содержащая не менее 2 фрагментов.

IP-адреса узлов сети одновременно являются адресами строк АП, по которым считываются IP всех устройств, взаимодействовавших с искомым, и время взаимодействия. В таблице 3.1 показан пример формирования адресной части и заполнения ячеек АП, где IP_n – адреса сетевых узлов, представленных в формате порядковых номеров, соответствующих реальным IP-адресам, t – время взаимодействия узлов, необходимое для восстановления последовательности передачи сетевых пакетов, «0» обозначает отсутствие взаимодействия.

Таблица 3.1 – Матричная модель АП в режиме восстановления маршрутов распространения вредоносного кода

Адрес ячейки АП	**Содержимое ячеек**															
IP	IP_1	IP_2	IP_3	IP_4	IP_5	IP_6	IP_7	IP_8	IP_9	IP_{10}	IP_{11}	IP_{12}	IP_{13}	IP_{14}	…	IP_n
IP_1	-	$t_{1.2}$	$t_{1.3}$	$t_{1.4}$	0	0	0	0	0	0	0	0	0	0	…	0
IP_2	0	-	0	0	0	0	0	0	0	$t_{2.10}$	0	0	0	0	…	0
IP_3	0	0	-	0	$t_{3.5}$	0	0	0	0	0	0	0	0	0	…	0
IP_4	0	$t_{4.2}$	0	-	0	$t_{4.6}$	0	$t_{4.8}$	0	0	0	0	0	0	…	0
IP_5	0	0	0	0	-	0	0	$t_{5.8}$	0	0	0	0	0	0	…	0
IP_6	0	0	0	0	0	-	0	$t_{6.8}$	0	0	0	0	0	0	…	0
IP_7	0	0	0	0	0	0	-	0	0	$t_{7.10}$	0	0	0	0	…	0
IP_8	0	0	0	0	0	0	0	-	$t_{8.9}$	0	$t_{8.11}$	0	0	0	…	0
IP_9	0	0	0	0	0	0	0	0	-	$t_{9.10}$	0	0	0	0	…	0
IP_{10}	0	0	0	0	0	0	0	0	0	-	0	0	0	0	…	0
IP_{11}	0	0	0	0	0	0	0	0	0	0	-	0	0	0	$t_{11.15}$	0
IP_{12}	0	0	0	0	0	0	0	0	0	0	0	-	$t_{12.13}$	0	…	0
IP_{13}	0	0	0	0	0	0	0	0	0	0	0	0	-	0	$t_{13.15}$	0
IP_{14}	0	0	0	0	0	0	0	0	0	0	0	0	$t_{14.13}$	-	…	0
…	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-	…
IP_n	$t_{n.1}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-

По адресам зараженных узлов, полученным от антивирусных средств защиты, производится обращение к соответствующей строке АП и считывание сведений об аномальных фрагментах трафика (адреса взаимодействующих с зараженным узлов и времени взаимодействия).

Для восстановления и анализа маршрутов необходимо построение цепочек распространения вредоносного кода по найденным аномальным пакетам сетевого трафика, связанным адресами участвующих в атаке узлов.

Классический подход к анализу маршрутов распространения вируса сводится к построению графовых, либо матричных моделей. Для повышения эффективности и иллюстративности анализа в данной работе предлагается комбинированная графо-матричная модель, представленная на рисунке 3.1.

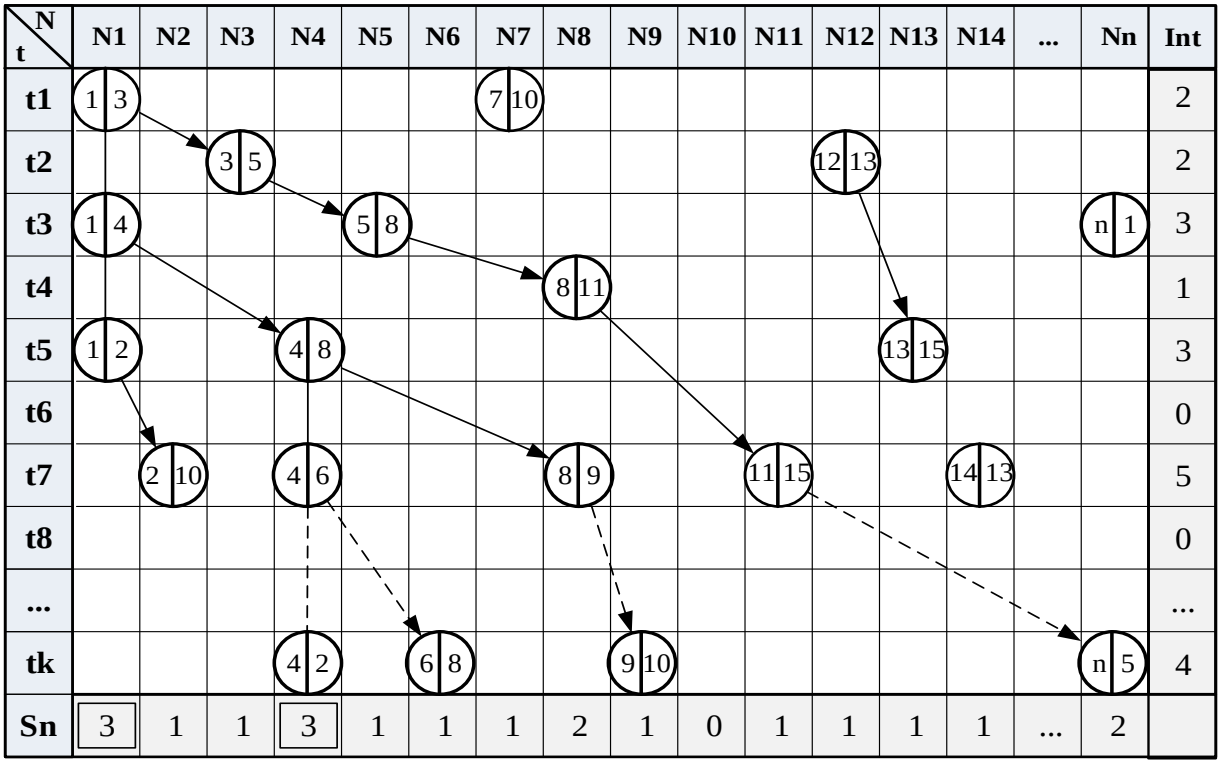


Рисунок 3.1 – Графо-аналитическая модель восстановления маршрутов распространения вредоносного кода

Процесс построения маршрута сводится к построению цепочек взаимодействия зараженных узлов сети *N* по IP-адресам, участвовавшим в атаке в период времени *t1 - tk*. Выявление источников распространения вируса производится среди фрагментов распознанных маршрутов по мажоритарному принципу, согласно выражению 3.3. В случае выявления нескольких источников определяется узел, начавший вредоносную рассылку раньше других.

Особенностью модели является то, что она объединяет достоинства графического и аналитического методов для анализа сетевого трафика. Вершины графов маршрутов, в отличие от традиционной матрицы смежности, обозначают адресную часть пакетов сетевого трафика в виде IP-адресов, ребра – направления их передачи. Модель позволяет описывать динамику маршрута по левой вертикаль-

ной временной оси ***t,*** определяющей моменты времени передачи пакетов, статистику встречаемости узлов в маршруте по нижней горизонтальной оси ***Sn***, интенсивность распространения вредоносного кода по правой вертикальной оси ***Int***, определять источники распространения вируса по принципу большинства встречаемости их адресов в маршруте.

Пример анализа маршрутов распространения вредоносного кода, согласно данным рисунка 3.1, представлен в таблице 3.2.

Таблица 3.2 – Анализ маршрутов распространения вредоносного кода

Хар-ка / Обозначение	**Маршруты распространения вредоносного кода**	**Число фрагментов**	**Временной интервал**	**Источник атаки**
R1	N1-N3-N5-N8-N11-N15-Nn-N5	6	t1 – tk	N1
R2	N1-N4-N8-N9-N10	4	t1 – tk	N1
R3	N1-N4-N6-N8	3	t1 – tk	N1
R4	N1-N4-N2	2	t1 – tk	N1
R5	N1-N2-N10	2	t1 – t7	N1
R6	N12-N13-N15	2	t2 – t5	N12
f1	N7-N10	1	t1	-
f2	Nn-N1	1	t3	-
f3	N14-N13	1	t7	-

В результате анализа было определено 6 маршрутов *R1 – R6* распространения вируса, и 3 аномальных фрагмента *f1 – f3*, не входящих ни в один из маршрутов. В качестве источника атаки определен узел *N1*.

Представленная модель легла в основу разработки метода восстановления маршрутов распространения вредоносного кода по данным сетевого трафика. Результаты разработки алгоритма, методики и программной реализации метода и средств восстановления маршрутов распространения вредоносного кода в распределенной КС представлены ниже.

3.2 Алгоритм, методика и программная реализация средств восстановления маршрутов распространения вредоносного кода в распределенной КС

Алгоритм восстановления маршрутов распространения вредоносного кода по данным сетевого трафика включает три этапа.

1. Обнаружение аномальных значений интенсивности сигнала СТ, связанных с сетевой атакой, с использованием метода обнаружения аномалий на основе дихотомического подхода. Экранная форма [37] обнаружения аномалии, связанной с распространением вируса-шифровальщика, представлена на рисунке 3.3 (а).

2. Поиск фрагментов сетевого трафика, передаваемых от всех зараженных узлов промышленной сети за период заражения по данным АП, как показано на рисунке 3.3 (б). Вид вирусной атаки и список адресов зараженных узлов определяется по сведениям, полученным из журналов антивирусных средств защиты.

3. Восстановление маршрутов и определение источников распространения вредоносного кода по найденным аномальным фрагментам на основе моделей, представленных в разделе 3.1, как показано на рисунке 3.4.

Схема алгоритма представлена на рисунке 3.2. Критериями останова цикла восстановления маршрутов являются достижение требуемой достоверности распознавания источника атаки $Sd \geq Sd_{порог}$., либо временные ограничения $T \geq T_{порог.}$ на поиск источника. Данные параметры определяются администратором безопасности. В случае если аномальные данные представлены в виде несвязанных фрагментов, администратору выводится информация об отдельных пакетах, узлах участвовавших в их посылке и времени их появления, формируется отчет о необходимости обновления параметров системы.

Представленные модель и алгоритм реализованы при разработке программ для поиска аномальных фрагментов сетевого трафика, построения маршрутов и определения источников распространения вредоносного кода [11, 13]. Экранные формы работы программ представлены на рисунках 3.3 (б) – 3.4.

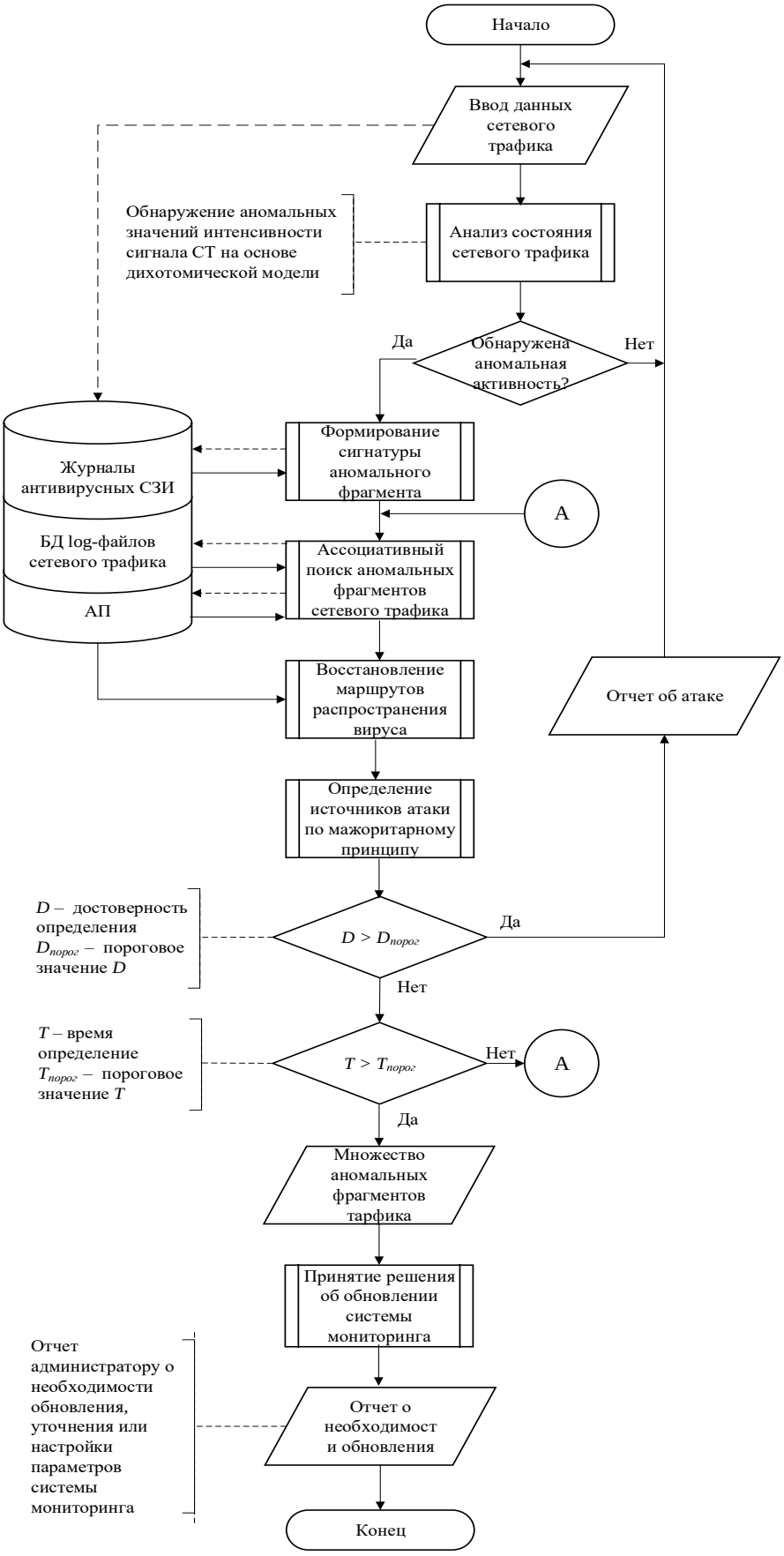
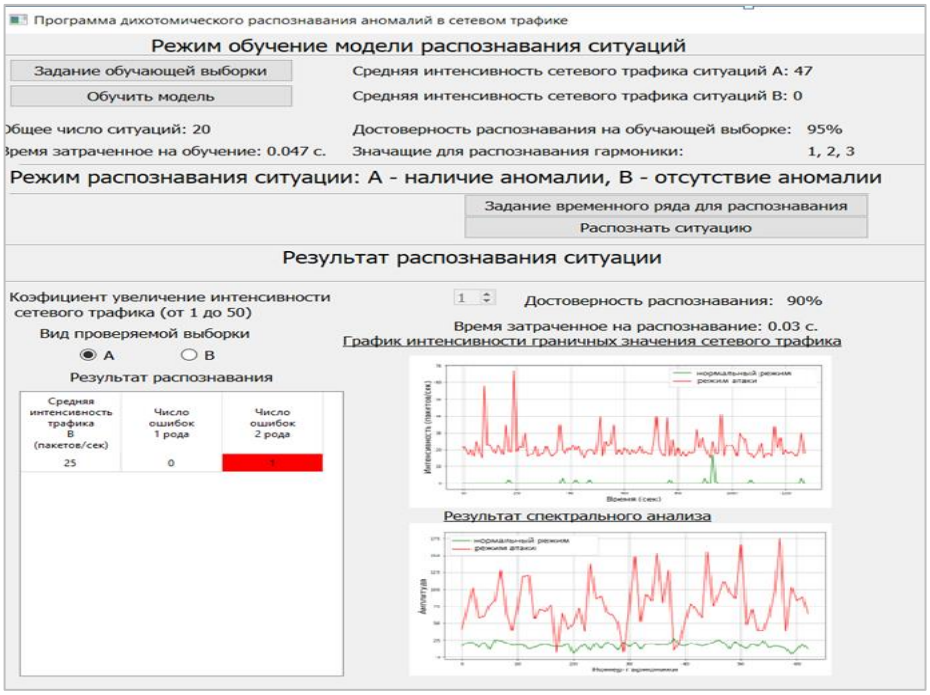
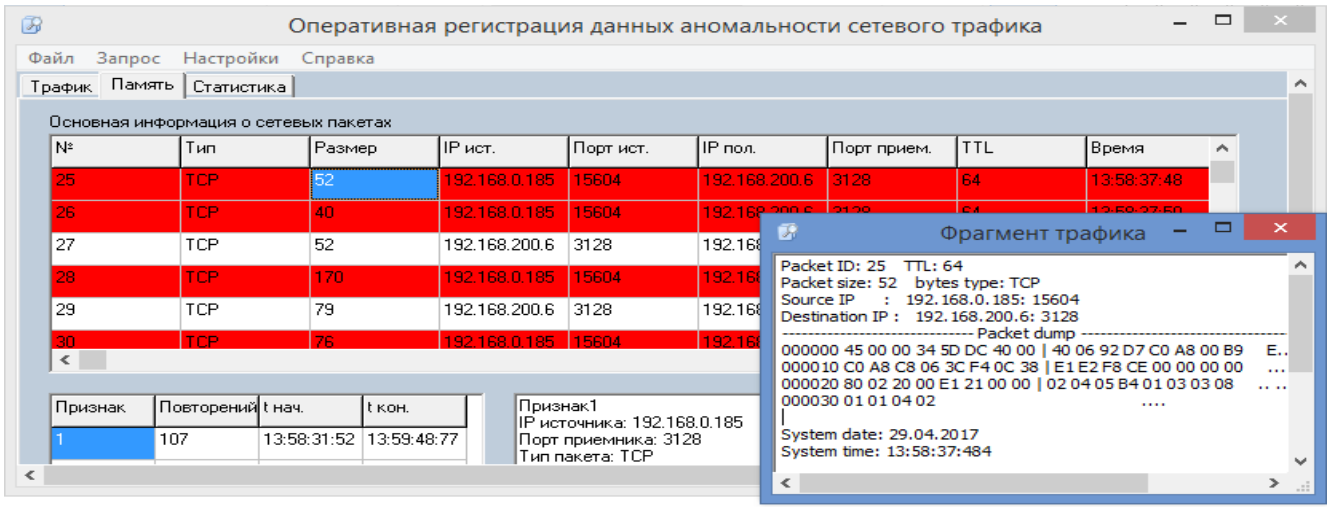


Рисунок 3.2 – Схема алгоритма восстановления маршрутов распространения вредоносного кода по данным сетевого трафика



а)



б)

Рисунок 3.3 – Экранные формы обнаружения аномалии (а) и поиска фрагментов данных о вирусной атаке (б)

Исходными данными для работы программ является поток сетевого трафика, регистрируемый в режиме реального времени, либо в виде лог-файла.

Программа «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» [11] предназначена для поиска пакетов, соответствующих признакам обнаруженной аномалии (в данном случае, распространения вируса в сети). В режиме обучения программы осуществляется за-

полнение базы данных (БД) аномальных признаков. В режиме поиска сведений об атаке осуществляется загрузка потока сетевого трафика и выделяется основная информация о проходимых пакетах. В АП записываются адреса взаимодействующих узлов, время их взаимодействия. Листинги модулей записи и поиска информации в АП представлены в приложении Ж.

Поиск аномальных пакетов осуществляется двумя способами:

- в автоматическом режиме с использованием БД аномальных признаков;

- по запросу администратора безопасности (в запросе указываются предполагаемые признаки аномалии, например, адреса зараженных узлов, полученные от антивируса).

Результатом работы программы являются статистика адресов, участвующих в атаке, и множество аномальных фрагментов log-файла, содержащих признаки сетевой атаки. Далее на основе найденных фрагментов с использованием программы [13] формируются маршруты распространения вредоносного кода. По мажоритарному принципу определяется источник распространения. На рисунке 3.4 представлена экранная форма определения маршрутов распространения и источника вредоносной рассылки.

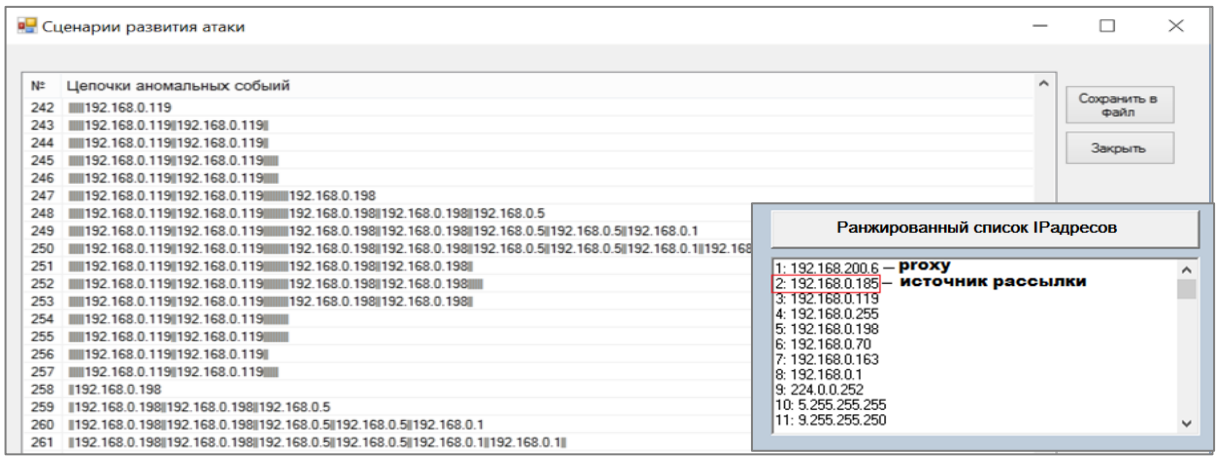


Рисунок 3.4 – Экранная форма восстановления маршрутов и определения источника распространения вредоносного кола

Достоинством предложенного решения является оперативность поиска данных в сетевом трафике, достигаемая за счет использования принципов ассоциа-

тивности и достоверность распознавания источника вредоносной информации по мажоритарному принципу.

Структурно-функциональная модель ассоциативного процессора для восстановления маршрутов распространения вредоносного кода, представлена на рисунке 2.9 в разделе 2.4.3. Адресом строки в ассоциативной памяти в блоке АП является адрес сетевого узла, а содержимое ячеек каждой строки включает адреса всех узлов, обменивающихся информацией с искомым, и время их взаимодействия. Поиск сведений о распространении вредоносного кода осуществляется в два этапа. На первом этапе производится обращение к соответствующей строке АП по адресу зараженного хоста, полученному из блока формирования адреса БАФ, и выборка ассоциированных с соответствующим IP-адресом данных (списка взаимодействовавших с ним адресов и время передачи пакета). Далее в блоке арифметико-логическом строятся маршруты распространения вредоносной информации и определяются источники атаки по принципу большинства встречаемости IP-адреса в маршруте (на основе мажоритарной функции).

Исследования предложенных метода и методики, проведенные в ходе экспериментов и представленные в работах [14, 7, 23, 45, 42] и разделе 4.2, подтвердили его высокую эффективность в сетях с большим числом узлов. Оперативное выявление источников и зараженных хостов позволяет принять превентивные меры по нейтрализации угрозы дальнейшего распространения вредоносного кода в КС (УБИ.1) [53], такие как временная изоляция и восстановление работоспособности зараженных устройств, поиск и устранение уязвимостей, эксплуатируемых для проведения атаки.

3.3 Имитационная модель и метод определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС

Для промышленных АСУ, как критически важных распределённых технологических объектов, необходимо организовывать надёжную высокоскоростную связь для всех подсистем, включая каналы выделенной сети, телефонной и дис-

петчерской связи, трансляции с камер видеонаблюдения, систем обнаружения утечек и систем мониторинга технического состояния, а также средств обеспечения технической безопасности. Согласно данным статистики причин повреждений линий связи в АСУ [88, 172] нарушение их целостности возможно при авариях на объекте, выполнении земельных работ, прохождении тяжелой техники, а также несанкционированной врезке в канал передачи данных. Часто к повреждениям линий связи ведут ошибки монтажа и стихийные природные явления (паводки, пожары и пр.).

Согласно публикациям [106, 183, 130], одним из основных способов обеспечения надежности связи в промышленных сетях является резервирование основных каналов и узлов информационного обмена, как наименее надежных элементов АСУ. Анализ публикаций [16, 93, 106, 150, 183] показал, что большинство известных методов резервирования каналов связи и маршрутизации сетевых потоков (например, с использованием протоколов STP, RSTP, MSTP, OSPF) требуют некоторого количества времени для определения резервного маршрута передачи информации, что ведет к потере части технологической информации.

Целью раздела является снижение рисков потери технологической информации на основе принятия оперативных мер по определению резервного маршрута и организации передачи информации по резервному каналу связи.

Для достижения цели разработаны:

- имитационная модель и метод определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС;

- алгоритм, методика и программная реализация метода и средств определения резервного маршрута;

- структурная схема ассоциативного процессора для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС.

Особенностью распределенных АСУ является необходимость передачи информации между множеством территориально распределенных подсистем. Источники информации, на которых установлены оборудование электропитания и

средства собора информации о состоянии технологического объекта, передают данные по линии связи приёмнику информации. Концепция защиты передачи технологической информации, представленная в работах [5, 117] и положенная в основу разрабатываемых модели и метода, предполагает, что после обнаружения обрыва линии связи, источники информации, потерявшие связь с диспетчером, воспользуются резервным каналом передачи информации – высоковольтной линией электропередач (ВЛЭП) – для обхода недоступного участка сети. Остальные источники будут работать в обычном режиме, продолжая передавать информацию по основному каналу.

Наличие источников и приемников технологической информации, направленный характер сетевых потоков позволили применить теорию графов для исследования процессов передачи информации о состоянии АСУ при обрыве линии связи. Обобщенная графовая модель потоков сетевого трафика в системе сбора и регистрации данных о состоянии технологического объекта представлена на рисунке 3.5. В данной модели структура сети представлена в виде ориентированного графа $G(A, R)$, где A – множество вершин графа, R – множество ребер графа.

Множество вершин графа $A=(A1, A2, A3, A4)$ включает:

- $A1=(I1, I2,..., In)$ – подмножество вершин, обозначающих источники технологической информации, n – количество источников информации;

- $A2=(K1, K2, ..., Kn)$ – подмножество вершин, обозначающих узлы коммутации;

- $A3=(k_{e1}, k_{e2}, ..., k_{en})$ – подмножество вершин, обозначающих порты обмена информацией между источником I и диспетчером D по основному каналу связи;

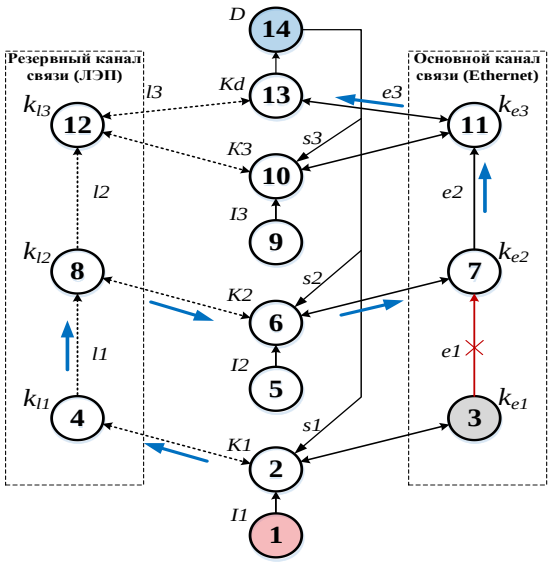
- $A4=(k_{l1}, k_{l2}, ..., k_{ln})$ – подмножество вершин, обозначающих порты обмена информацией между источником I и диспетчером D по резервному каналу связи. В каждый момент времени порты обмена находятся в состоянии $k=1$ (активен), либо $k=0$ (неактивен).

Множество ребер графа $R=(R1, R2, R3)$ включает:

- $R1=(e_1, e_2, \ldots, e_n)$ – подмножество ребер, обозначающих сегменты линии связи основного канала; каждый сегмент может находиться в регламентированном состоянии $e_n = 1$, либо в состоянии обрыва $e_n = 0$.

-$R2=(l_1, l_2, \ldots, l_n)$ – подмножество ребер, обозначающих сегменты линии связи резервного канала; все сегменты резервного канала условно находятся в регламентированном состоянии $e_l = 1$, обрыв ВЛЭП не рассматривается в виду малой вероятности события;

- *R3* - подмножество ребер, обозначающих линии связи между узлами коммутации и портами обмена информацией.



а)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	1	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	1	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	1	0	0	0	0	0	0
5	0	0	0	0	0	1	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	1	1	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	1	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	1	0	0
9	0	0	0	0	0	0	0	0	0	1	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	1	1	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	1	0
12	0	0	0	0	0	0	0	0	0	0	0	0	1	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	1
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0

б)

Рисунок 3.5 – Обобщенная графовая модель переключения потоков сетевого трафика в системе передачи данных с резервным каналом связи для 3 источников информации: (а) графовая модель, (б) матрица смежности графа

Обрыв основной линии связи возможен на любом из участков *e1 – en*. При этом шинная топология сети предполагает потерю связи со всеми узлами, находящимися дальше места обрыва, что требует немедленного их переключения на резервный канал.

Для определения маршрутов в режимах переключения на резервные каналы связи используется матрица смежности, позволяющая наглядно показать связи

между узлами системы. Матрица смежности для графа, изображенного на рисунке 3.5 (а), представлена на рисунке 3.5 (б).

Задача маршрутизации сетевых потоков в режимах переключения на резервные каналы связи включает три основных этапа: определение факта и участка обрыва основного канала связи, определения оптимального маршрута передачи данных с использованием резервного канала связи и обход недоступных участков сети по резервному каналу.

Определение факта обрыва основного канала связи осуществляется путем регистрации потери связи с одним или несколькими участками АСУ. Код сигнатуры распознавания обрыва C_S включает в себя IP-адрес A_p недоступного узла и временной интервал Δt_p между двумя следующими друг за другом запросами на соединение с узлом A_p. Обобщенная формула формирования кода сигнатуры C_S, имеет следующий вид (3.4):

$$C_S = F_A(A_p, \Delta t_p), \tag{3.4}$$

где F_A – функция формирования кода сигнатуры.

Адрес места обрыва e определяется по мажоритарному принципу (местом обрыва считается тот участок основного канала связи, за которым находятся большинство недоступных узлов) и одновременно является адресом ячейки АП, по которому определяется начальная точка резервного маршрута M передачи данных.

Задача определения маршрута передачи данных при обрыве линии связи ставится следующим образом:

- $M=\{M_1, M_2, \dots, M_n\}$ – множество разрешенных маршрутов передачи информации, n – число разрешенных маршрутов;

- $m=\{m_1, m_2, \dots, m_s\}$ – множество звеньев маршрута; s– количество звеньев маршрута.

- $O=\{O_1, O_2, \dots, O_n\}$ – множество возможных событий обрыва линии связи.

Для каждого источника информации I требуется определить маршрут передачи данных M^x диспетчеру (оператору) D, при котором при любом возможном

событии *O* будет обеспечена полнота получаемой диспетчером информации о состоянии технологического объекта.

Для определения оптимального маршрута передачи данных на вход средств маршрутизации подаются данные о состоянии сегментов основного канала связи. При обнаружении обрыва для обхода заблокированного участка осуществляется переключение портов коммутатора на узлах коммутации на резервный канал. Для переключения используются следующие правила: если источник информации теряет связь с диспетчером, то ближайший к нему узел коммутации переключается на порт резервного канала связи; после обхода заблокированного участка осуществляется обратное переключение на основной канал связи. Если связь с диспетчером установлена, то источник продолжает передавать данные по основному каналу связи.

Пример передачи информации с обходом заблокированных участков КС для сети с 4 источниками представлен на рисунке 3.6.

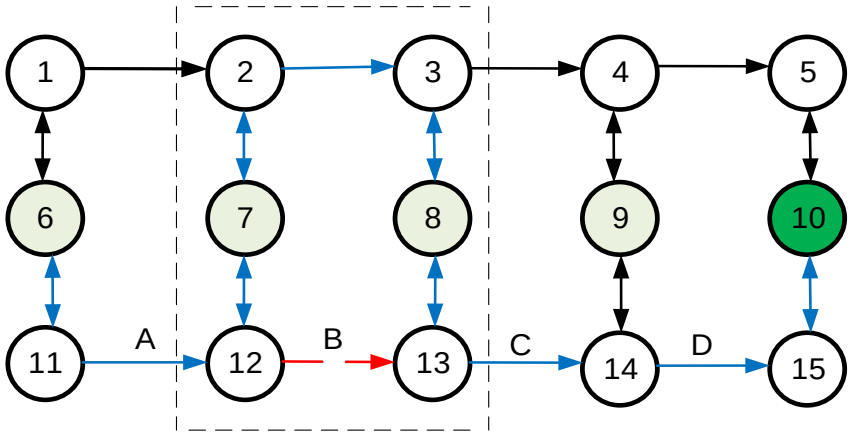


Рисунок 3.6 – Граф маршрутизации сетевых потоков с обходом заблокированных участков для 4 источников информации

Узлами 6 - 8 обозначены источники информации, 10 – диспетчер, 11 – 15 узлы коммутации основного канала связи, 1 - 5 – узлы коммутации резервного канала. Стрелки показывают направления передачи информации по линиям связи. На участке *B* красным цветом обозначен адрес предполагаемого участка потери (обрыва линии) связи, синими стрелками показан маршрут передачи данных с обходом заблокированного участка.

Множество резервных маршрутов, содержащих фрагменты основного и резервного каналов связи, хранится в АП системы защиты информации в центральном диспетчерском пункте АСУ.

Отличительной особенностью является то, что адрес ячейки АП, по которому хранится адрес каждого следующего узла маршрута, формируется на основе адреса текущего узла и сигнала его доступности. В случае доступности информация передается на следующий узел основного канала связи, иначе – резервного. В таблице 3.3 представлен пример заполнения АП в режимах маршрутизации сетевых потоков с обходом заблокированных участков для 4 источников информации.

Таблица 3.3 - Система адресации в АП в режимах маршрутизации сетевых потоков с обходом заблокированных участков для 4 источников информации

Адресная часть ассоциативной памяти в десятичном коде		**Содержимое ячейки памяти в десятичном коде**	**Адресная часть ассоциативной памяти в двоичном коде**		**Содержимое ячейки памяти в двоичном коде**
1	0	2	1	0	10
1	1	6	1	1	110
2	0	3	10	0	11
2	1	7	10	1	111
3	0	4	11	0	100
3	1	8	11	1	1000
4	0	5	100	0	101
4	1	9	100	1	1001
5	1	10	101	1	1010
6	0	1	110	0	1
6	1	11	110	1	1011
7	0	2	111	0	10
7	1	12	111	1	1100
8	0	3	1000	0	11
8	1	13	1000	1	1101
9	0	4	1001	0	100
9	1	14	1001	1	1110
11	1	12	1011	1	1100
11	0	6	1011	0	110
12	0	7	1100	0	111
12	1	13	1100	1	1101
13	0	8	1101	0	1000
13	1	14	1101	1	1110
14	0	9	1110	0	1001
14	1	15	1110	1	1111
15	1	10	1111	1	1010

Пример таблицы маршрутизации сетевых потоков в режимах переключения на резервные каналы связи для четырех источников информации представлены в таблице 3.4.

Таблица 3.4 - Таблица маршрутизации сетевых потоков в режиме переключения на резервные каналы связи для 4 источников информации

Таблица маршрутизации											
Адрес обрыва	**Источник**	**Маршрут**									
A	**6**	1	2	7	12	13	14	15	10		
	7	12	13	14	15	10					
	8	13	14	15	10						
	9	14	15	10							
B	**6**	11	12	7	2	3	8	13	14	15	10
	7	2	3	8	13	14	15	10			
	8	13	14	15	10						
	9	14	15	10							
C	**6**	11	12	13	8	3	4	9	14	15	10
	7	12	13	8	3	4	9	14	15	10	
	8	3	4	9	14	15	10				
	9	14	15	10							
D	**6**	11	12	13	14	9	4	5	10		
	7	12	13	14	9	4	5	10			
	8	13	14	9	4	5	10				
	9	4	5	10							
None	**6**	11	12	13	14	15	10				
	7	12	13	14	15	10					
	8	13	14	10							
	9	14	15	10							

Для исследования модели маршрутизации в динамике была разработана программа на языке Visual Basic Application (VBA) с использованием макросов табличного процессора Excel. В качестве примера реализации модели рассмотрена автоматизированная система управления, включающая диспетчера и четыре источника информации о состоянии технологического объекта. Экранная форма работы программы представлена на рисунке 3.7.

Результатом работы имитационной модели является перечень маршрутов передачи данных для каждого из источников с учетом наличия и места обрыва основного канала связи.

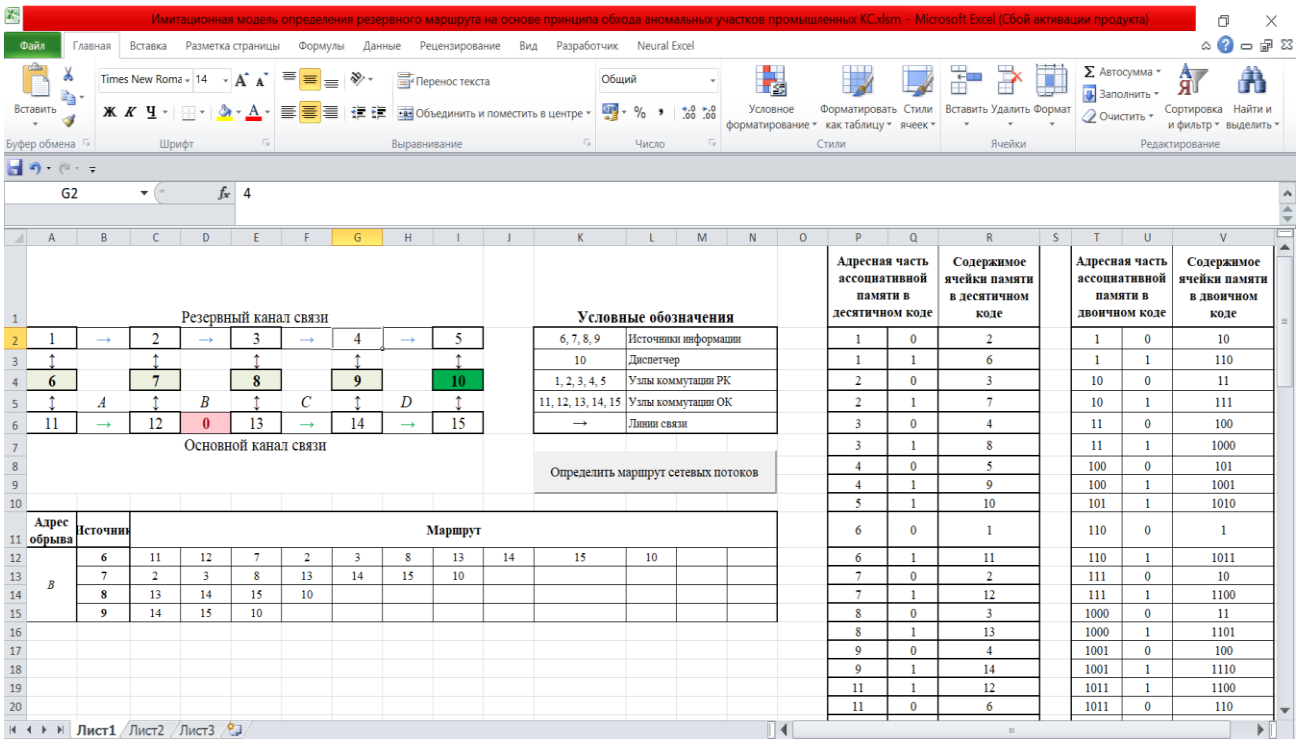


Рисунок 3.7 – Экранная форма имитационной модели определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС

Достоинством разработанной модели является определение каждого следующего узла маршрута в один цикл за время обращения к АП, что повышает оперативность переключения на резервный канал.

Представленная модель положена в основу метода работы определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС. Результаты разработки алгоритма, методики и программной реализации метода и средств для определения резервного маршрута приведены ниже.

3.4 Алгоритм, методика и программная реализация средств определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС

В основе метода определения резервного маршрута лежит принцип обеспечения бесперебойной передачи информации в случае отказа участка основного канала связи по причине его блокирования или физического обрыва.

Схема алгоритма определения резервного маршрута передачи данных на основе принципа обхода аномальных участков промышленных КС представлена на рисунке 3.8.

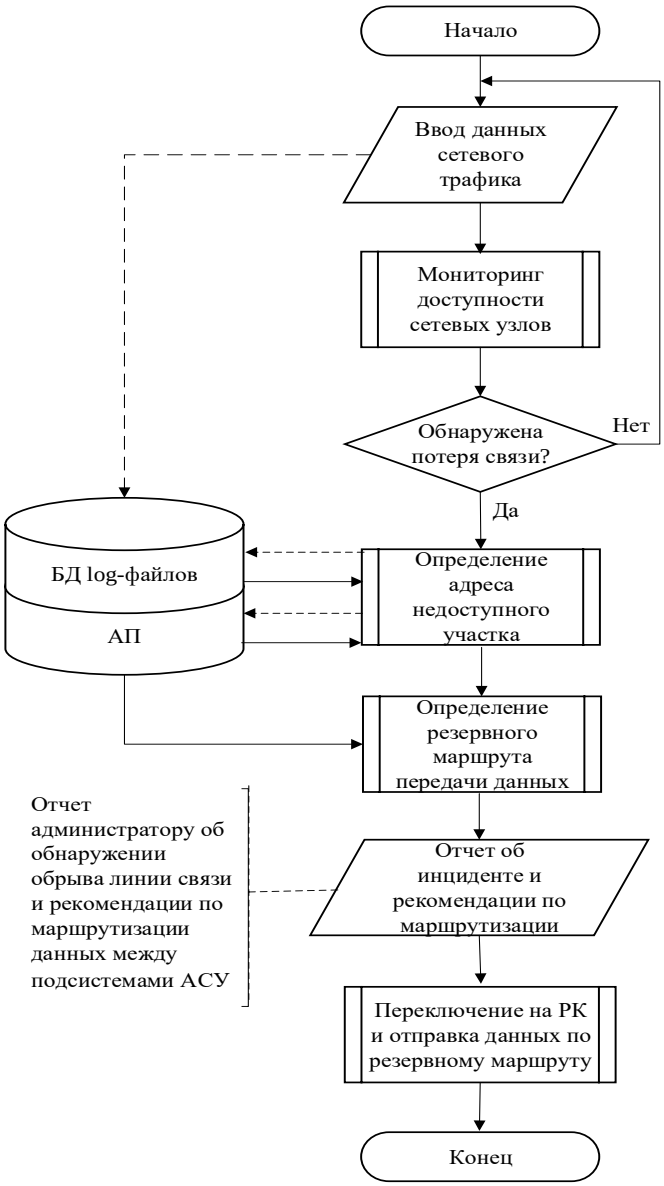


Рисунок 3.8 – Схема алгоритма определения резервного маршрута передачи данных на основе принципа обхода аномальных участков промышленных КС

Исходными данными для мониторинга целостности каналов передачи информации являются сетевые пакеты, передаваемые в промышленной сети. Информация об обрыве линии связи отражается в потоке сетевого трафика. Регламентированные состояния АСУ соответствуют наличию связи между всеми узла-

ми распределённой системы. Нерегламентированные состояния характеризуются наличием повреждения канала связи.

Обнаружение потери связи происходит путем регистрации времени отсутствия ответа от IP-адресов источников информации с использованием штатных средств мониторинга технического состояния АСУ, либо с использованием разработанной программы [5]. Время отсутствия ответа определяется как время между первым и последним запросом на соединение, ответы на которые не были получены. При регистрации потери связи по данным АП производится определение оптимального маршрута передачи данных с использованием резервного канала связи с обходом заблокированных участков сети.

Представленный алгоритм положен в основу разработки программных средств для маршрутизации сетевых потоков в режимах переключения на резервные каналы связи. Экранная форма обнаружения потери связи с использованием программы оперативной регистрации аномальности сетевого трафика [5] представлена на рисунке 3.9.

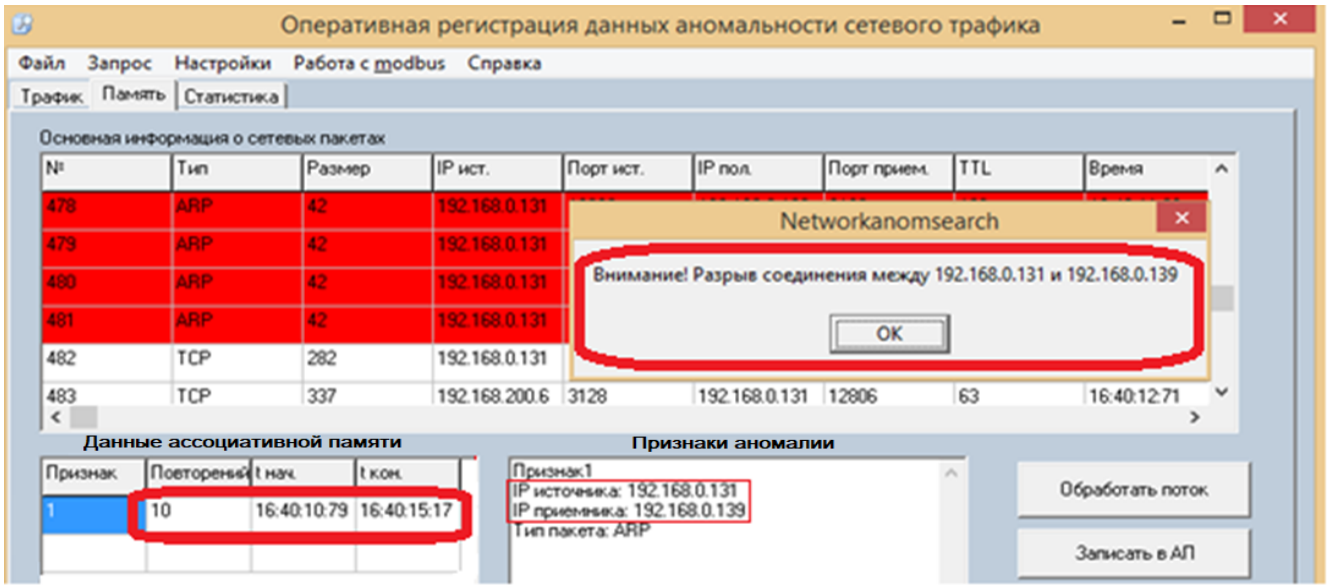


Рисунок 3.9 – Экранная форма обнаружения потери связи

Программа выполняет поиск пакетов, содержащих запрос на соединение с узлами сети, и вычисляет время между регистрацией первого и последнего пакетов запросов, ответы на которые не были получены. В случае превышения време-

ни ожидания ответа на запрос выводится сообщение о разрыве соединения между соответствующими узлами, после чего предлагается резервный маршрут передачи данных.

Экранная форма работы программы определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС представлена на рисунке 3.10. Ввод исходных данных о структуре КС осуществляется администратором на этапе настройки программы.

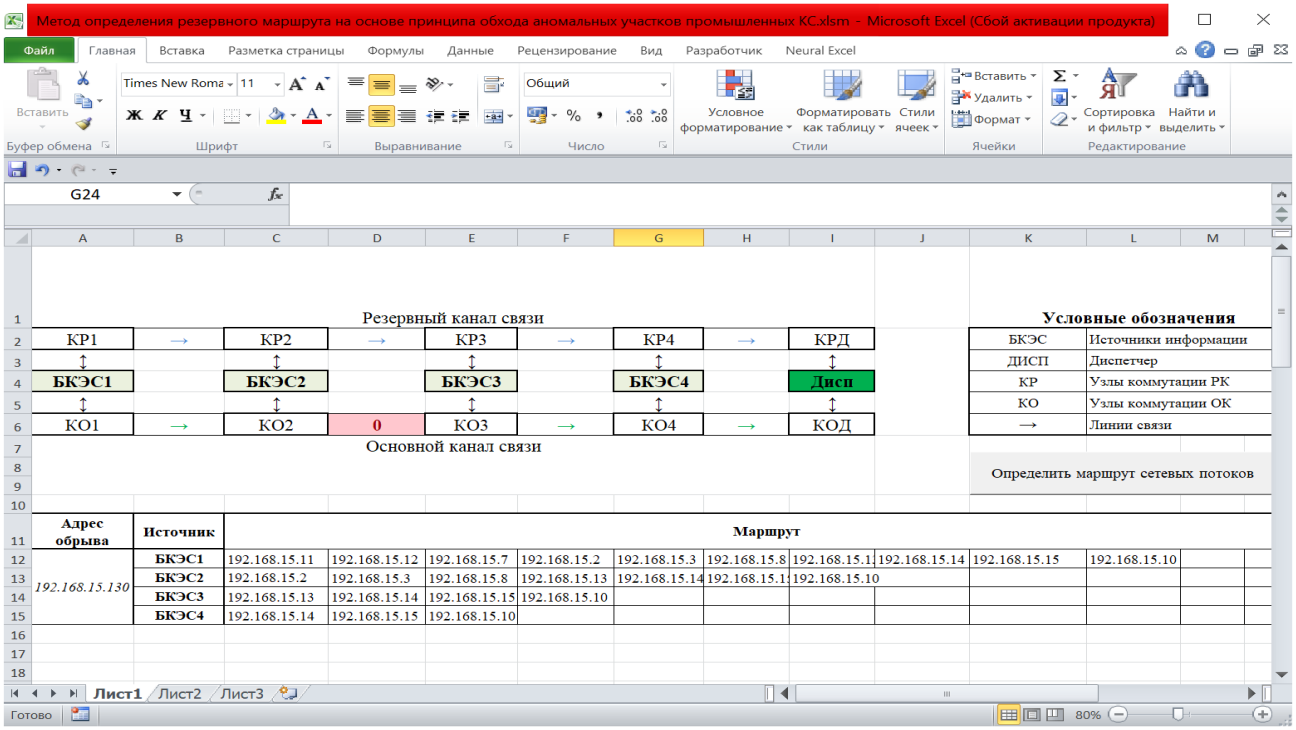


Рисунок 3.10 – Экранная форма определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС

Программа строит маршруты передачи информации между узлами АСУ в зависимости от адреса потери связи. Наличие и отсутствие соединения между узлами обозначены «→» и «0» соответственно. В таблице маршрутизации выводятся рекомендованные маршруты передачи информации между узлами. Перенаправление информации по резервному маршруту может осуществляться администратором сети путем корректировки таблиц коммутации, согласно предложенным маршрутам.

На рисунке 3.11 представлена структурная схема ассоциативного процессора для определения резервного маршрута. На рисунке представлены следующие условные обозначения: *Рг1* – регистр для ввода адреса начального узла маршрута; *Рг2* – регистр ввода адреса конечного узла маршрута; *Рг3* – регистр текущего адреса узла маршрута; *КАУМ* – коммутатор адреса узла маршрута; *АП* - ассоциативная память; БУ – блок управления; СС – схема сравнения; *Вх1* – вход устройства для ввода адреса начального узла маршрута; *Вх2* – вход устройства для ввода адреса конечного узла маршрута; *Вх3* – вход устройства для ввода сигнала готовности к принятию информации от предыдущего узла последующим узлом; *Вых1* – выход устройства для вывода информации об адресе текущего узла маршрута; *Вых2* – выход устройства для вывода запроса о готовности следующего узла к принятию информации.

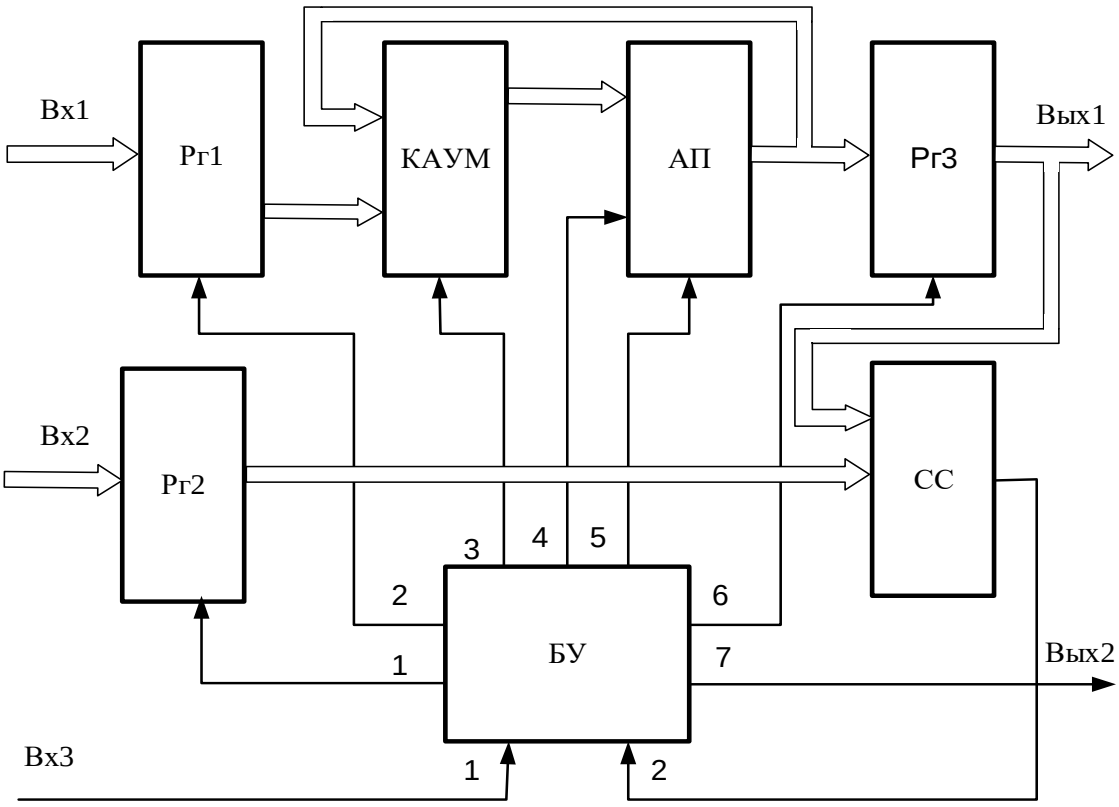


Рисунок 3.11 - Структурная схема ассоциативного процессора для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС

На входы устройства *Рг1* и *Рг2* подаются адреса начального и конечного узлов маршрута соответственно. По адресу начального узла <*n,1*> в ячейке АП считывается адрес следующего узла маршрута n_{+1}, после чего через *Вых2* на узел n_{+1} посылается сигнал запроса о готовности к принятию информации. В случае поступления сигнала готовности, поступающего через *Вх3*, в АП по адресу <n_{+1},*1*> считывается адрес n_{+2} узла и т.д. В случае отсутствия сигнала готовности по адресу <n_{+1},*0*> считывается адрес ближайшего узла резервного маршрута. В блоке *СС* осуществляется сравнение адресов текущего и конечного узлов маршрута. При их совпадении цикл построения маршрута завершается.

Особенностью разработанных метода и методики является использование в качестве резервного канала для обхода заблокированного участка линии передачи электроэнергии промышленного объекта, в данном случае – транспортного трубопровода. В отличие от известных методов маршрутизации, реализуемых с использованием специализированных протоколов (STP, RSTP, OSPF), в предложенном варианте определение маршрута производится за один цикл за время работы ассоциативного процессора.

Оперативное определение резервного маршрута и переключение на резервный канал связи в случае блокирования участка основного канала позволяет снизить риски от угрозы потери технологической информации и предупредить аварии, возникающие в результате несвоевременного выявления и реагирования на изменение параметров технологического процесса. Исследования разработанного метода, результаты которых представлены в работе [45] и разделе 4.2, подтвердили его эффективность на практике.

3.5 Структурно-функциональная модель и метод контроля управляющих транзакций в АС на основе сигнатурного принципа

Одним из основных требований, определяющих эффективность работы АСУ, является корректное выполнение регламентированных управляющих программ и отдельных команд персоналом. Данное требование в настоящее время

приобретает особую актуальность для территориально распределенных АСУ из-за дистанционного характера мониторинга технологических объектов, специфики полевых условий работы персонала и необходимости оперативного принятия решений.

По этой причине задачи мониторинга управляющих действий в АСУ с применением эффективных методов и средств являются актуальными и нашли отражение в современной научной литературе по этой тематике, в частности в работах [31, 32, 48, 101, 102, 107, 108, 119, 136, 146, 161, 163, 169]. Однако в большинстве доступных работ рассматриваются вопросы защиты АСУ от внешнего нарушителя, а контроль сводится к анализу отдельных операций, а не логических последовательностей действий - транзакций. Одним из недостатков рассматриваемых систем мониторинга также является невысокая оперативность средств контроля в условиях работы в режиме реального времени. Вопросы повышения производительности процедур контроля на базе аппаратно-программных средств, по мнению автора, нуждаются в исследованиях и внедрении результатов в распределенных сетях АСУ.

Целью разработки модели и метода мониторинга действий персонала в АС является снижение риска от нерегламентированных управляющих транзакций пользователей промышленной сети на основе анализа сетевого трафика. Для достижения данной цели были разработаны математическая и структурно-функциональная модели контроля управляющих транзакций персонала АСУ, алгоритм и программа мониторинга действий персонала, устройство логического контроля ассоциативности сигнатур управляющих транзакций.

В основу моделей контроля транзакций персонала положены принципы модели Гогена-Мезигера, представленной в работе [19]. В данной модели переход системы из одного состояния в другое выполняется только в соответствии с базой правил, в которой указано, какие операции может выполнять пользователь. Для перевода системы из одного состояния в другое, используются транзакции, то есть некоторые совокупности команд, обеспечивающие смену состояний.

Под управляющей транзакцией в АСУ понимается конечная последовательность логически связанных операций персонала системы (оператора или диспетчера), связанная, например, с переключением исполнительных механизмов системы и изменением режимов работы трубопровода. Все контролируемые транзакции условно делятся на два класса: регламентированных (*Treg*) и нерегламентированных (*Tunreg*). К нерегламентированным относятся транзакции, не соответствующие установленным политикам безопасности на объекте.

Математическая модель контроля транзакций персонала включает [20]:

- множество Q контролируемых транзакций: $Q = \{q_1, q_2, \ldots, q_j, \ldots q_M\}$, где M – число транзакций;

- множество операций в транзакции $O=\{o_1, o_2, o_3, \ldots o_N\}$, где N – число операций;

- множество K информативных признаков транзакции: $P = \{p_1, p_2, \ldots, p_i, \ldots p_K\}$.

В качестве основных признаков распознавания транзакции использованы:

- *IP* - адрес источника транзакции;

- *KT* - код транзакции;

- *NO* - номер операции в транзакции;

- *KO* - код операции.

Кортеж значений перечисленных признаков, полученный по данным сетевого трафика, представленный выражением (3.14), формирует кодовую сигнатуру S для распознавания легитимности операции в транзакции. Код сигнатуры используется в качестве адреса АП, по которому считывается код соответствующей легитимной операции. В таблице 3.5 на примере одной транзакции *KT1*, задаваемой с пульта управления с сетевым адресом *IP1*, показана схема формирования адресной части АП. Содержимое ячеек АП формируется администратором АСУ.

В процессе контроля проверяется совпадение кода адресной части *KO* и кода содержимого ячейки <*KO*>. Несоответствие кодов *KO* и <*KO*> свидетельствует о нелегитимности этой операции, в частности, и всей транзакции в целом.

Таблица 3.5 – Система адресации в АП в режиме контроля транзакции

Адрес ячейки АП					**Содержимое ячейки**
IP	*KT*	*NO*	*H*	*KO*	*<KO>*
IP_1	KT_1	$NO_{1.1}$	$H_{1.1}$	$KO_{1.1}$	$KO_{1.1}$
IP_1	KT_1	$NO_{1.2}$	$H_{1.2}$	$KO_{1.2}$	$KO_{1.2}$
…	…	…	…	…	…
IP_1	KT_1	NO_{1n}	H_{1n}	KO_{1n}	KO_{1n}

Особенностью данной системы адресации является включение в адресную часть параметра *H*, значение которого увеличивается на единицу для каждой последующей операции в случае легитимности предыдущей, что обеспечивает контроль заданной очередности выполнения операций.

Процедура контроля транзакции *T* описывается выражениями (3.5) – (3.9), в которых приняты следующие условные обозначения:

- A_{IP} , A_{KT} , A_{NO}, $A_{KO,}$ A_H представляют собой области допустимых значений, соответственно, для *IP, KT, NO, KO* и *H;*

- Y_O, X_{IP} , X_{KT} , X_{NO} , X_{KO} , X_H представляют собой, соответственно, функцию и аргументы легитимности операции.

$$S = < IP,\ KT,\ NO,\ KO,\ H >; \tag{3.5}$$

$$A = \{A_{IP},\ A_{KT},\ A_{NO},\ A_{KO},\ A_H\}; \tag{3.6}$$

$$Y_o = F(X_{IP}, X_{KT}, X_{NO}, X_{KO}, X_H); \tag{3.7}$$

$$X_{IP} = \begin{cases} 1, \text{ если } X_{IP} \in A_{IP}; \\ 0, \text{ если } X_{IP} \notin A_{IP}; \end{cases} \tag{3.8}$$

$$Y_T = F(Yo_1, Yo_2, \ldots Yo_i, \ldots Yo_N), \quad i = 1, N; \qquad T \in \begin{cases} T_{reg}, \text{ если } Y_T = 1; \\ T_{unreg}, \text{ если } Y_T = 0. \end{cases} \tag{3.9}$$

Операция транзакции из множества *O* считается легитимной в случае, если значение соответствующей логической функции Y_o равно единице. Значение функции Y_o «истина» в случае истинности всех ее аргументов. Значения аргументов функции Y_o (3.7) равно единице в случае принадлежности параметров сигна-

туры S из выражения (3.5) соответствующей области допустимых значений из множества A (3.15). В выражении (3.8) приведено правило определения легитимности операции по аргументу $X_{IP.}$ Определение легитимности по аргументам $X_{KT,}$ $X_{NO,}$ X_{KO} и X_H производится аналогично.

Транзакция T относится к множеству регламентированных T_{reg} в случае истинности функции легитимности транзакции Y_T, значение функции Y_T «истина» в случае истинности всех ее аргументов, согласно выражениям (3.9).

Структурно-функциональная модель последовательного контроля операций персонала при выполнении транзакций в исходной автоматизированной системе показана на рисунке 3.12. В данной модели переходы от одной команды к другой осуществляются без учета результатов предыдущих этапов контроля.

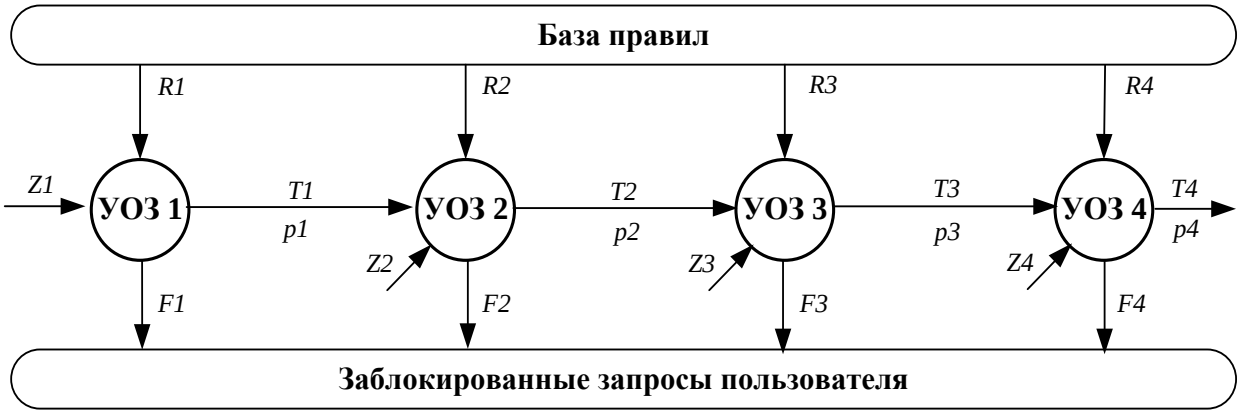


Рисунок 3.12 - Структурно-функциональная модель последовательного контроля операций персонала в исходной автоматизированной системе

На рисунке 3.15 приняты следующие обозначения:

– *Z1 – Z4* – сигналы запросов на выполнение операций транзакции;

– *УОЗ 1 – УОЗ 4* – узлы обработки запроса;

– *T1 – T3* – сигналы разрешения на выполнение операций;

– *F1 – F4* – сигналы блокировки запроса;

– *R1 - R4* – правила контроля операций пользователя;

– *p1 – p4* – оценки вероятностей реализации несанкционированной операции.

При использовании модели, представленной на рисунке 3.12, контроль операций в транзакции осуществляется последовательно с учетом действующих правил и ограничений на ввод команды. Подобный способ не предусматривает проверку результатов предыдущих этапов контроля. Таким образом, в случае получения несанкционированного доступа, злоумышленник получает возможность реализации заключительной операции транзакции, без проверки выполнения предыдущих. Ошибочные команды санкционированных пользователей (операторов, диспетчеров АСУ) на предыдущих этапах транзакции также не учитываются.

Модель, представленная на рисунке 3.13, описывает процедуру выполнения транзакции при полном контроле всех операций персонала на каждом этапе выполнения.

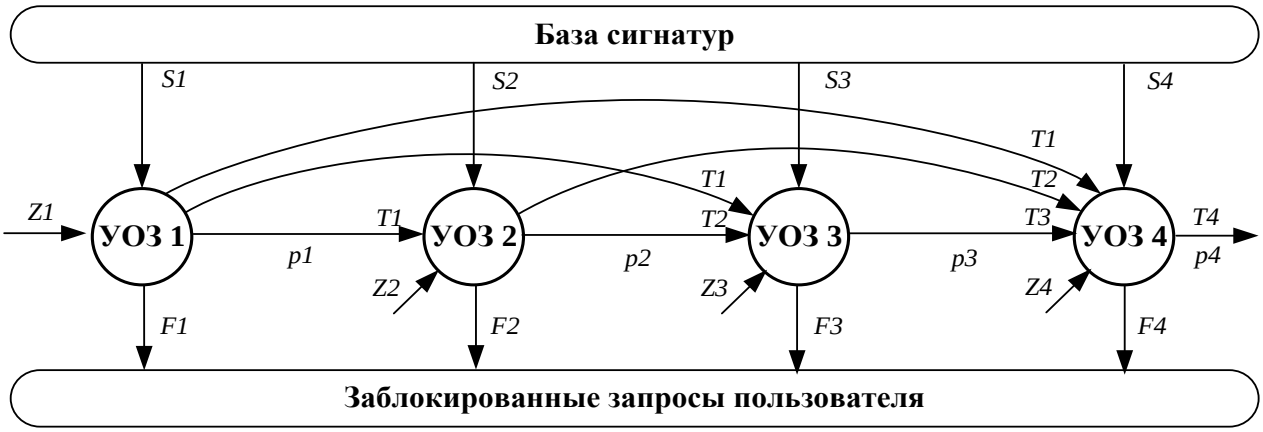


Рисунок 3.13 – Структурно-функциональная модель контроля управляющих транзакций в АСУ на основе сигнатурного принципа

В данной модели в качестве правил контроля выступают сигнатуры операций пользователя *S1 – S4*. Все операции транзакции связаны между собой параметром *H*. При выполнении каждой операции производится проверка санкционированности ее выполнения, а также проверка регламентированности всех предыдущих операций с использованием соответствующих сигнатур. Решение о санкционированности транзакции принимается в том случае, если все действия пользователя в транзакции регламентированы. Если проверка не пройдена – запрос на выполнение транзакции блокируется.

Отличительной особенностью разработанных моделей является невозможность выполнения транзакции в случае несанкционированного доступа нарушителя к заключительной операции, минуя все предыдущие. Также осуществляется мониторинг ошибочной последовательности команд диспетчеров и операторов АСУ при отправке управляющей транзакции.

На основе представленных моделей разработан метод мониторинга действий персонала в АС. Метод предназначен для мониторинга последовательности управляющих операций персонала системы на предмет их соответствия регламентированным инструкциям.

Результаты разработки алгоритма, методики и программно-аппаратной реализации метода и средств мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций представлены ниже.

3.6 Алгоритм, методика и программно-аппаратная реализация средств мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций

Обобщенная схема алгоритма контроля управляющих действий персонала в АСУ представлена на рисунке 3.14. На первом этапе работы алгоритма производится регистрация пакетов сетевого трафика по протоколу Modbus TCP и формирование сигнатуры $\boldsymbol{S}$ операции, согласно выражению (3.5). Далее по выражениям (3.7) - (3.8) на основе сведений, хранящихся в АП, определяется легитимность операции с использованием соответствующих сигнатур. Цикл анализа транзакции завершается, когда достигнуто конечное число операций N. В случае корректного выполнения всех операций производится расчет функции легитимности транзакции по выражениям (3.9).

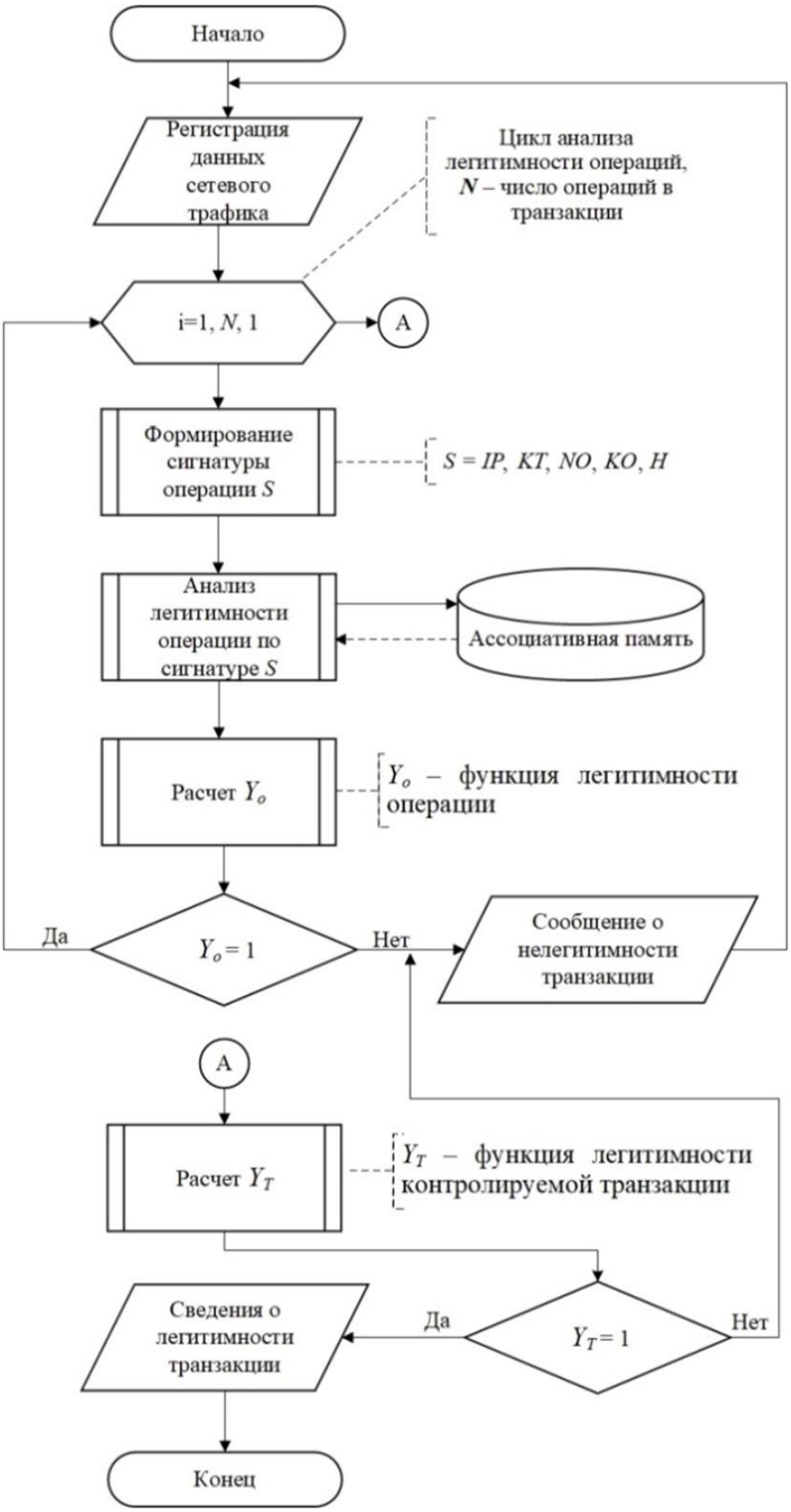


Рисунок 3.14 – Схема алгоритма контроля управляющей транзакции персонала по данным сетевого трафика

Алгоритм положен в основу разработки программного средства [121] для мониторинга управляющих действий персонала. Экранная форма работы программы представлена на рисунке 3.15. Программа предназначена для мониторинга поведения пользователей автоматизированных систем управления по данным сетевого трафика в режиме реального времени. Результатом работы программы являются сведения о нерегламентированных командах и транзакциях персонала АСУ, отражающихся в сетевых информационных потоках системы.

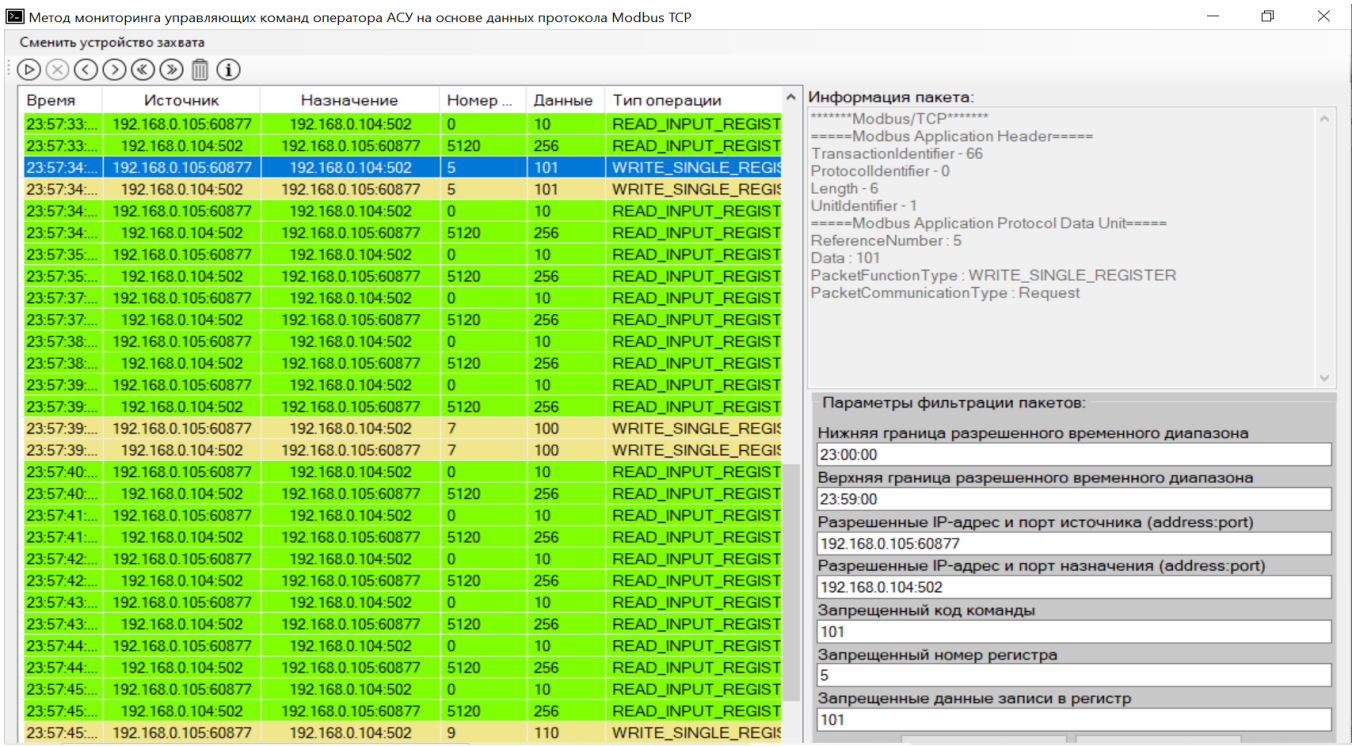


Рисунок 3.15 – Экранная форма процедуры контроля управляющих транзакций персонала

В качестве технического решения по реализации метода разработано устройство для контроля управляющих действий персонала АСУ [45, 143]. Устройство предназначено для использования в системах защиты информации, в частности, для защиты от несанкционированного доступа и нерегламентированных команд персонала системы.

Устройство функционирует в трех режимах:

– режим контроля поведения пользователя АСУ;

– режим анализа поведения;

– режим обучения.

На рисунке 3.16 представлена структурная схема устройства.

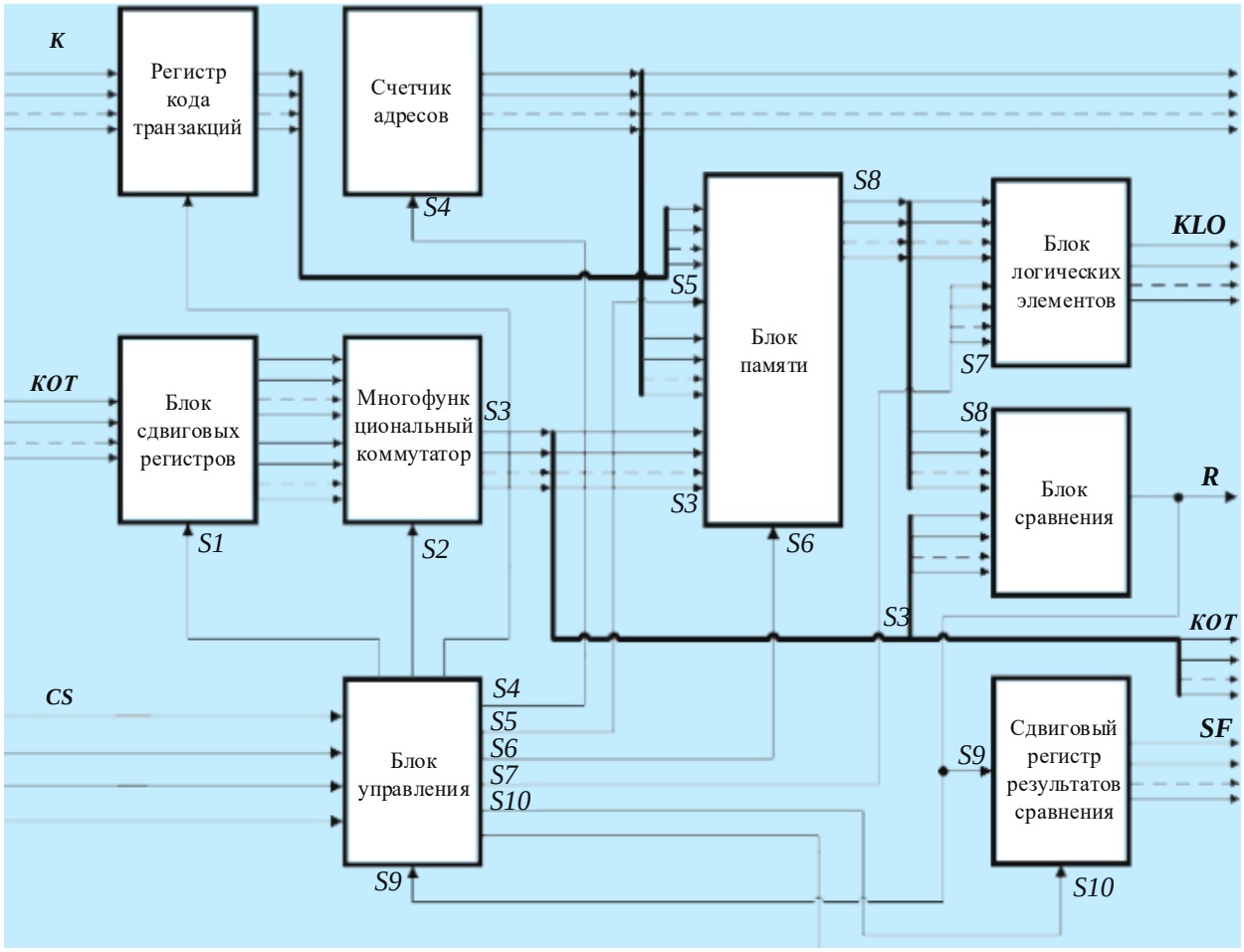


Рисунок 3.16 – Структурная схема устройства для контроля управляющих действий персонала

Буквами на схеме обозначены: *K* – код транзакции, *KOT* – код операции транзакции, *CS* – управляющие сигналы; сигналы: *S1, S2* – подачи *KOT* на вход, *S3* – сигнал записи *KOT* в блок памяти (БП), *S4, S5* – счетные импульсы, *S6* – сигнал чтения, *S7* – сигнал подачи *KLO* на выход , *S8, KLO* – код легитимной операции, *S9* , *SF* – сигнал об ошибке, *S10* – сигнал регистрации ошибки, *R* – разрешение на ввод следующей операции.

В режиме контроля на входы устройства подается код транзакции и код команды. В блоке памяти содержится информация, соответствующая санкциониро-

ванной последовательности команд. Код каждой команды, поданной пользователем, инициирует чтение соответствующего кода из блока памяти. После чего на вход блока сравнения поступает код первой команды пользователя и контрольные коды этой команды из блока памяти. При неравенстве этих кодов режим контроля завершается. При равенстве кодов разрешается ввод последующей команды. При достижении конечного числа команд режим контроля завершается.

Инициализация режима анализа осуществляется путем подачи команды на соответствующий управляющий вход устройства. Режим анализа поведения пользователя предназначен для выявления характера ошибок в поведении пользователя при выполнении транзакции. Режим анализа поведения работает аналогично режиму контроля за исключением того, что при возникновении ошибки ввод команд пользователем продолжается. Код корректности команд фиксируется в сдвиговом регистре результатов сравнения, и по достижении конечного числа команд режим анализа завершается.

Режим обучения предназначен для ознакомления пользователя с составом команд транзакции и порядком их задания. Исходное состояние устройства в режиме обучения соответствует конечному состоянию его в режиме анализа. Ознакомление с командами транзакции осуществляется путем считывания контрольных команд из БП независимо от кодов, сформированных в адресной части блока памяти. Адресный код блока памяти состоит из 4 групп двоичных разрядов: A, B, C и D. Первая адресная группа A содержит код транзакции. Она определяет содержание блока памяти для конкретной транзакции. Код B – одноразрядный, он представляет вторую адресную группу и определяет содержание блока памяти для конкретного режима работы устройства, причем значение разряда равно единице, если устройство работает в режиме контроля и анализа. Значение разряда равно нулю, если устройство работает в режиме обучения. Группа C определяет номер операции в транзакции, а группа D – код операции транзакции, вводимой пользователем.

В качестве примера заполнения БП была взята последовательность действий, совершаемых оператором при управлении задвижкой нефтепровода:

– послать запрос на чтение данных регистров ПЛК;

– открыть задвижку;

– установить значение давления в 70 атм.

Выбранная транзакция вместе с кодами показана в таблице 3.6.

Таблица 3.6 – Коды команд транзакции

Номер по порядку	1	2	3
Обозначение команды	Запрос	Откр/задв	P=70
Код команды	0 0 1	0 1 0	0 1 1

В таблице 3.7 представлено содержимое БП в режиме контроля без ошибок.

Таблица 3.7 – Содержимое БП в режиме контроля без ошибок

№ строки	**Адресная часть**										**Данные**			**Корректность**	**Команда**
	A			B	C			D			E			F	G
0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	не исп.
1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	Запрос
2	0	0	1	1	0	1	0	0	1	0	0	1	0	0	Откр/задв
3	0	0	1	1	0	1	1	0	1	1	0	1	1	0	P=70

Основным достоинством разработанного устройства является возможность распознавания и анализа поведения пользователя, как взаимосвязанной последовательности образов, а также возможность обучения персонала АСУ при выполнении требуемой последовательности операций. Также существует возможность контроля содержимого памяти, самого устройства со стороны администратора безопасности, когда он по специальной проверочной процедуре по гарантированно корректным командам транзакции инспектирует работу самого устройства.

Устройство реализуется на доступной элементной базе электронных микросхем (например, типовые микросхемы серии К155 и микросхема К565РУ1 для блока памяти). Новизна устройства подтверждена патентом на изобретение [143].

Исследования метода, результаты которых представлены в разделе 4.2 и работах [24, 45], показали его высокую эффективность, в частности, значительное снижение вероятности выполнения нерегламентированной транзакции в АСУ, что позволяет нейтрализовать угрозы, связанные с неправомерными действиями персонала системы (УБИ. 061, УБИ. 063, УБИ.107) [53].

3.7 Выводы по третьей главе

Разработаны алгоритмы, методики и программная реализация методов и средств обнаружения аномалий и нейтрализации угроз в КС распределенных автоматизированных систем на основе принципов построения ассоциативных процессоров, что позволяет повысить производительность, достоверность, универсальность средств и снизить риски от угроз БИ. В частности, разработаны:

- метод, алгоритм, методика и программное обеспечение для определения и восстановления маршрутов распространения вредоносного кода по данным сетевого трафика, позволяющие оперативно выявлять маршруты и источники распространения вредоносной информации в КС и принимать превентивные меры по нейтрализации угрозы дальнейшего распространения;

- метод, алгоритм, методика и программное обеспечение для определения резервного маршрута с обходом аномальных участков промышленных КС, позволяющие снизить риски от угроз потери информации о состоянии объекта защиты при ее передаче по каналам связи распределенной АС и повысить оперативность реагирования на возникновение аварийной ситуации;

- метод, алгоритм, методика и программно-аппаратное обеспечение для мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций, позволяющие снизить риски от угроз нерегламентированных управляющих воздействий на систему.

Предложенные решения позволяют повысить технико-экономические показатели подсистем сетевой защиты, учета действий персонала и защиты доступности технологической информации, в частности:

- повышают оперативность поиска данных об аномалии в больших объемах сетевого трафика сложных систем управления за счет использования ассоциативного подхода к хранению и поиску информации о состоянии АСУ;
- повышают достоверность обнаружения и распознавания аномальных состояний АСУ за счет снижения вероятности ошибок 1-го и 2-го рода;
- позволяют снизить ущерб от возникновения нерегламентированных состояний АСУ за счет снижения рисков от наиболее значимых угроз безопасности информации.

Достоверность разработок подтверждена зарегистрированными программными средствами и патентом на изобретение, представляющими практический интерес при построении систем защиты информации для распределенных АСУ. Архитектура разработанного программного комплекса, его характеристика, результаты выбора инструментария для его разработки представлены в приложении Е. Листинги модуля записи данных в ассоциативную память и модуля ассоциативного поиска сведений об аномалии, лежащих в основе работы программных средств, представлены в приложении Ж.

Экспериментальная оценка эффективности результатов исследований и разработка рекомендаций их практического применения в распределенных автоматизированных системах на примере АСУ ТП транспортировки нефтегазового сырья представлены в главе 4.

ГЛАВА 4. ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЙ И РАЗРАБОТКА РЕКОМЕНДАЦИЙ ИХ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ПРИМЕРЕ АСУ ТП ТРАНСПОРТИРОВКИ НЕФТЕГАЗОВОГО СЫРЬЯ

4.1 Сопоставительный анализ методов реализации дихотомического разделения состояний сетевого трафика на основе мажоритарной и нейросетевой моделей

Актуальность проведенных исследований определяется необходимостью выбора рационального инструментального средства для распознавания состояния компьютерной сети (КС). Решению этой задачи посвящен представительный ряд публикаций, в которых в качестве источника исходных данных для анализа состояний используется сетевой трафик (СТ) [38, 64, 70, 59, 180]. В частности, в работе авторского коллектива, проведенной по грантовской тематике [70], определяется обобщённая схема и требования к анализу СТ, рассматриваются основные классы существующих систем анализа с учетом особенностей подключения сетевых узлов к сетям обмена данными и используемой программно-аппаратной базы. В данной работе приводится классификация типовых трафиков, одним из классов которой выделен трафик «сетевая атака/нормальный трафик», исследуемый для защиты от сетевых атак. При этом отмечается, что в случае обнаружения признаков атаки, трафик подлежит дальнейшей уточняющей классификации.

Одним из основных вопросов анализа состояния КС по данным СТ является выбор и обоснование методов и средств классификации временных рядов, отражающих различные состояния КС, в частности, в нормальном (регламентированном) режиме и в режиме передачи по сетевым каналам вредоносного кода.

В качестве альтернативных вариантов классов инструментальных средств (ИС) в исследованиях по тематике раздела чаще всего рассматриваются класс методов на основе нейросетевого подхода [58, 65, 52] и класс методов, основанных на принципах, не связанных с основами построения нейронных сетей. Ко второму классу относятся такие методы распознавания образов, как: метод Байеса, корреляционный подход, рассматриваемый в работе метод с использованием мажоритарной функции, метод геометризированных гистограмм [147].

В качестве критериев оценки качества ИС чаще всего используются оценки характеристик по точности вычислений результатов прогноза, достоверности распознавания, вычислительной и пространственной сложности используемых алгоритмов и загруженности используемых вычислительных средств [111]. Выбор рационального одного метода из двух классов, а также задача разработки метода анализа с учетом достоинств средств для двух альтернативных классов гипотетически улучшает эффективность решения задач распознавания образов.

Целью исследований, приведенных в настоящем разделе, является выбор и обоснование рационального подхода к распознаванию аномального состояния компьютерной сети по спектральным характеристикам временного ряда сетевого трафика. В качестве альтернативных вариантов распознавания аномалии в КС рассматриваются: разработанный автором метод выявления аномальной ситуации в КС на основе мажоритарной модели [36] и на основе типовой нейросетевой модели RProp [28, 198].

Для достижения цели решены следующие задачи:

- дана краткая характеристика альтернативных методов;

- определены критерии сравнительного анализа;

- выбраны и обоснованы инструментальные средства для решения задачи на основе альтернативных моделей;

- проведены экспериментальные исследования для разработки рекомендаций по применению метода распознавания состояния СТ.

В качестве альтернативного нейросетевого в работе рассматривается метод на основе алгоритма обучения Resilient Propagation (Rprop), предложенного в 1993

году М. Ридмиллером (M.Riedmiller) и Г. Брауном (H.Braun). Алгоритм и характеристика метода представлены в интернет-ресурсах [28, 198]. Выбор этого метода обусловлен его высокой производительностью и достоверностью распознавания.

В качестве критериев для сопоставления выбраны два типа критериев:

- параметры ошибок первого и второго рода при распознавании регламентированного образа СТ и образа, соответствующего режиму сетевой атаки;
- параметр вычислительной сложности алгоритма метода на этапе распознавания образа.

Выбор критериев обусловлен возможностью их простого вычисления и использования для выявления лучшего варианта по критерию достоверности распознавания. В качестве инструментальных средств для сопоставления альтернативных вариантов распознавания состояния КС во время распространения по сети вредоносного кода выбраны:

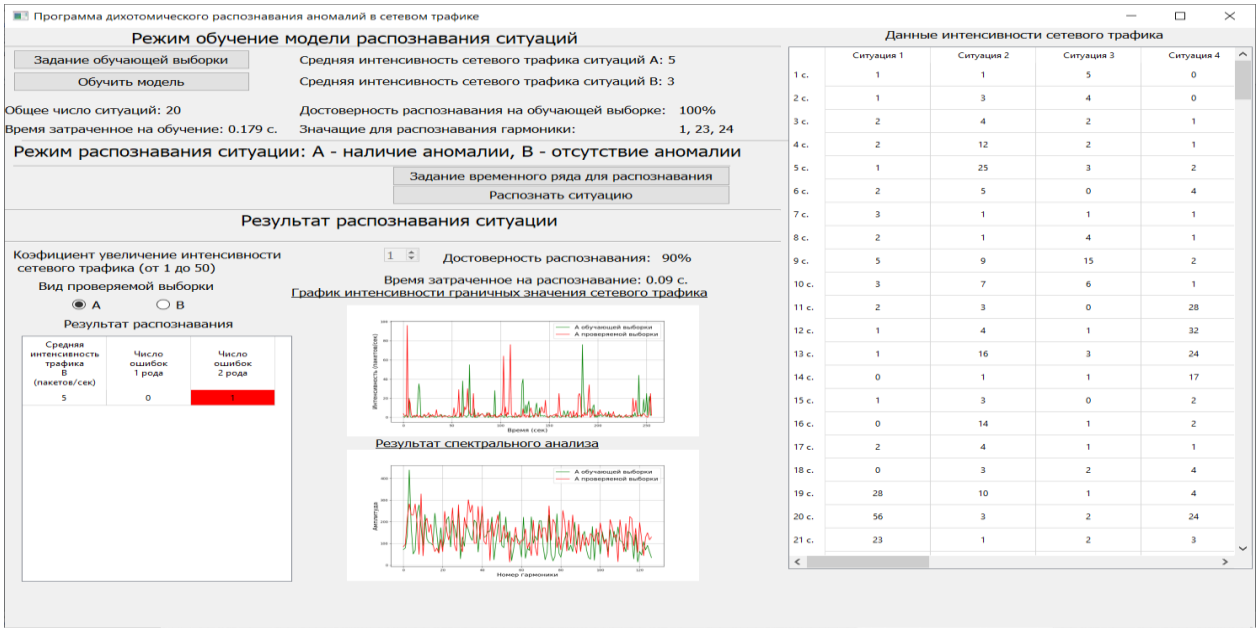
- авторская программа дихотомического распознавания аномалий в сетевом трафике [37], предназначенная для решения научно-исследовательских и учебных задач на персональных компьютерах типа IBM PC 686/Pentium/AMD под управлением операционных систем MS Windows 7/8/10/11 64- или 86-битной архитектуры, систем Linux с использованием Windows API – Wine;

- табличный процессор MS Excel с предустановленной аналитической надстройкой Neural Excel [198], позволяющей создавать, настраивать и обучать нейронные сети типа персептрон.

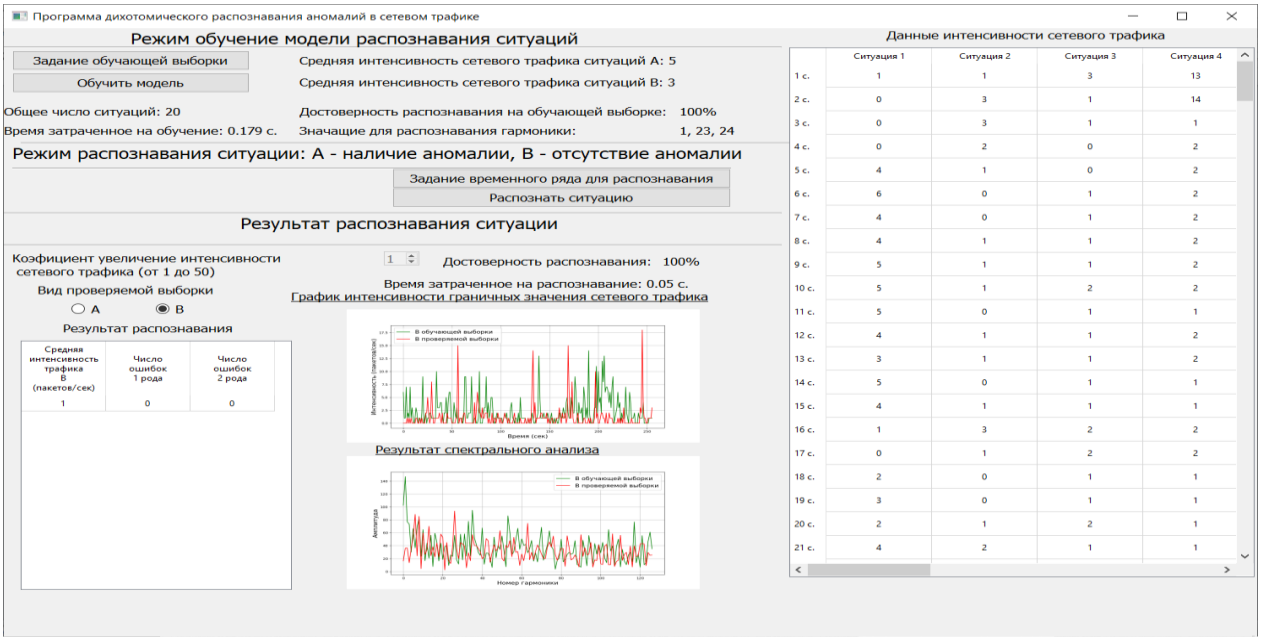
Выбор данной надстройки среди доступных инструментов для разработки и применения нейронных сетей (НС), в частности, MATLAB и PYTHON, обусловлен простотой использования, возможностью быстрого конфигурирования и обучения НС, функциональной полнотой сервисных операций, позволяющих наблюдать за порядком обучения и использования модели.

Обучение и исследование моделей проведено на базе данных из трех источников: полученных экспериментально на учебно-исследовательском сетевом стенде кафедры вуза, данных сетевого сервера Оренбургского государственного университета и с использованием данных датасета сетевого трафика [195] объе-

мом около 1 Гб. На рисунке 4.1 представлены экранные формы интерфейса программы, реализующей дихотомический подход на основе разделяющей функции мажоритарного вида в режимах распознавания состояния СТ во время развития атаки (*A*) и в нормальном состоянии (*B*).



а)



б)

Рисунок 4.1 - Экранная форма интерфейса программы дихотомического распознавания ситуации СТ на основе мажоритарной функции (а – по данным режима атаки, б – по данным регламентированного режима работы сети)

Как видно из рисунка, в качестве информативных модель определила гармоники с номерами 1, 23 и 24. При этом достоверность распознавания состояния с атакой (*A*, пункт «а») на экзаменационной выборке составляет 90%, т.е. одна ошибка на 10 испытаний. В пункте «б» рисунка модель определила результаты без ошибок. Особенностью исследований мажоритарной модели является проверка ее работы в более сложных ситуациях за счет искусственного увеличения интенсивности сетевого трафика I_{cm} в нормальном режиме с целью зашумления информативных гармоник.

Исследования нейросетевой модели проводилось на идентичных исходных данных с использованием табличного процессора MS Excel с предустановленной аналитической надстройкой Neural Excel. На рисунках 4.2 и 4.3 представлены результаты обучения нейронной сети.

Из рисунка 4.2 видно, что обучение модели завершилось после 27 эпох настройки с невысокими ошибками в вычислении результата.

Рисунок 4.2 – Экранная форма графиков обучения нейросетевой модели

Данные рисунка 4.3 позволяют оценить вычислительную сложность алгоритма для конкретного случая с учетом числа слоев модели, числа нейронов по слоям.

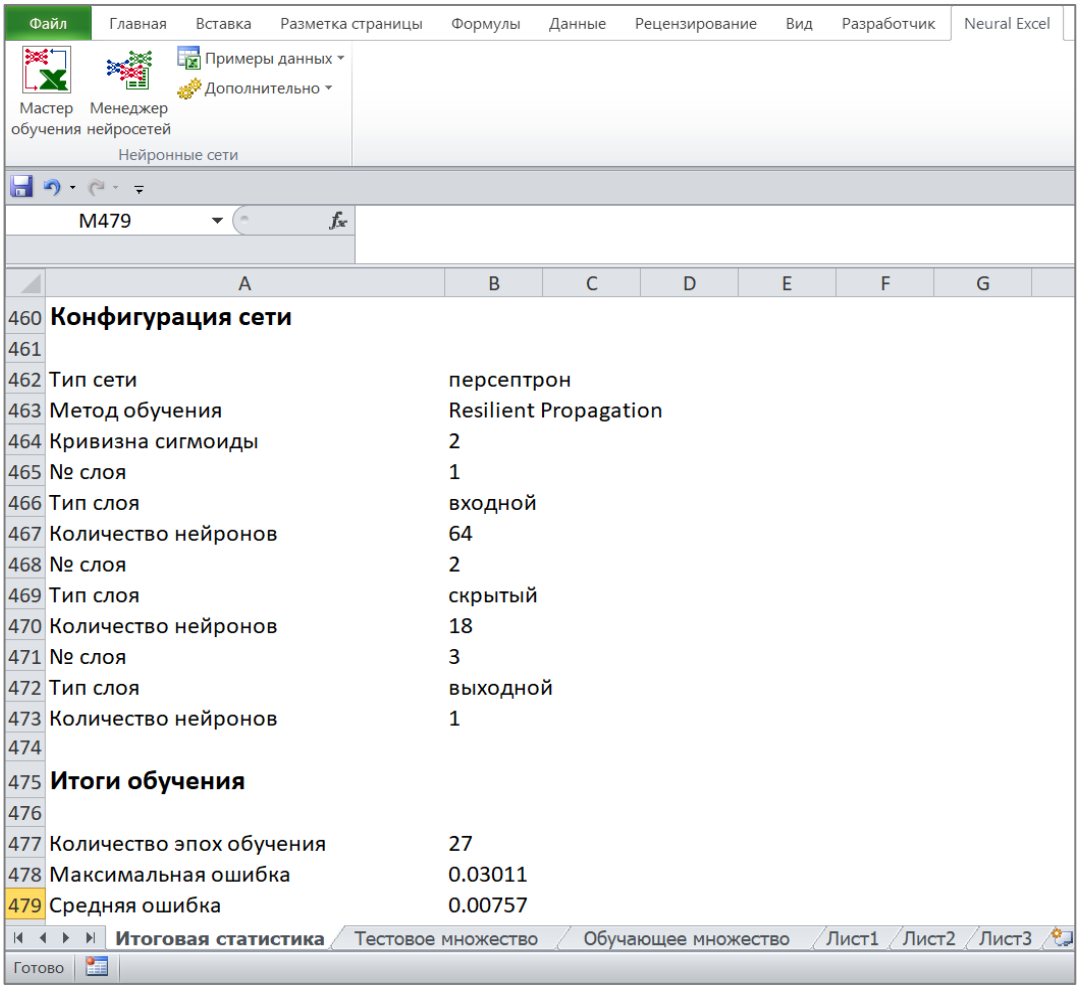
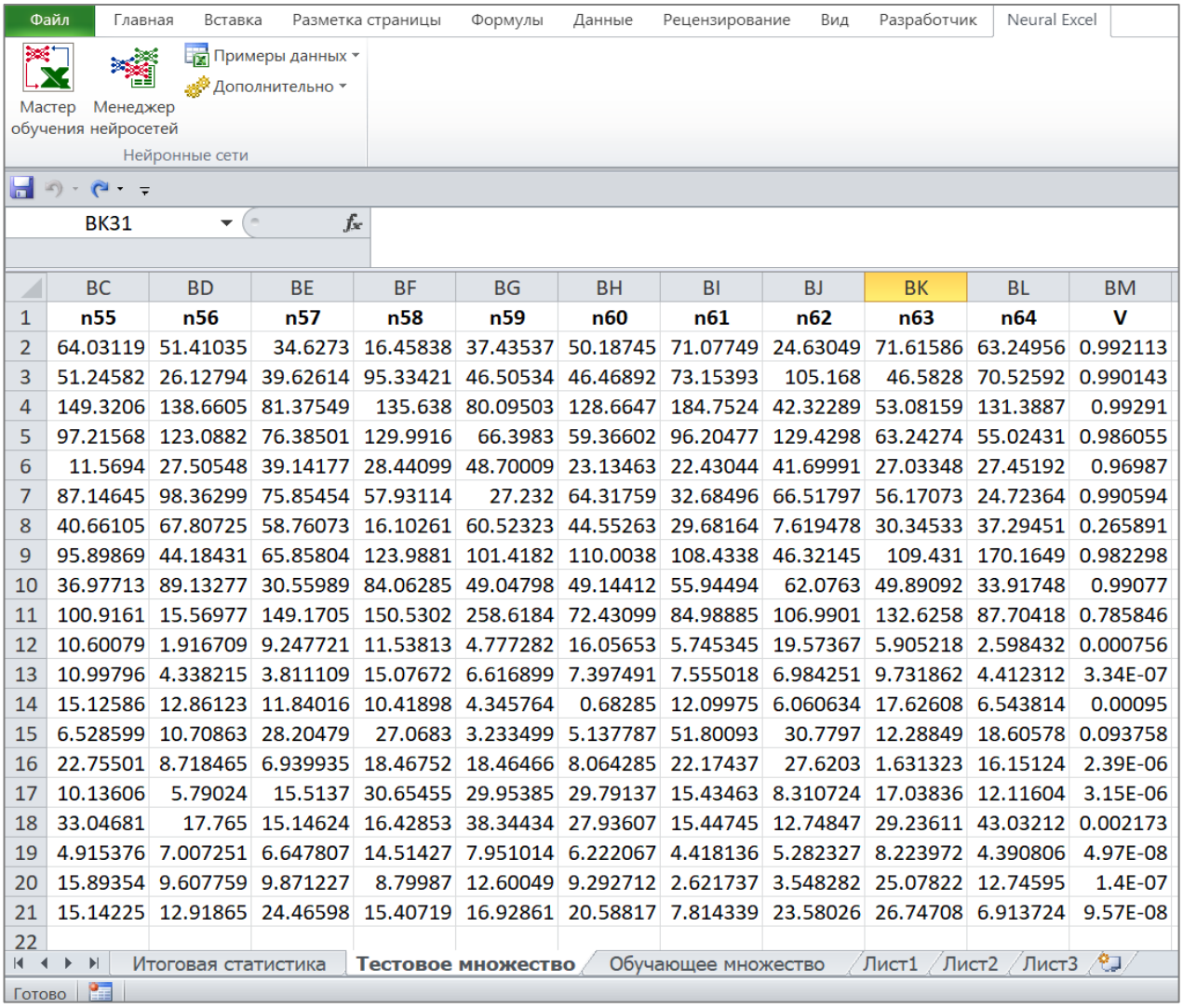


Рисунок 4.3 – Данные результатов обучения нейросетевой модели

На рисунке 4.3 представлен фрагмент таблицы Neural Excel с исходными данными спектральных характеристик гармоник (столбцы *BC-DL*) и колонкой результатов распознавания (колонка *BM*), в которой приводятся оценки принадлежности конкретной строки спектральных оценок состоянию атаки (числа, близкие по величине к 1) и к нормальному состоянию (числа, близкие по величине к 0). Общее число колонок в таблице (64) соответствует числу гармоник. Случайные или выборочные изменения значений спектров в таблице приводят к негативному изменению значений результатной колонки *BL*, что свидетельствует о корректности модели и чувствительности ее к изменению исходных данных.

Данные таблицы, приведенные на рисунках 4.3 и 4.4, свидетельствуют о высокой точности вычисления результатов и достоверности распознавания нейросетевой модели.



	BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM
1	**n55**	**n56**	**n57**	**n58**	**n59**	**n60**	**n61**	**n62**	**n63**	**n64**	**V**
2	64.03119	51.41035	34.6273	16.45838	37.43537	50.18745	71.07749	24.63049	71.61586	63.24956	0.992113
3	51.24582	26.12794	39.62614	95.33421	46.50534	46.46892	73.15393	105.168	46.5828	70.52592	0.990143
4	149.3206	138.6605	81.37549	135.638	80.09503	128.6647	184.7524	42.32289	53.08159	131.3887	0.99291
5	97.21568	123.0882	76.38501	129.9916	66.3983	59.36602	96.20477	129.4298	63.24274	55.02431	0.986055
6	11.5694	27.50548	39.14177	28.44099	48.70009	23.13463	22.43044	41.69991	27.03348	27.45192	0.96987
7	87.14645	98.36299	75.85454	57.93114	27.232	64.31759	32.68496	66.51797	56.17073	24.72364	0.990594
8	40.66105	67.80725	58.76073	16.10261	60.52323	44.55263	29.68164	7.619478	30.34533	37.29451	0.265891
9	95.89869	44.18431	65.85804	123.9881	101.4182	110.0038	108.4338	46.32145	109.431	170.1649	0.982298
10	36.97713	89.13277	30.55989	84.06285	49.04798	49.14412	55.94494	62.0763	49.89092	33.91748	0.99077
11	100.9161	15.56977	149.1705	150.5302	258.6184	72.43099	84.98885	106.9901	132.6258	87.70418	0.785846
12	10.60079	1.916709	9.247721	11.53813	4.777282	16.05653	5.745345	19.57367	5.905218	2.598432	0.000756
13	10.99796	4.338215	3.811109	15.07672	6.616899	7.397491	7.555018	6.984251	9.731862	4.412312	3.34E-07
14	15.12586	12.86123	11.84016	10.41898	4.345764	0.68285	12.09975	6.060634	17.62608	6.543814	0.00095
15	6.528599	10.70863	28.20479	27.0683	3.233499	5.137787	51.80093	30.7797	12.28849	18.60578	0.093758
16	22.75501	8.718465	6.939935	18.46752	18.46466	8.064285	22.17437	27.6203	1.631323	16.15124	2.39E-06
17	10.13606	5.79024	15.5137	30.65455	29.95385	29.79137	15.43463	8.310724	17.03836	12.11604	3.15E-06
18	33.04681	17.765	15.14624	16.42853	38.34434	27.93607	15.44745	12.74847	29.23611	43.03212	0.002173
19	4.915376	7.007251	6.647807	14.51427	7.951014	6.222067	4.418136	5.282327	8.223972	4.390806	4.97E-08
20	15.89354	9.607759	9.871227	8.79987	12.60049	9.292712	2.621737	3.548282	25.07822	12.74595	1.4E-07
21	15.14225	12.91865	24.46598	15.40719	16.92861	20.58817	7.814339	23.58026	26.74708	6.913724	9.57E-08
22											

Рисунок 4.4 – Таблица результатов распознавания состояния сетевого трафика с использованием нейросетевой модели

Одной из особенностей исследований по двум вариант является тот факт, что обе модели ошиблись на одной и той же ситуации в СТ (строка 8 в таблице) на рисунке 4.4.

В таблице 4.1 представлены результаты исследования альтернативных вариантов, определяющих требования к техническим средствам для их реализации

на серийном ноутбуке, используемом в научных исследованиях со следующими характеристиками:

- процессор: Intel(R) Core (TM) i5-8250U CPU @ 1.60GHz 1.80 GHz;

- оперативная память: 4,00 GB (3,86 GB usable);

- операционная система: Windows 10 Home, 64-bit operating system, x64-based processor.

Таблица 4.1 - Анализ технических характеристик альтернативных средств

Вид выборки	**Параметры оценки** / **Вид аномалии**	**Алгоритмическая сложность метода** (ММ/НСМ)	**Объем памяти для хранения программы**		**Загрузка процессоров**		**Достоверность распознавания образов**	
			ММ	НСМ	ММ	НСМ	ММ	НСМ
Реальные данные	Ddos-атака на сервер вуза	$N_{иг} / N_г$ где $N_{иг}$ – число информативных гармоник спектра, используемых при распознавании образа; $N_г$ — общее число гармоник в спектре временного ряда СТ	59 Kb	124 Kb	3,6 – 4,2 %	5 - 8 %	1 ошибка 2 рода	1 ошибка 2 рода
	Распространение вируса-шифровальщика CryptoWall				3,3 – 4,4 %	6 - 9 %	1 ошибка 1 рода, 1 ошибка 2 рода	Без ошибок
Экспериментальные	Данные моделирования Ddos-атаки на сетевом стенде вуза				3,2 – 4 %	6 - 9 %	Без ошибок	1 ошибка 2 рода

Данные по загрузке процессоров, приведенные в таблице при использовании мажоритарной модели (ММ) и нейросетевой модели (НСМ), имеют оценочный характер, определяемый архитектурой используемого компьютера и настройкой операционной системы.

По данным таблицы можно сделать следующие выводы:

- при одинаковых результатах по достоверности распознавания сравниваемых вариантов нейросетевой метод требует примерно в два раза больше памяти для хранения программных и информационных средств, а также загруженности процессорных средств, превышающих альтернативный метод в диапазоне от 30% до 200%;

- алгоритмическая сложность обоих вариантов зависит от объемов исходных данных, причем, для нейросетевого подхода число параметров, используе-

мых при обучении и распознавании равно числу исходных гармоник $N_г$. Для варианта с мажоритарной функцией число параметров на этапе распознавания меньше и соответствует числу информативных гармоник $N_{иг}$, которое определяется на этапе обучения. Для сравниваемых вариантов: $N_{иг} = 3$ для варианта ММ, для варианта НСМ число гармоник, используемых для распознавания, равно 64.

В результате сопоставительного анализа двух методов можно сделать следующие выводы: представленный дихотомический метод распознавания состояния атаки в КС по временному ряду сетевого трафика на основе мажоритарной модели по достоверности не уступает нейросетевому методу, при этом обладает меньшей вычислительной сложностью алгоритма на этапе распознавания образа за счет меньшего числа информативных гармоник, определяемых на этапе обучения распознающей модели. Соотношение $N_{иг} / N_г$ определятся спецификой временных рядов сетевого трафика и требованиями к решению задачи.

4.2 Экспериментальная оценка эффективности применения методов обнаружения аномалий и нейтрализации угроз в распределенных АСУ ТП

Согласно стандарту [79] эффективность применения методов и средств защиты информации следует рассматривать в контексте затрат на обеспечение ИБ в сравнении с издержками, сопряженными с рисками. В соответствии с положениями стандарта и пособия [72] для оценки эффективности разработанных методов использована формула (4.1).

$$E = \frac{R_b - R_n}{\mathrm{C}} \quad , \tag{4.1}$$

где R_b – риск БИ до внедрения разработанного метода, R_n – риск после внедрения, C – стоимость средства защиты информации, реализующего метод.

Эффективность результатов диссертационной работы оценивалась по критерию снижения уровня риска ИБ по отношению к базовым СЗИ с учетом затрат на реализацию средств защиты на основе разработанных методов.

Оценка риска в базовом и новом вариантах производилась на основе вычислительных экспериментов на примере характеристик АСУ транспортировкой нефтегазового сырья одного из месторождений Оренбургской области. В качестве исходных данных для экспериментальной оценки эффективности разработанных методов были использованы данные статистики [115] и сведения, полученные в результате посещения объектов нефтегазовой отрасли Оренбургской области.

В качестве средств защиты информации рассмотрены разработанные программные средства, представленные в таблице В.4 в приложении В.

4.2.1 Исследование эффективности применения метода определения и восстановления маршрутов распространения вредоносного кода

Особое место в перечне задач, направленных на борьбу с распространением вредоносного кода в КС, занимает выбор подхода к мониторингу сетевого трафика на предмет поиска сведений о вирусной атаке и источниках ее распространения, отвечающего требованиям высокой производительности и достоверности. Подобные задачи рассматривались в доступных публикациях, посвященных разработке и исследованию эффективности методов и средств поиска и распознавания аномалий в компьютерных сетях [124, 132, 137, 182].

Среди подходов к мониторингу известны: базовый подход к анализу сетевого трафика как последовательного потока данных [95, 182, 194], и ассоциативно-мажоритарный подход, представленный в работах [41, 112, 137, 184] и положенный в основу методики разработки аппаратно-программных средств и метода восстановления маршрутов распространения вредоносного кода.

Целью настоящего раздела является обоснование эффективности ассоциативного подхода в задачах восстановления маршрутов распространения вредоносного кода в КС. Цель исследования эффективности - выбор высокопроизводительного средства мониторинга сетевого трафика для решения задач антивирусной защиты информации. Объектом исследования являются подсистемы и отдельные хосты КС распределенных автоматизированных систем, а так же процессы обмена информацией между ними. Предмет исследования – методы и методи-

ки мониторинга сетевого трафика на основе базового (*S*) и ассоциативного (*AS*) подходов.

Задача восстановления маршрута распространения вредоносного кода заключается в поиске аномальных пакетов в потоке сетевого трафика и определения связей между ними, формирующих цепочки передачи вредоносной информации. В базовом варианте задача решается простым последовательным перебором и анализом всех записей лог-файла, содержащихся в блоке памяти сетевого трафика ассоциативного процессора (рисунок 2.10). При использовании *AS*-подхода для поиска сведений о распространении вируса производится обращение к строке АП по адресу зараженного хоста и выборка списка взаимодействовавших с ним адресов с учетом времени взаимодействия. Далее в блоке арифметико-логическом строятся маршруты распространения вредоносной информации.

Эффективность метода восстановления маршрута определяется рядом технических характеристик системы мониторинга сетевого трафика, среди которых наиболее важным является производительность, определяемая временем *T* поиска связей (взаимодействий) между IP-адресами зараженных компьютеров. По этой причине в процессе исследований сравнительная оценка альтернативных методов производится по соотношению временных затрат *T* в базовом и новом вариантах в соответствии с выражением: $K = Ts/Tas$, где T_s и T_{as} – время поиска при использовании базового и ассоциативного подходов к анализу сетевого трафика соответственно.

В базовом варианте параметр T_s зависит от числа зарегистрированных пакетов (строк) в анализируемом лог-файле. Для получения полной картины взаимодействия зараженных хостов производится анализ, в среднем, половины строк лог-файла. В каждой строке анализируются поля, содержащие сведения об IP-адресах источника и приемника пакета.

При использовании *AS*-подхода адрес зараженного хоста является адресом строки АП, содержащей сведения о его сетевых взаимодействиях (IP-адрес и время передачи пакета). Для поиска связей между зараженными IP-адресами производится обращение к соответствующим строкам ассоциативной памяти по адре-

сам-сигнатурам. Таким образом, параметр T_{as} в большей степени зависит от числа зараженных компьютеров в сети *Nz*.

Для оценки эффективности ассоциативного подхода спланирован и проведен численный эксперимент, в котором в качестве исходных условий приняты:

- объем лог-файла сетевого трафика: *V*=200; *V*=500; *V*=1000 строк (объемы файлов для исследования выбраны, исходя из материалов датасета [189] распространения вируса wannacry из базы [195]);

- число зараженных хостов *Nz*: 1 – 100;

- время обращения к строке лог-файла и строке АП равно 1 такту (например, 1 мс): t_s = 1 мс, t_{as} = 1 мс;

- каждый IP-адрес встречается в маршруте не более 1 раза.

Результаты эксперимента представлены на рисунке 4.5 и в таблице В.1 в приложении В.

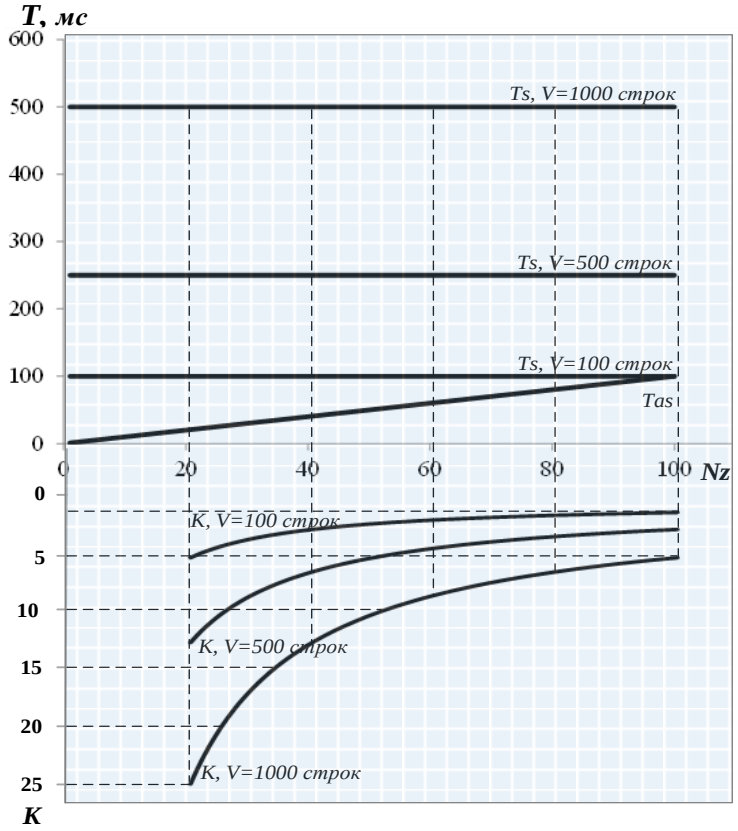


Рисунок 4.5 – Графики зависимости времени восстановления маршрутов распространения вируса в базовом (*Ts*) и новом (*Tas*) вариантах от числа зараженных хостов *Nz* при различных объемах V лог-файла сетевого трафика

Анализ результатов эксперимента показал, что время поиска и восстановления связей между IP-адресами по *AS*-варианту пропорционально числу зараженных компьютеров и, в отличие от базового варианта, не зависит от длительности атаки и объемов анализируемого сетевого трафика. В исследуемой области (при заражении более 20 хостов в КС) показатель производительности поиска ***K*** увеличивается более чем в 2 раза по сравнению с базовым вариантом. Максимальная величина производительности определяется длительностью атаки и увеличивается в десятки раз с увеличением объемов анализируемого трафика.

Повышение оперативности поиска информации о маршрутах и источниках распространения вредоносного кода позволяет предотвратить дополнительный ущерб и, как следствие, снизить риски от сетевой вирусной атаки.

Оценка снижения уровня риска (за счет снижения ущерба от вирусных атак) при использовании метода восстановления маршрутов распространения вредоносного кода проведена на основе вычислительных экспериментов с применением датасетов с вирусными атаками в промышленных КС.

Для оценки возможного ущерба от вирусной атаки проведен численный эксперимент на примере информационно-управляющей подсистемы верхнего уровня с учетом реальных характеристик участка исследуемой АСУ. В ходе эксперимента была смоделирована ситуация, связанная с распространением в подсистеме вируса-шифровальщика с полной потерей программного обеспечения, установленного на автоматизированных рабочих местах (АРМах) в КС. Перечень и средняя стоимость программного обеспечения для одного АРМа на 2022 год представлена в таблице 4.2.

Таблица 4.2 – Стоимость программного обеспечения АСУ

№ п/п	**Программное обеспечение**	**Стоимость лицензии для 1 АРМа**
1	SCADA TRACE MODE 6 + СУБД SIAD/SQL™ 6	11 118 руб.
2	Microsoft Windows 10 Professional (x32/x64)	6 990 руб.
3	Microsoft 365 для бизнеса стандарт	11 700 руб.
4	Kaspersky Endpoint Security для бизнеса расширенный	3 708 руб.
	Итого:	**33 516 руб.**

Таким образом, минимальный ущерб от заражения одного АРМа вирусом шифровальщиком составляет 33 516 рублей. Суммарный ущерб зависит от числа зараженных компьютеров и увеличивается с течением времени.

Вероятность реализации угрозы УБИ.205 [53], характерной для исследуемого класса АСУ при распространении вируса-шифровальщика (согласно базовой модели угроз), составляет $p \approx 0{,}2$. В рамках эксперимента принято условие, что каждый АРМ заражает 2 хоста в минуту.

Результаты численного эксперимента представлены в таблице 4.3.

Таблица 4.3 - Результаты расчета значений ущерба и риска при распространении вируса-шифровальщика

T, ед.	**Число зараженных хостов (Nz)**	**Ущерб (U), руб.**	**Риск базовый (R_b), руб.**
1	1	33516	6703
2	3	100548	20110
3	7	234612	46922
4	15	502740	100548
5	31	1038996	207799
6	63	2111508	422302
7	127	4256532	851306

Анализ графиков на рисунке 4.5 показал, что применение разработанной методики позволяет повысить оперативность восстановления маршрутов и определения маршрутов распространения вредоносного кода более чем в 2 раза по сравнению с базовым вариантом. На основании вышеизложенного, можно сделать вывод, что в случае выявления всех зараженных хостов за T_s = 4 единиц времени с использованием базовых средств риск составит R_b = 100548 руб., в то время как при использовании предложенной методики риск снизится до R_n= 20110 руб. за счет оперативности средств мониторинга сетевого трафика (при T_s = 6, R_b = 422302 и T_{as} = 3, R_n= 46922 и т.д.). Таким образом, для исследуемой системы значение риска от угрозы УБИ.1 снижается не менее чем на 80 тыс. рублей.

Степень снижения риска зависит от числа хостов в сети и величины предотвращенного ущерба и рассчитывается индивидуально для каждой КС.

Результаты оценки экономического эффекта, представленные в приложении Г, показали, что общая себестоимость программных средств для реализации метода составила C = 69368 руб. Подставив результаты оценки рисков в базовом и новом вариантах и стоимость разработанного ПО в формулу (4.1), получим значение $E > 1$, что свидетельствует об эффективности применения разработанного метода.

4.2.2 Исследование эффективности применения метода определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС

Особенностью разработанного метода является концепция использования ВЛЭП в качестве резервного канала связи для обхода заблокированного участка основного канала. В связи с небольшой пропускной способностью ВЛЭП необходимо исследование работы метода на реальных данных. Для исследования был проведен вычислительный эксперимент с учетом реальных характеристик участка АСУ транспортным трубопроводом, представленного на рисунке 1.2.

Объем потока, поступающей диспетчеру, является суммой потоков, передаваемых по каналам связи: основному, информационному (ИК) и резервному (РК) каналам. Предполагаемый объем информации, передаваемой по ИК и РК зависит от числа заблокированных участков и вероятности потери связи с участком p_n (например, в результате повреждения основного канала). Для обеспечения надежной работы АСУ количество получаемой диспетчером информации о состоянии технологического объекта должно отвечать критерию полноты, т. е. информация от каждого источника должна быть доставлена диспетчеру по основному, либо резервному каналу связи своевременно и без потерь. Оперативность и полнота получаемой диспетчером информации зависит от пропускной способности резервного канала и количества источников, передающих информацию.

Базовый риск потери информации R_b при передаче по каналам связи определяется по формуле (4.2).

$$R_b = p_n * (\sum_{n=1}^{N} U_n) * t, \quad (4.2)$$

где p_n – вероятность обрыва основного канала связи на n-ом участке; вероятность p_n на каждом из участков определяется частной моделью угроз; N – число недоступных участков, потерявших связь с диспетчером; U_n – ущерб от потери информации, передаваемой с n-го участка в единицу времени; ущерб U_n зависит от объема информации λ_n, которую необходимо передать диспетчеру с соответствующего недоступного участка; t – время отсутствия связи.

Риск потери информации при использовании резервного канала связи R_r связан с ограничением пропускной способности ВЛЭП и определяется по формуле (4.3):

$$R_r = p_n * \Delta\lambda * t, \quad (4.3)$$
$$\Delta\lambda = (\sum_{n=1}^{N} \lambda_n) - \lambda_L, \Delta\lambda \geq 0,$$

где $\Delta\lambda$ - разница между суммарным потоком информации, передаваемым по резервному каналу связи, и реальной пропускной способностью РК λ_L. В случае, если пропускной способности резервного канала достаточно для передачи информации от всех недоступных участков, $\Delta\lambda = 0$. Обрыв резервного канала связи ввиду его низкой вероятности не рассматривается.

Исследование эффекта от применения разработанного метода проведено на примере АСУ транспортировкой нефтегазового сырья, включающей 10 участков (рисунок 1.2). В качестве исходных данных для исследования выбраны следующие значения: объем передаваемой с одного участка информации $\lambda_n = 5$ Мбит/сек, тестовая пропускная способность резервного канала ВЛЭП - 7 Мбит/сек. Такие значения объема и пропускной способности характерны для рассматриваемых систем [91, 118].

В процессе исследования были рассчитаны риски потери информации при равных вероятностях обрыва каждого из участков p_n=*0,1* основного канала связи при использовании базового варианта АСУ (без резервного канала) и АСУ с резервным каналом. Гистограмма зависимости рисков информационных потерь от

числа недоступных участков основной линии связи представлена на рисунке 4.6. Результаты вычислительного эксперимента представлены в приложении Г.

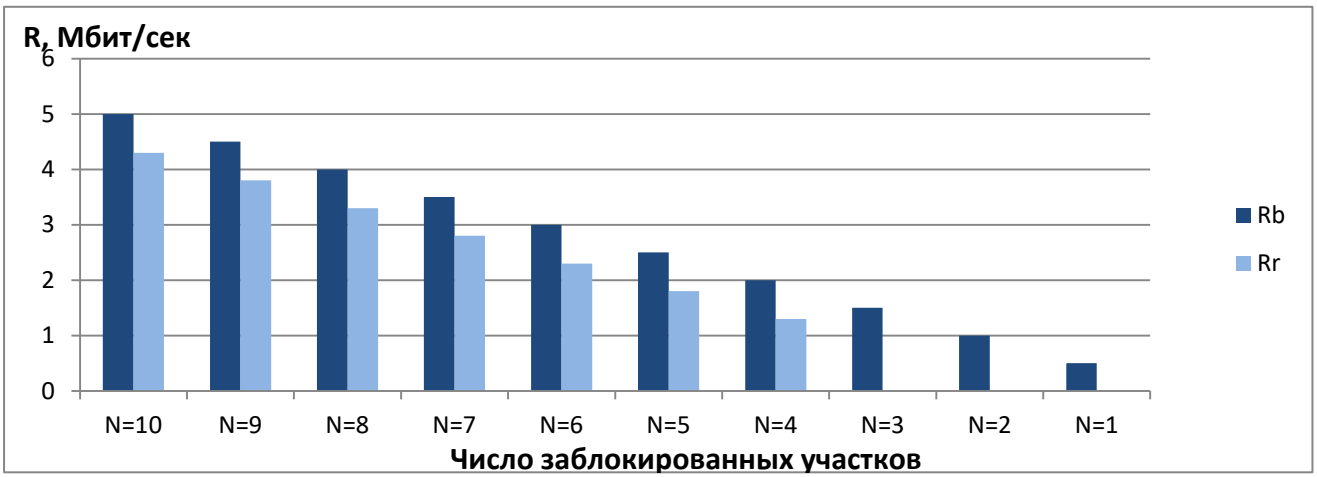


Рисунок 4.6 – Гистограмма зависимости рисков информационных потерь *R* от числа заблокированных участков *N* основной линии связи: *Rb* – базовый риск, *Rr* – риск при резервировании

Анализ полученных результатов позволил выявить зависимость между числом заблокированных участков и величиной ущерба. Риск потери информации при использовании средств маршрутизации на основе разработанных методики и метода определения резервного маршрута для исследуемой системы возникает в том случае, когда потеря связи произошла на 4 и более участках.

Проведенные исследования показали, что использование метода позволяет снизить риск потери информации о состоянии технологического объекта не менее чем на 0,7 Мбит (рисунок 4.6), что составляет 14% технологической информации, необходимой для управления системой. Значения ущерба зависят от стоимости технологической информации в конкретной АСУ.

В отличие от аналогичных средств резервирования, предполагающих передачу информации по резервному каналу вдоль всей линии связи, в основу предложенного метода положен принцип обхода заблокированных участков, что снижает нагрузку на канал ВЛЭП. Определение резервного маршрута производится за один цикл за время обращения к АП, что повышает оперативность передачи данных диспетчеру.

Результаты оценки экономического эффекта от использования разработанного метода, представленные в приложении Г, показали, что стоимость программного средства для его реализации составляет C = 63888,2 руб. Согласно данным статистики [109] ущерб U от аварий на магистральных нефтепроводах, связанных с несвоевременным реагированием на аварийную ситуацию, составляет более 1 миллиона рублей, что значительно выше стоимости разработанного ПО. Таким образом, риск от нейтрализуемой угрозы потери технологической информации (УБИ 136) [53], значительно превышает стоимость разработанного программного обеспечения, что свидетельствует об эффективности применения разработанного метода.

4.2.3 Исследование эффективности применения метода мониторинга действий персонала в АС

Для исследования эффективности метода был проведен численный эксперимент по оценки риска от угрозы несанкционированных действий пользователей АСУ в базовом и новом вариантах. В качестве примера реализации угрозы рассмотрена нерегламентированная транзакция управления давлением в трубопроводе, состоящая из 4 операций.

В рассматриваемой задаче значение риска определяется вероятностями Pt_1 и Pt_2 реализации угрозы выполнения несанкционированной транзакции в базовом и новом вариантах соответственно. При равных значениях вероятности реализации каждой ее операции p_i вероятность реализации всей транзакции определяется по формуле (4.4):

$$Pt = \prod_{i=1}^{n} p_i, \tag{4.4}$$

где n – число операций.

Выполнение нерегламентированной транзакции возможно, например, в результате получения оператором или злоумышленником доступа к одной из заключительных операций, минуя предыдущие. В исходной системе вероятность

реализации транзакции Pt_1 зависит от номера операции, к которой был получен несанкционированный доступ. Чем он ближе к заключительной операции, тем меньше рубежей защиты необходимо преодолеть нарушителю и выше вероятность несанкционированной реализации всей транзакции.

В случае контроля каждой операции пользователя с учетом санкционированности всех предыдущих операций вероятность реализации транзакции в новом варианте Pt_2 одинакова на каждом из этапов ее выполнения (за счет проверки корректности всех предыдущих команд) и соответствует минимальной вероятности, рассчитываемой по формуле (4.4). Графики зависимости вероятностей в базовом Pt_1 и новом Pt_2 вариантах от числа преодолеваемых нарушителем рубежей защиты N при различных исходных значениях p_i представлены на рисунке 4.7. Результаты вычислительного эксперимента представлены в приложении Г.

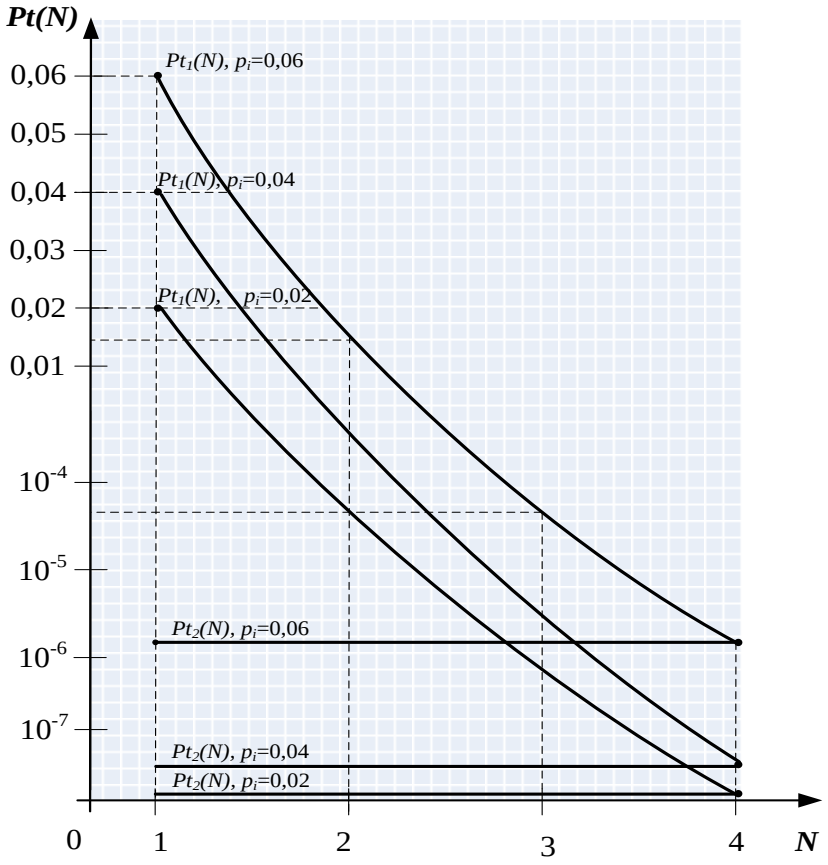


Рисунок 4.7 – Графики зависимости вероятностей реализации несанкционированной транзакции в базовом Pt_1 и новом Pt_2 вариантах от числа преодолеваемых нарушителем рубежей защиты N

На рисунке видно, что вероятности реализации несанкционированной транзакции Pt_1 в исходной системе в значительной степени зависят от числа рубежей защиты, которые приходится преодолевать нарушителю. Соответственно, при получении доступа к последней операции транзакции вероятность ее несанкционированного выполнения максимальна. При применении разработанного метода соответствующие вероятности Pt_2 постоянны для всех операций и соответствуют значениям при максимальном уровне защиты.

Исследование графиков, представленных на рисунке 4.7, показало значительный технический эффект, в частности, снижение вероятности осуществления неправомерной транзакции (более чем в 2 раза).

При равных значениях ущерба в базовом и новом вариантах значение риска от угроз, связанных с нерегламентированными действиями персонала (УБИ. 061, УБИ. 063, УБИ.107) [53] увеличивается прямо пропорционально вероятности реализации неправомерной транзакции. Из этого следует, что аппаратно-программные средства для мониторинга действий персонала в АС, разработанные на основе методики мониторинга действий персонала, позволяют снизить риски от угроз более чем в 2 раза в транзакциях, включающих 2 и более операции.

Результаты оценки экономического эффекта от использования разработанного метода мониторинга, представленные в приложении Г, показали, что стоимость программного средства для ее реализации составляет C = 72463,2 руб, что в разы ниже стоимости коммерческих аналогов (например, системы обнаружения вторжений Kicks for networks [192] или средства защиты от несанкционированного доступа StaffCop [205]). Стоимость аппаратного обеспечения рассчитывается для каждой конкретной системы индивидуально.

Согласно отчету компании Dragos, занимающейся вопросами кибербезопасности АСУ ТП, средняя стоимость одного инцидента ИБ с АСУ ТП обходится организации почти в 3 миллиона долларов ($U \approx$ 284 000 000 руб.). Таким образом, при вероятностях реализации угрозы p = 0,02 – 0,06 (что соответствует базовой модели угроз для исследуемого объекта) риск от нейтрализуемых угроз БИ значи-

тельно превышает стоимость разработанного программного обеспечения, что также свидетельствует об эффективности от применения разработанного метода.

4.2.4 Анализ эффективности разработанных методов

Анализ эффективности разработанных методов проводился на основе системного подхода с учетом особенностей функционирования объекта исследования и модели угроз для рассматриваемой АСУ ТП. Цель анализа - подтверждение технической и экономической эффективности разработанных методов.

В таблице 4.4 представлены результаты анализа эффективности разработанных методов, проведенного по итогам вычислительных экспериментов, представленных в разделах 4.1 – 4.2, результатов лабораторных испытаний, а также испытаний, проведенных в рамках реализации грантов по теме исследования [14 – 41, 45, 46, 42, 184]. Копия справки о выполнении научных проектов по теме исследования представлена в приложении З.

Таблице 4.4 – Анализ эффективности методов обнаружения аномалий и нейтрализации угроз в распределенных АСУ

Метод	**Эффект**		
	Технический	Экономический	Социальный или иной эффект
Метод матричной кластеризации угроз и моделей угроз (МУ) подсистем распределенной АСУ	Сокращение временных затрат на построение СЗИ за счет использования принципов типового проектирования	Сокращение стоимостных затрат на построение СЗИ за счет использования принципов типового проектирования	Повышение эргономических показателей за счет автоматизации процесса анализа частных МУ на этапе предпроектного обследования объекта защиты
Метод обнаружения аномалий в сетевом трафике АС на основе дихотомического подхода	Метод по достоверности не уступает аналогичным, в частности, нейросетевым, при этом обладает меньшей вычислительной сложностью алгоритма на этапе распознавания образа за счет меньшего числа информативных признаков	Затраты на реализацию соизмеримы с затратами на аналогичное программное обеспечение	Повышение эргономических показателей за счет автоматизации процесса обнаружения аномалии в сетевом трафике

Продолжение таблицы 4.4

Метод	**Эффект**		
	Технический	Экономический	Социальный или иной эффект
Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Увеличение оперативности поиска сведений об источниках и маршрутах распространения вредоносной информации в сетевом трафике не менее чем в 2 раза за счет наличия ассоциативных связей между адресами зараженных узлов и признаками вирусной атаки. Максимальная производительность определяется длительностью атаки и увеличивается в десятки раз с увеличением объемов трафика.	Стоимость разработанных программных средств для реализации метода значительно ниже рисков от нейтрализуемых угроз БИ и более чем в 4 раза ниже стоимости коммерческих аналогов (например, системы обнаружения вторжений KICS for Networks)	Снижение рисков от распространения вредоносного кода не менее чем на 80 тыс. рублей, за счет исключения возможности дальнейшего распространения.
Метод определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	Сокращение времени переключения на резервный канал связи за счет определения резервного маршрута передачи данных по адресу обрыва за 1 такт.	Стоимость программного средства для реализации метода значительно ниже рисков от нейтрализуемых угроз БИ и более чем в 4 раза ниже стоимости коммерческих аналогов. Используемый резервный канал связи не требует дополнительных затрат на модернизацию сетевой инфраструктуры.	Снижение риска потери информации о состоянии технологического объекта не менее чем на 0,7 Мбит, что составляет 14% технологической информации, необходимой для управления системой.
Метод мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций	Снижение вероятности несанкционированной транзакции в АСУ не менее чем в 2 раза за счет контроля последовательности и очередности подачи управляющих команд.	Стоимость разработанного программного средства для реализации метода значительно ниже рисков от нейтрализуемых угроз БИ и более чем в 4 раза ниже стоимости коммерческих аналогов	Снижение риска от угроз несанкционированных действий персонала АСУ не менее чем в 2 раза за счет контроля последовательности и очередности подачи управляющих команд.

В таблице 4.5 представлены результаты анализа выполнения требований приказа ФСТЭК №239 [129] при внедрении разработанных методов.

Таблица 4.5 – Анализ выполнения требований приказа ФСТЭК №239

Наименование решения	**Выполнение требований ФСТЭК**
Метод матричной кластеризации угроз и моделей угроз (МУ) подсистем распределенной АСУ	Выполняет требования приказа ФСТЭК №239: - кластеризация информационной (автоматизированной) системы (ОДТ.7).
Метод обнаружения аномалий в сетевом трафике АС на основе дихотомического подхода	Выполняет требования приказа ФСТЭК №239: - контроль и анализ сетевого трафика (АУД.5); - обнаружение компьютерных атак (СОВ.1).
Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Выполняет требования приказа ФСТЭК №239: - реализация антивирусной защиты (АВЗ.1); - обнаружение и предотвращение компьютерных атак (СОВ.1). Позволяет нейтрализовать угрозы БДУ ФСТЭК: - угроза автоматического распространения вредоносного кода (УБИ. 001);
Метод определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	Выполняет требования приказа ФСТЭК №239: - управление сетевыми потоками (ЗИС.6); - резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций (ДНС.4). Позволяет нейтрализовать угрозы БДУ ФСТЭК: - угроза потери информации вследствие несогласованности работы узлов хранилища данных (УБИ. 136); - угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации (УБИ.214);
Метод мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций	"Выполняет требования приказа ФСТЭК №239: - анализ действий отдельных пользователей (АУД.9); - контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях (ОЦЛ.5). Позволяет нейтрализовать БДУ ФСТЭК: - угроза некорректного задания структуры данных транзакции (УБИ. 061); - угроза некорректного использования функционала программного и аппаратного обеспечения (УБИ. 063); - угроза отключения контрольных датчиков (УБИ.107).

Анализ результатов экспериментальной оценки эффекта от использования разработанных методов показал: увеличение оперативности поиска данных о распространении вредоносной информации в сетевом трафике не менее чем в 2 раза за счет принципов ассоциативности, что позволяет снизить риски от угрозы распространения вредоносного кода в КС не менее чем на 80 тыс. рублей; снижение риска потери информации о состоянии объекта защиты не менее чем на 14% за счет использования принципов горячего резервирования и оперативного определения резервного маршрута передачи данных; снижение риска от угрозы несанкционированных действий персонала АСУ не менее чем в 2 раза за счет контроля

последовательности и очередности подачи управляющих команд. При одинаковых функциональных и технических характеристиках суммарные затраты на разработку программных средств для реализации разработанных методов в 4 раза ниже стоимости коммерческих аналогов, в частности KICS for Networks.

Результаты многоаспектного анализа разработанных методов и средств в задаче защиты информации представлены в приложении Д.

Для разработки рекомендаций по применению методов в распределенных управляющих системах проведена их апробация в условиях, соответствующих типовым состояниям промышленной АСУ.

4.3 Апробация результатов исследований

Одной из важных задач построения систем защиты информации в АСУ является исследование внештатных режимов их работы, близких к экстремальным, в частности, в предаварийных состояниях [116, 170, 17]. Разработанные методы предназначены для оперативного обнаружения и распознавания аномального состояния КС АСУ и реагирования на внештатные ситуации, связанные с сетевыми вирусными атаками, потерей связи между подсистемами АСУ, нерегламентированными действиями злоумышленников и персонала системы.

В основе разработанных методов лежит комплекс программных средств, представленных в работах [13, 5, 8, 11, 37, 121]. Анализ проектных решений [116, 125, 154, 183] показал совместимость технических и программных компонентов АСУ с различными СЗИ, при использовании одинаковой размерности физических параметров, а также стандартных интерфейсов и протоколов. Подобная унификация позволяет интегрировать разработанные программные средства в подсистему защиты информации в АСУ, работающую на базе типовых аппаратных и программных решений.

Целью настоящего раздела является проверка работоспособности представленных методов в условиях, соответствующих типовым состояниям промышленной системы управления. Необходимо отметить, что апробация результатов диссертационной работы в реальных АСУ ТП транспортировкой нефтегазового сы-

рья затруднительна, ввиду непрерывности производственных процессов. По этой причине разработанные программные средства были апробированы в лабораторных условиях, максимально приближенных к реальным производственным. В ходе апробации были решены следующие задачи:

- разработана структурная схема имитационной модели мониторинга сетевого трафика в подсистеме сбора и регистрации данных о состоянии АСУ;
- построена мнемосхема системы мониторинга технического состояния нефтепровода в программе «SCADA TRACE MODE»;
- проведены эксперименты по моделированию ситуаций, связанных с сетевыми вирусными атаками, потерей связи между подсистемами АСУ, нерегламентированными действиями персонала;
- проведена апробация разработанных программных средств в условиях, близких реальным внештатным ситуациям в КС АСУ.

При моделировании были учтены основные особенности исследуемой системы, в частности: распределенность АСУ, используемые программные и аппаратные компоненты, сетевые протоколы. Исследования проводились с учетом результатов анализа пространственно-временных моделей угроз для АСУ данного типа. Основные результаты исследований опубликованы в работах [10, 16, 24, 45].

Для получения достоверных оценок были выбраны два вида инструментальных средств: разработанная имитационная модель мониторинга сетевого трафика в подсистеме сбора и регистрации данных о состоянии АСУ на базе средств автоматизации SCADA и программного эмулятора промышленного протокола ModBus TCP.

Структурная схема имитационной модели мониторинга сетевого трафика в подсистеме сбора и регистрации данных о состоянии АСУ представлена на рисунке 4.8. Имитационная модель представлена подсистемой моделирования датчиков *Д1* и *Д2* и исполнительного механизма *ИМ*, модулем управления, представленным подсистемой моделирования программируемого логического контроллера *ПЛК*, подсистемами моделирования верхнего и нижнего уровней АСУ и мониторинга сетевых аномалий. Все структурные компоненты

представленной модели имитировались на стационарных компьютерах научно-исследовательского сетевого стенда кафедры вычислительной техники и защиты информации Оренбургского государственного университета в лабораторных условиях. Описание информативных признаков аномалии по данным поученного сетевого трафика представлено в приложении Б.

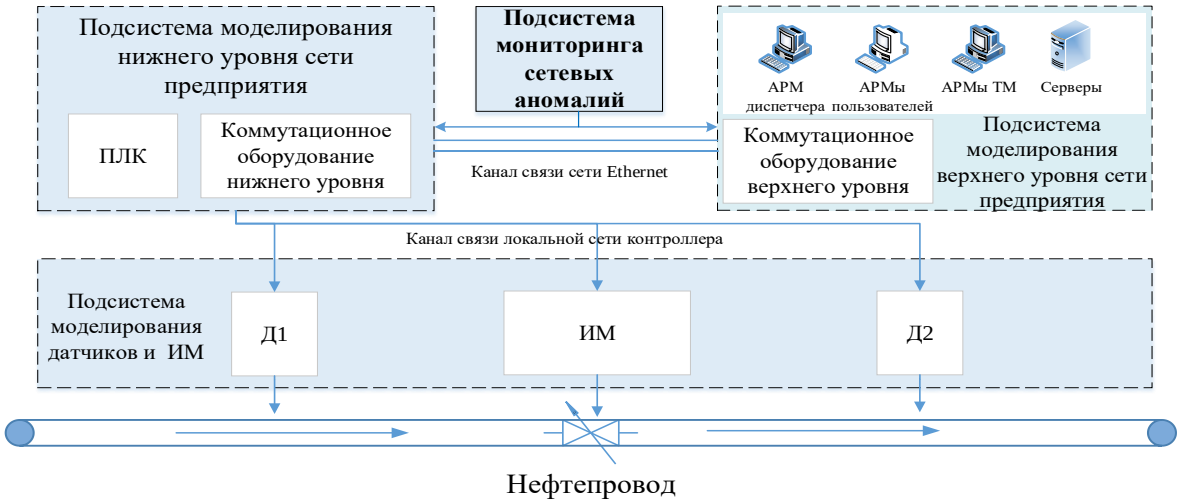


Рисунок 4.8 – Структурная схема имитационной модели мониторинга сетевого трафика в подсистеме сбора и регистрации данных о состоянии АСУ ТП

Для моделирования нефтепровода, датчиков, ПЛК и исполнительного механизма в программе для автоматизации технологических процессов «SCADA TRACE MODE» [154, 202] была построена мнемосхема, представленная на рисунке 4.9, и разработан программный комплекс для формирования промышленного сетевого трафика. Разработанный программный комплекс состоит из программ: PLC_Simulator и Scada_pipeline [10]. Программа PLC_Simulator имитирует работу удаленного ПЛК, контролирующего давление в трубопроводе, а также управляющего открытием/закрытием задвижки. Программа Scada_pipeline реализована в среде Trace Mode 6.0 и позволяет контролировать и управлять состоянием трубопровода через удаленный ПЛК. Подключение к удаленному ПЛК производится по протоколу ModBus TCP.

Подсистема мониторинга, мнемосхема которой приведена на рисунке 4.9, обеспечивает контроль основных технологических параметров участка трубопро-

вода: давления, температуры, загазованности, расхода нефти и т.д. Давление на данном участке нефтепровода регулируется задвижкой, переключаемой исполнительным механизмом. Измерение значений давления происходит с помощью датчиков, устанавливаемых до и после задвижки. Команды на исполнительный механизм поступают от контроллера после получения им соответствующих директив от диспетчера.

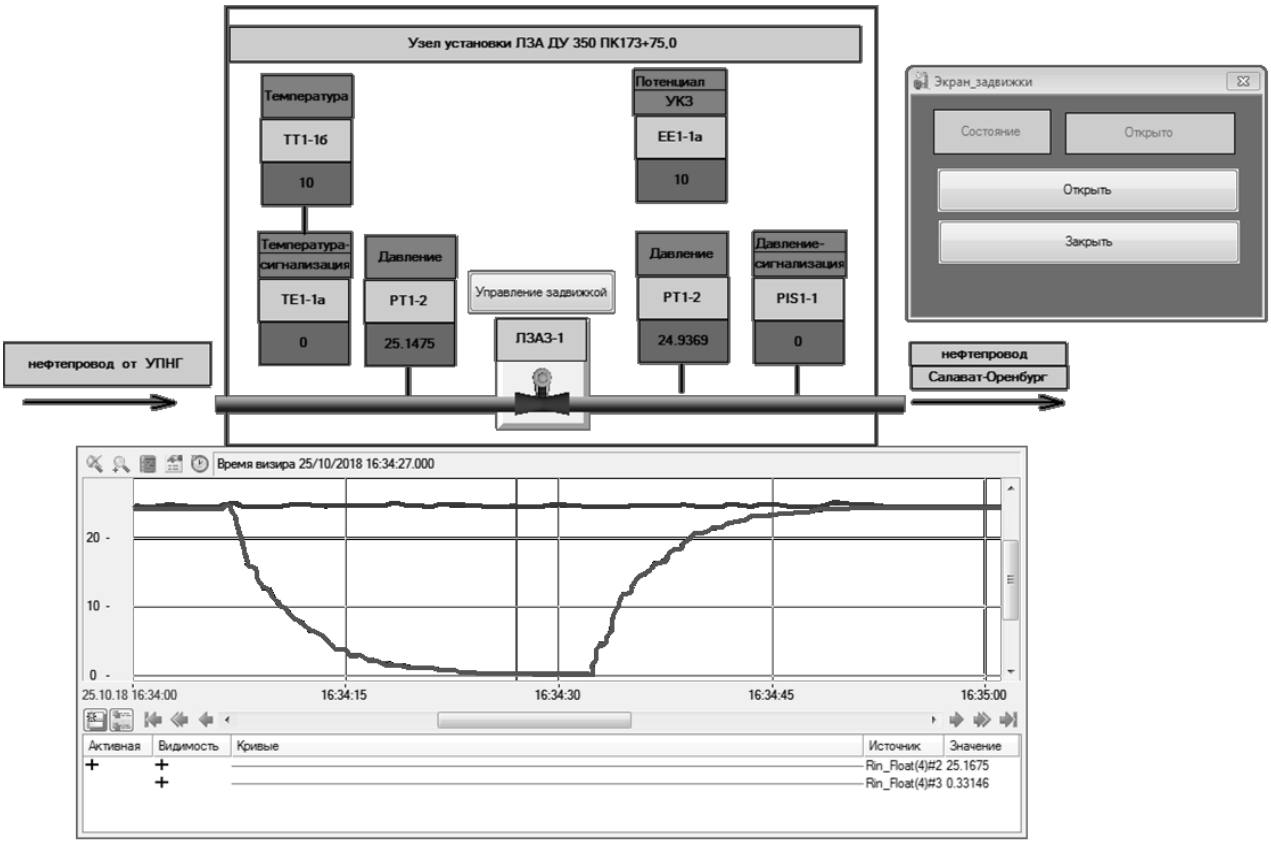


Рисунок 4.9 – Мнемосхема подсистемы мониторинга технического состояния участка нефтепровода

На экране компьютера оператора в режиме реального времени отражаются основные параметры технологического процесса. При выходе контролируемых параметров за границы допустимых значений оператор должен получать извещение об аномальном состоянии системы.

В ходе апробации моделировались различные варианты воздействия на КС АСУ. Исходные данные экспериментальных исследований, проведенных при апробации, представлены в таблице 4.6.

Таблица 4.6 – Исходные данные экспериментальных исследований

Апробируемый метод	Моделируемый инцидент	Исходные данные	Цель
Метод обнаружения аномалий в сетевом трафике АС на основе дихотомического подхода	Аномальное состояние КС, вызванное инцидентом ИБ (на примере сетевых атак)	Повышенная интенсивность сетевого трафика, вызванная сетевой атакой	Обнаружение аномального состояния КС
Метод восстановления маршрутов распространения вредоносного кода	Распространение вредоносного кода по локальной сети	Заражение одного из хостов сети вирусом удаленного доступа с последующей рассылкой с него вируса-шифровальщика компьютерам сети	Поиск маршрутов распространения вируса-шифровальщика, всех зараженных узлов и источника заражения, открывающего удаленный доступ к сети
Метод определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	Обрыв линии основного канала связи	Физический разрыв соединения между компьютерами, имитирующими диспетчера и ПЛК	Обнаружение факта обрыва линии связи, извещение диспетчера об инциденте, определение резервного маршрута передачи данных
Метод мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций	Несанкционированная транзакция закрытия задвижки	Запись в регистры контроллера команд на закрытие задвижки трубопровода	Обнаружение несанкционированной транзакции управления

Результаты апробации разработанных методов представлены ниже.

4.3.1 Апробация метода обнаружения аномалий в сетевом трафике АС на основе дихотомического подхода

Для исследования работы метода при высоких интенсивностях сетевого трафика, была построена экспериментальная вычислительная сеть на базе научно-исследовательского сетевого стенда (НИСС) [3]. Структурная схема стенда представлена на рисунке 4.10.

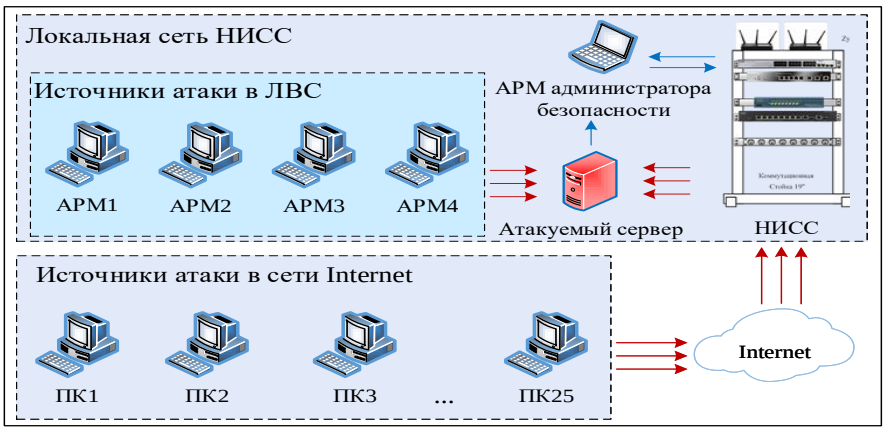
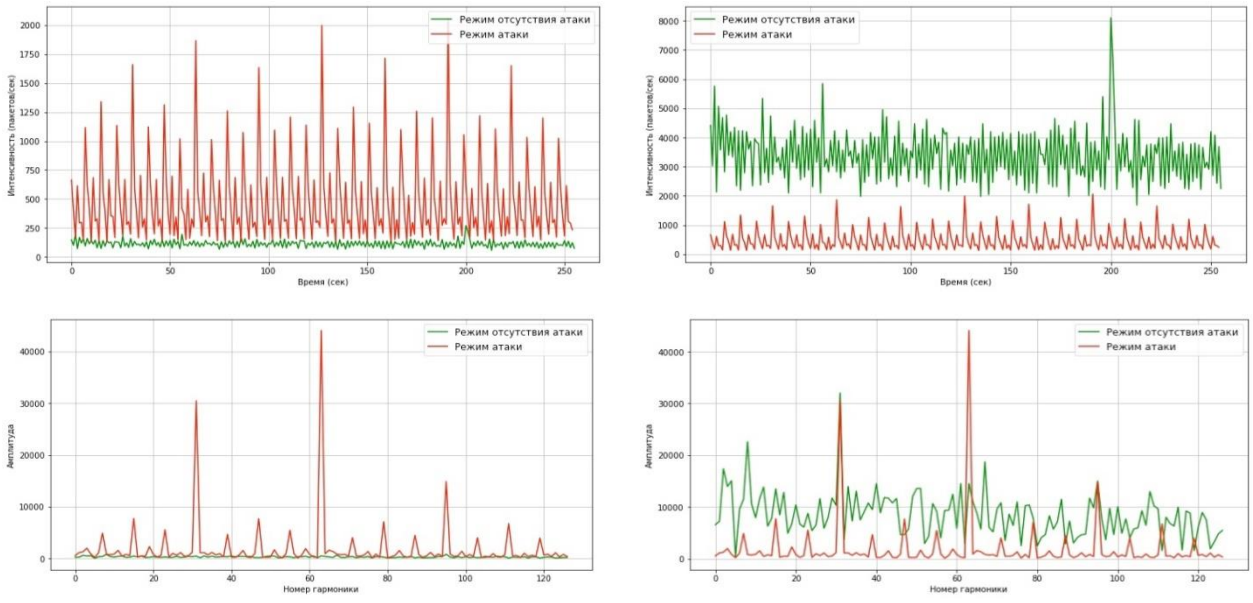


Рисунок 4.10 – Структурная схема НИСС

В ходе натурного эксперимента была исследована работа метода с учетом разных уровней интенсивности сетевого трафика в режимах сетевой атаки (на примере вирусной и dos атак) и отсутствия атаки. Для моделирования аномалий было проведено 10 экспериментов. В результате был собран трафик работы сети в режиме атаки и в режиме отсутствия атаки общим объемом около 700 Мбайт. На основе полученных данных сформированы обучающее и тестовое множества файлов сетевого трафика.

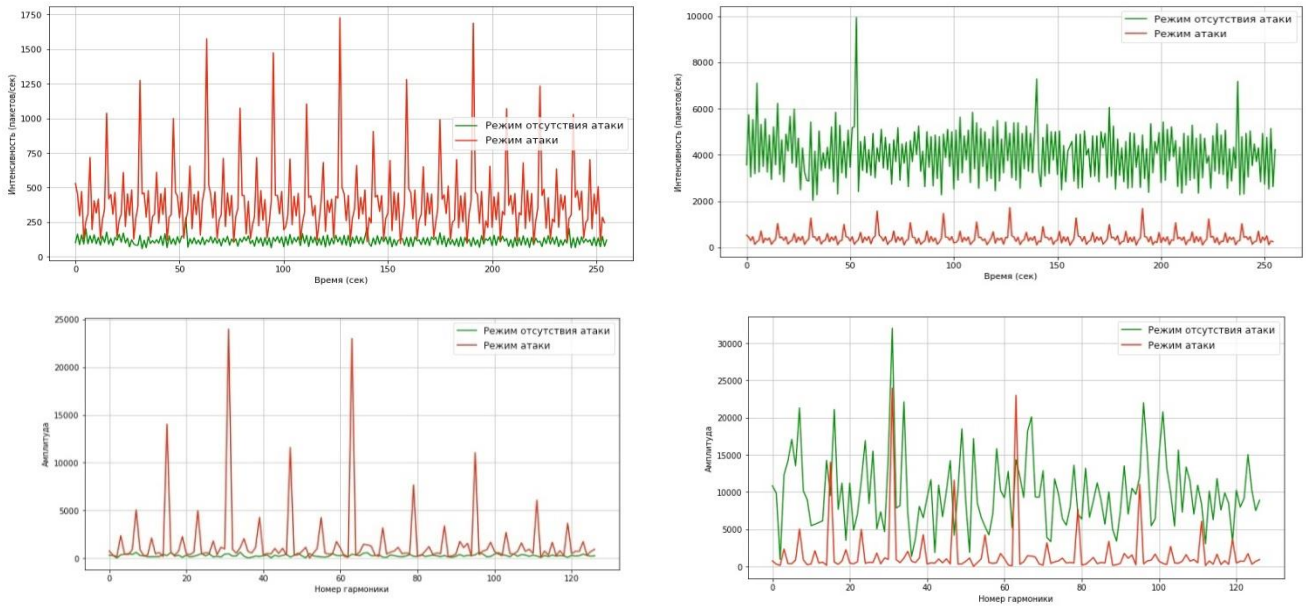
Ввиду невозможности создания высокой интенсивности сетевых потоков в экспериментальной сети, был проведен вычислительный эксперимент с генерацией высокоинтенсивного трафика. В качестве исходного материала для исследования использовались собранные за 256-секундные интервалы значения интенсивности сетевого трафика, полученного в ходе натурного эксперимента.

Графики интенсивности и результаты спектрального анализа сетевого трафика при низком и высоком уровнях интенсивности сетевого трафика представлены на рисунках 4.11 – 4.12.



а) б)

Рисунок 4.11 - Графики интенсивности и результаты спектрального анализа сетевого трафика: (а) при низкой интенсивности сетевых потоков, (б) при высокой интенсивности сетевых потоков с ошибкой 1 рода



а) б)

Рисунок 4.12 - Графики интенсивности и результаты спектрального анализа сетевого трафика: (а) при низкой интенсивности сетевых потоков, (б) при высокой интенсивности сетевых потоков с ошибкой 2 рода

Анализ полученных результатов показал высокую достоверность распознавания аномалий. Ошибки распознавания характерны для временных рядов со средней интенсивностью трафика 3,5 тыс. пакетов в секунду (для ошибок 1 рода) и 4 тыс. пакетов в секунду (для ошибок 2 рода). Малая вероятность такой интенсивности сетевого трафика в реальных сетях позволяет сделать вывод о высокой достоверности распознавания. Исследование модели с интенсивностью, характерной для штатного режима работы сети (до 1 тыс. пакетов в секунду) показало отсутствие ошибок 1 и 2 рода при распознавании на экзаменационной выборке.

При распознавании ситуаций по данным СТ с интенсивностями верхнего уровня диапазона ошибки первого и второго рода не превышали 5 %.

Апробация метода также проводилась на основе реальных данных сетевого трафика, полученных при регистрации Dos-атаки в КС Оренбургского государственного университета. Интенсивность поступления пакетов не превышала 110 пакет/сек. со средней дисперсией 93,8 в режиме атаки и 7,3 в режиме отсутствия атаки.

Погрешности первого и второго рода при распознавании аномалий в КС на реальных данных СТ компьютерной сети вуза не превышали 3 %.

Анализ результатов показал высокую оперативность и достоверность выявления аномального состояния КС по характеристикам интенсивности пакетов сетевого трафика на основе дихотомического подхода.

4.3.2 Апробация метода восстановления маршрутов распространения вредоносного кода по данным сетевого трафика

Для апробации метода была смоделирована атака на локальную сеть, в ходе которой проводилось заражение компьютера диспетчера программой удаленного доступа с последующей рассылкой с него вируса-шифровальщика всем узлам промышленной сети.

В качестве исходных данных для анализа был использован сетевой трафик, полученный с коммутационного оборудования верхнего уровня моделируемой промышленной сети. Экранная форма процесса поиска фрагментов данных о вирусной атаке представлена на рисунке 4.13.

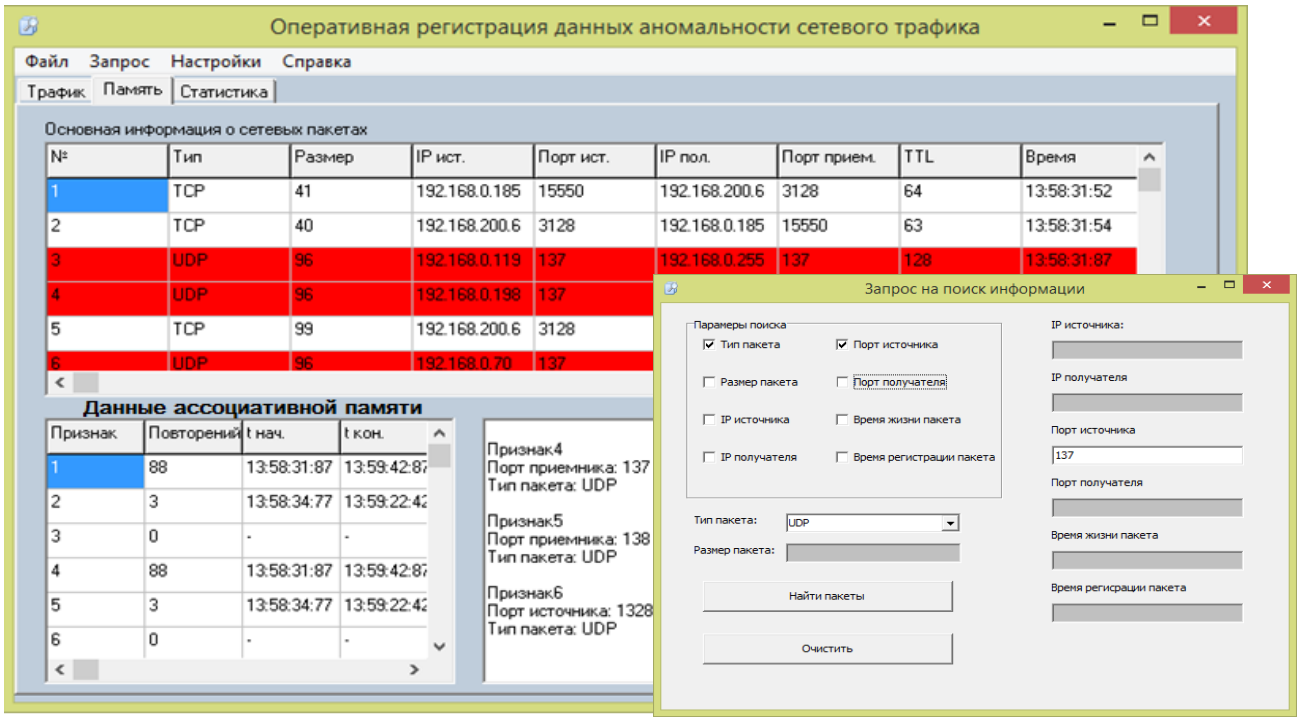


Рисунок 4.13 – Экранная форма поиска фрагментов данных о вирусной атаке

В качестве признаков для поиска использованы следующие условия: атака была осуществлена через приложение, использующие UDP порты 128, 138 и TCP порты 139, 445. На рисунке видно, что из общего объема сетевого трафика по данным признакам были выделены пакеты, непосредственно связанные с атакой.

Далее для установления причинно-следственных связей были построены возможные маршруты распространения вируса в КС. Для построения маршрутов были сгенерированы цепочки пакетов, связанных между собой по IP-адресам пересылки пакетов. Полученные маршруты представлены на рисунке 4.14.

№	Гипотеза
1	192.168.0.119‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163
2	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.119‖192.168.0.119‖192.168.0.163
3	192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.163
4	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.198
5	192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.185‖192.168.0.185‖192.168.0.1‖192.168.0.1‖192.168.0.163
6	192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.185‖192.168.0.185‖192.168.0.1‖192.168.0.1‖192.168.0.185
7	192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.185
8	192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.163
9	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1
10	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.163‖192.168.0.163‖192.168.0.198‖192.168.0.198‖192.168.0.163
11	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.163‖192.168.0.163‖192.168.0.119‖192.168.0.119‖192.168.0.163
12	192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163
13	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.119
14	192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.0.163
15	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.185
16	192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198
17	192.168.0.119‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198
18	192.168.0.119‖192.168.0.163‖192.168.0.163‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163
19	192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6
20	92.168.200.6‖192.168.0.185‖192.168.0.185‖192.168.0.1‖192.168.0.1‖192.168.0.163‖192.168.0.163‖192.168.0.198‖192.168.0.198‖192.168.0.163
21	192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.0.1
22	192.168.200.6‖192.168.0.185‖192.168.0.185‖192.168.0.1‖192.168.0.1‖192.168.0.163‖192.168.0.163‖192.168.0.119‖192.168.0.119‖192.168.0.163
23	192.168.0.1‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.70
24	192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163‖192.168.0.163‖192.168.0.1‖192.168.0.1‖192.168.0.185
25	192.168.0.1‖192.168.0.163‖192.168.0.163‖192.168.0.185‖192.168.0.185‖192.168.200.6‖192.168.200.6‖192.168.0.198‖192.168.0.198‖192.168.0.163

Рисунок 4.14 – Экранная форма построения маршрутов распространения вируса

В результате анализа маршрутов распространения вируса получена информация о зараженных узлах сети и сделан вывод о вероятных источниках распространения. Экранная форма анализа сведений об атаке и определения источника распространения вредоносной информации представлена рисунке 4.15.

Рисунок 4.15 – Экранная форма определения источника распространения вируса

Ранжированный список IP-адресов показал, что наиболее активным хостом сети (помимо proxy-сервера) при распространении вредоносной информации является компьютер с адресом 192.168.0.185, что характеризует его как вероятный первоначальный источник атаки.

4.3.3 Апробация метода определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС

В качестве исходных данных для моделирования инцидентов, связанных с потерей связи между подсистемами АСУ, использован сетевой трафик, зарегистрированный при физическом разрыве соединения между компьютерами, имитирующими диспетчера и ПЛК. Для выявления инцидента осуществлялся поиск сетевых пакетов, связанных с запросом на соединение, по следующим признакам: протокол – ARP, IP-адрес недоступного узла - 192.168.0.131, время отсутствия ответа – более 5 секунд. Результаты анализа трафика на предмет обнаружения обрыва линии связи, проведенного с помощью программы [11], представлены на рисунке 4.16.

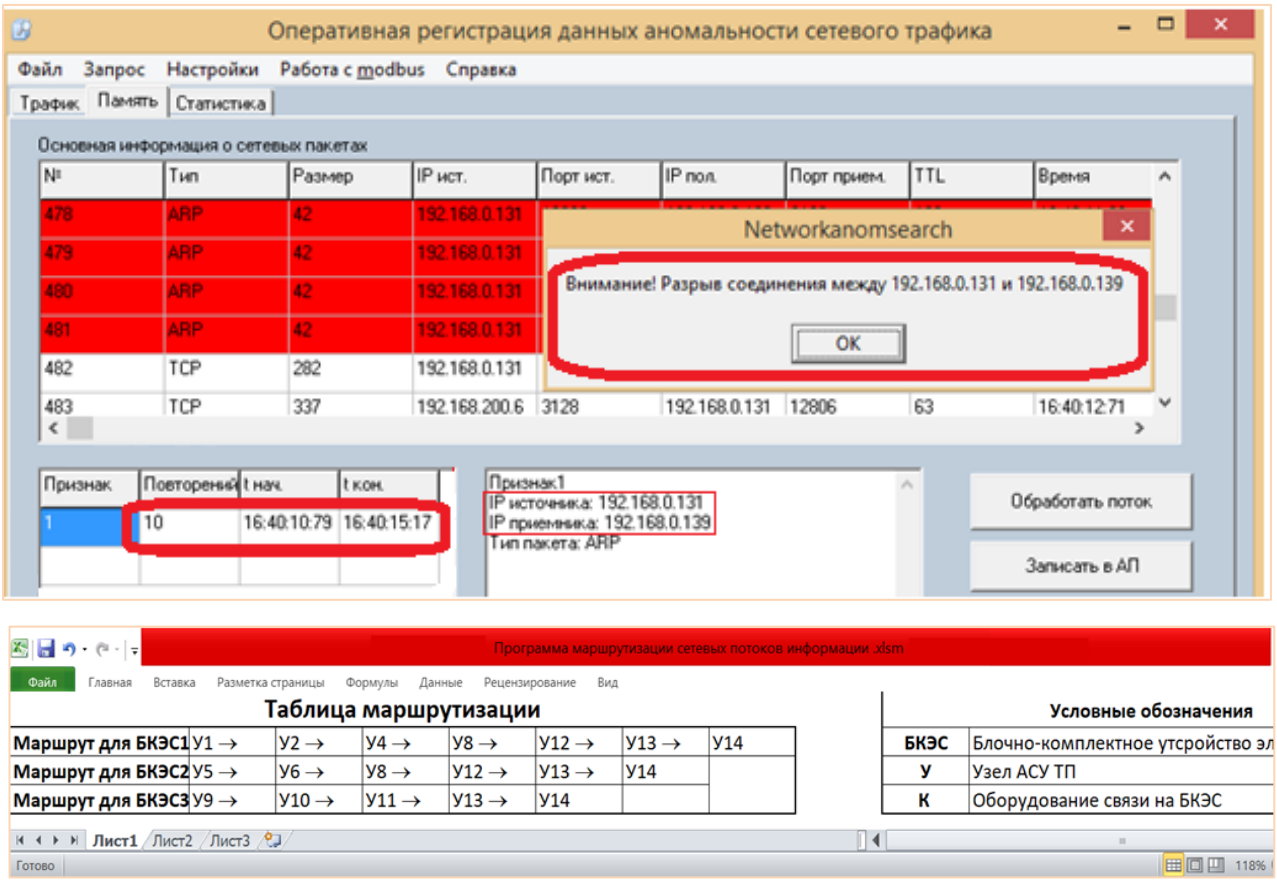


Рисунок 4.16 – Экранная форма обнаружения обрыва линии связи и определения резервного маршрута передач данных

Результатом работы программы является извещение сотрудника АСУ об отсутствии связи между узлом с адресом 192.168.0.131 и узлом 192.168.0.139 и рекомендуемые маршруты передачи данных.

4.3.4 Апробация метода мониторинга действий персонала в АС

Для апробации метода проведен эксперимент на модельных данных сетевого трафика сегмента информационно-управляющей подсистемы АСУ транспортировкой нефтегазового сырья, построенного с использованием:

- программного комплекса Scada Trace Mode, на базе которого разработана мнемосхема участка нефтепровода, имитирующая работу датчиков и исполнительного механизма;

- программ-эмуляторов промышленного протокола Modbus TCP (Modbus Pool и Modbus Slave) для моделирования работы контроллера и автоматизированного рабочего места оператора;
- программы мониторинга управляющих операций оператора АСУ [121].

В ходе моделирования с компьютера, имитирующего диспетчера на компьютер, имитирующей ПЛК посылалась команда на закрытие задвижки трубопровода. По завершении эксперимента проведен анализ данных трафика промышленной сети, содержащего сведения о нерегламентированной управляющей транзакции, представленные на рисунке 4.17.

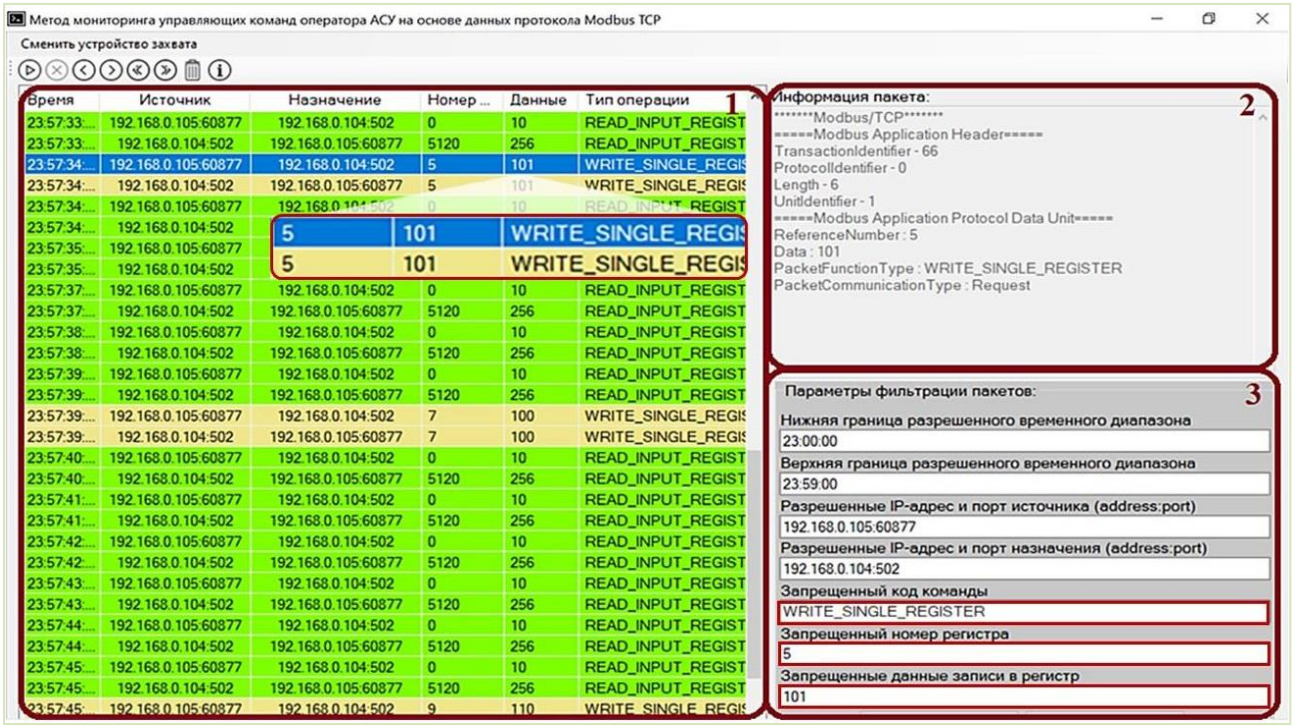


Рисунок 4.17 – Экранная форма обнаружения нерегламентированной управляющей транзакции персонала

Анализ результатных данных показал наличие последовательности операций, содержащих нерегламентированные значения, записываемые в регистры контроллера. В частности, зарегистрирована попытка записи данных «101» в регистр «5», запрещенных настройками безопасности в поле 3. В поле 2 выведены сведения о соответствующей операции, формирующие сигнатуру распознавания ее легитимности.

Проведенный эксперимент подтвердил работоспособность метода при работе с данными, приближенными к реальному промышленному трафику. Разработанное программное средство позволило оперативно обнаружить и предупредить неквалифицированные действия персонала.

Апробация результатов диссертационной работы показала, что в реальных условиях разработанные методы могут быть интегрированы в систему защиты информации в АСУ, работающую на базе типовых аппаратных и программных решений.

Результаты исследований, проведенных в ходе вычислительных и натурных экспериментов и апробации, позволили разработать рекомендации по применению методов обнаружения аномалий и нейтрализации угроз в распределенных АСУ с учетом требований отраслевых стандартов и нормативных документов в сфере информационной безопасности.

4.4 Разработка рекомендаций по внедрению результатов исследований

Как уже отмечалось, общая протяженность транспортных трубопроводов Оренбуржья составляет более 9000 км, что свидетельствует об актуальности использования результатов диссертационной работы на предприятиях и в организациях области, занимающихся нефте-газодобычей, транспортировкой и обработкой нефтегазового сырья.

Разработанные методы могут быть применены на различных этапах жизненного цикла систем защиты информации в распределенных АСУ ТП, в частности – их разработки, эксплуатации, внедрения и модернизации.

На рисунке 4.18 представлена схема взаимосвязей методов, средств и элементов декомпозиции процесса построения подсистем защиты информации с использованием результатов диссертационной работы.

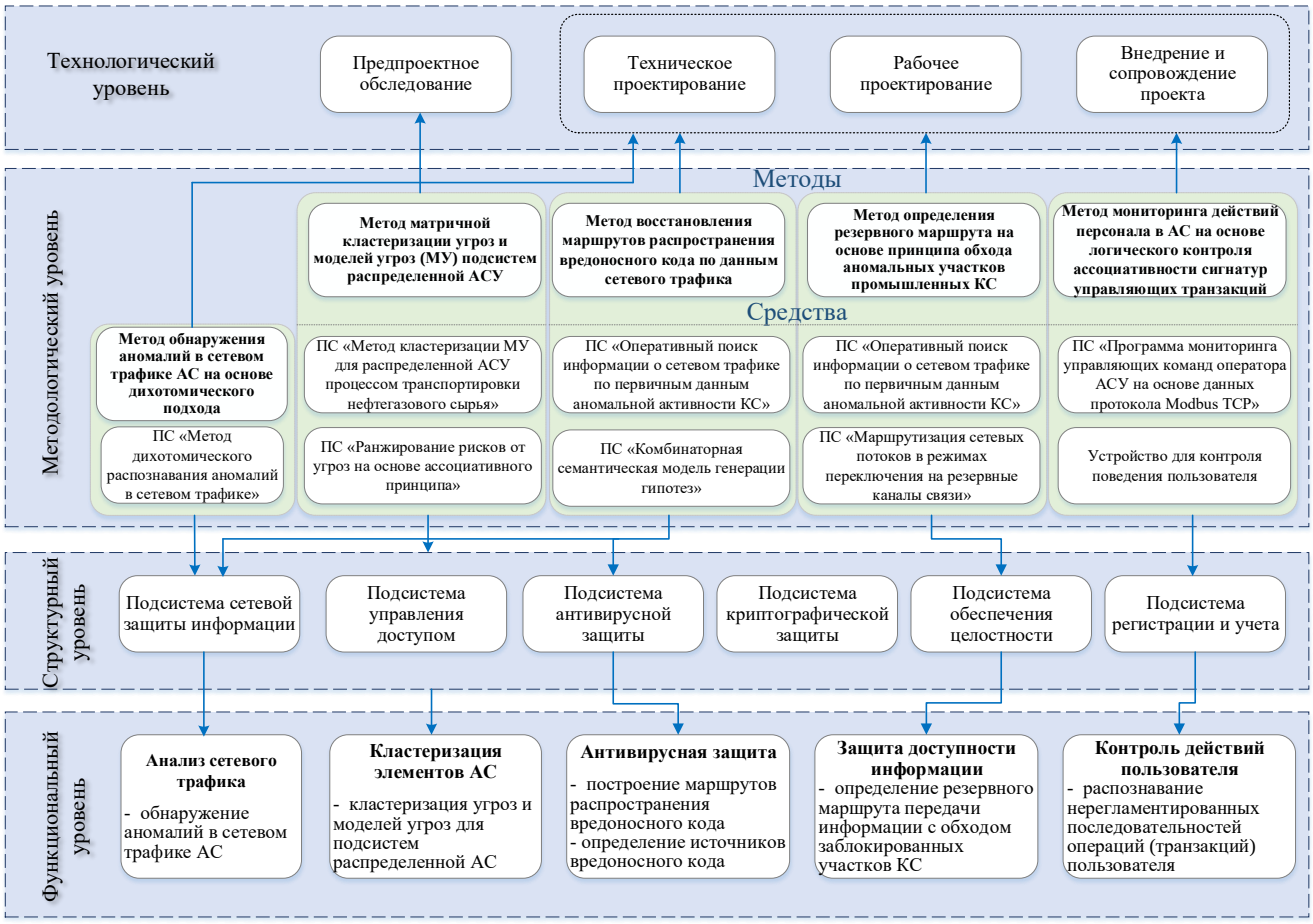


Рисунок 4.18 – Схема взаимосвязей методов, средств и элементов декомпозиции процесса построения подсистем защиты информации

Метод матричной кластеризации угроз и МУ предназначен для оценки степени актуальности угроз, приоритетности их нейтрализации и определения характера изменения угрозы на последовательности подсистем распределенной АСУ ТП на этапе предпроектного обследования, а так же при модернизации любой из подсистем СЗИ.

Метод обнаружения аномалий в сетевом трафике на основе дихотомического подхода позволяет повысить производительность и достоверность средств обнаружения и может быть использован как в составе подсистем антивирусной защиты информации, регистрации и учета действий персонала, обеспечения целостности и защиты доступности технологической информации, так и в подсистеме сетевой защиты информации.

Методики и методы восстановления маршрутов распространения вредоносного кода, определения резервного маршрута и мониторинга действий персонала АС применяются на этапах технического и рабочего проектирования, внедрения, сопровождения проектов и позволяют повысить функциональную полноту средств антивирусной защиты информации, учета действий персонала и защиты доступности технологической информации в составе СЗИ.

Разработанный комплекс программных средств может быть использован в центрах SOC, SIEM-системах и системах поддержки и принятия решений в подразделениях информационной безопасности на предприятиях нефтегазовой отрасли. На рисунке 4.19 представлена структурная схема модифицированной подсистемы мониторинга аномалий для исследуемой в работе АСУ транспортировкой нефтегазового сырья с использованием разработанных методов.

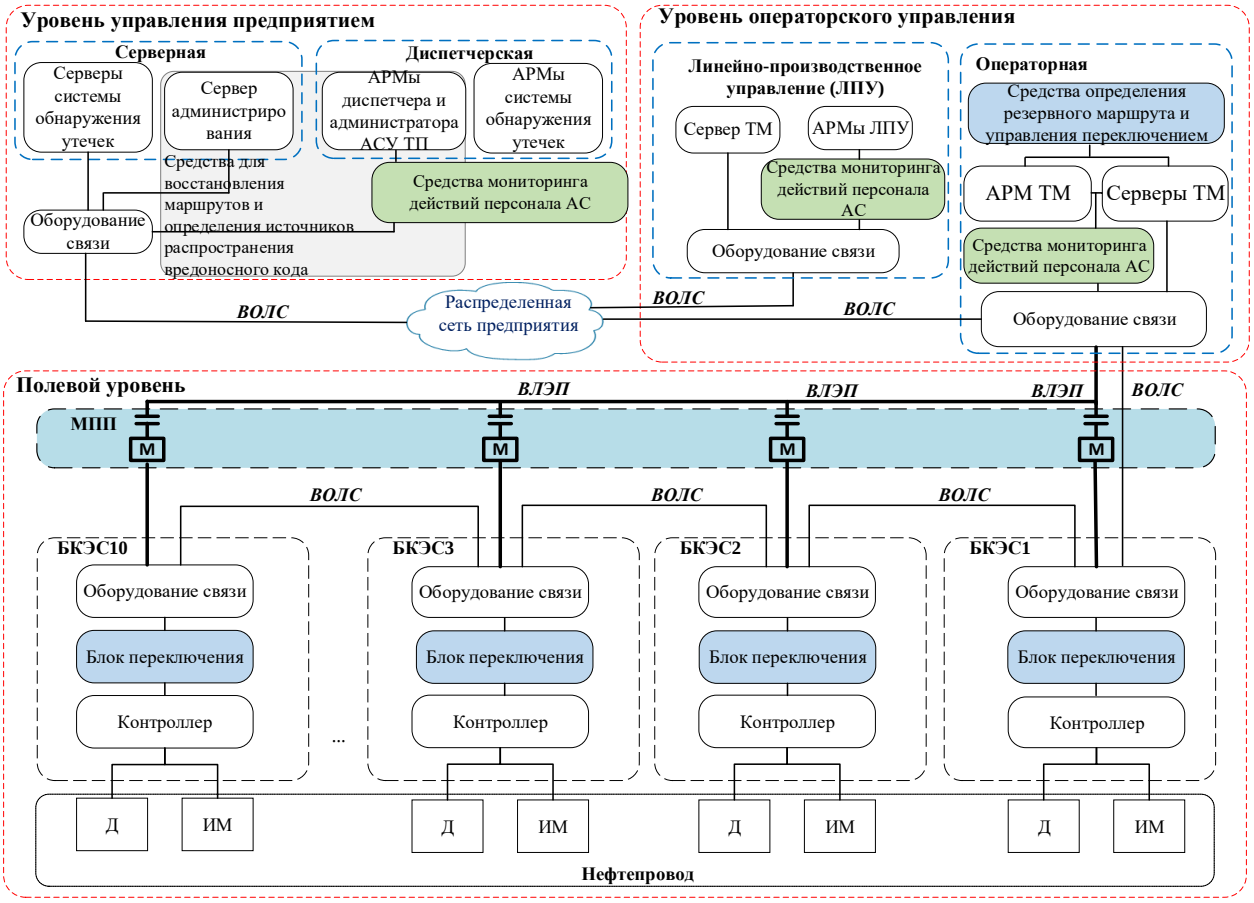


Рисунок 4.19 – Структурная схема модифицированной подсистемы обнаружения аномалий и нейтрализации угроз в распределенных АСУ ТП на основе мониторинга сетевых информационных потоков

Рекомендации по применению методов и программных средств для восстановления маршрутов распространения вредоносного кода, определения резервного маршрута и мониторинга действий персонала АС в подсистемы антивирусной и сетевой защиты информации, защиты доступности технологической информации и учета действий персонала соответственно представлены ниже.

4.4.1 Разработка рекомендаций по применению метода восстановления маршрутов распространения вредоносного кода в подсистемах антивирусной и сетевой защиты информации

Проблема распространения вредоносного кода актуальна для многих корпоративных промышленных сетей, в том числе, и для КС исследуемой в работе АСУ. Сетевой вирус распространяется через незакрытые уязвимости операционных систем, почтовые сообщения, открытые ресурсы общего пользования.

Для решения задач сетевой и антивирусной защиты в СЗИ рассматриваемого класса АСУ используются антивирусное средство Kaspersky endpoint security [191] от «Лаборатории Касперского» и программно-аппаратный комплекс DATAPK [187] от «УЦСБ».

Целью внедрения разработанного метода восстановления маршрутов распространения вредоносного кода является повышение функциональных возможностей подсистем антивирусной и сетевой защиты информации при сборе и анализе данных о вредоносной активности в АСУ. Блок определения и восстановления маршрутов распространения вредоносного кода является частью подсистем антивирусной и сетевой защиты включает:

- модуль сбора данных о зараженных компьютерах;
- модуль восстановления маршрутов и определения источников распространения вредоносного кода.

Модуль сбора данных предназначен для централизованного накопления сведений и формирования базы данных о зараженных компьютерах. Для решения данной задачи предлагается использование программы централизованного управ-

ления антивирусными средствами Kaspersky Administration Kit [190]. Данное средство устанавливается на сервер администрирования сети и позволяет осуществлять централизованный сбор и регистрацию событий о вирусной атаке с программ-клиентов, установленных на конечных узлах сети. Программа формирует отчет, содержащий информацию об основных инцидентах в сети:

- название зарегистрированного события;
- уровень важности события;
- описание события;
- IP-адрес и имя компьютера, на котором произошло событие;
- название и версия программы, в работе которой зафиксировано событие;
- название задачи, в результате действия которой возникло событие;
- дата и время возникновения события.

Алгоритм работы модуля сбора данных представлен на рисунке 4.20.

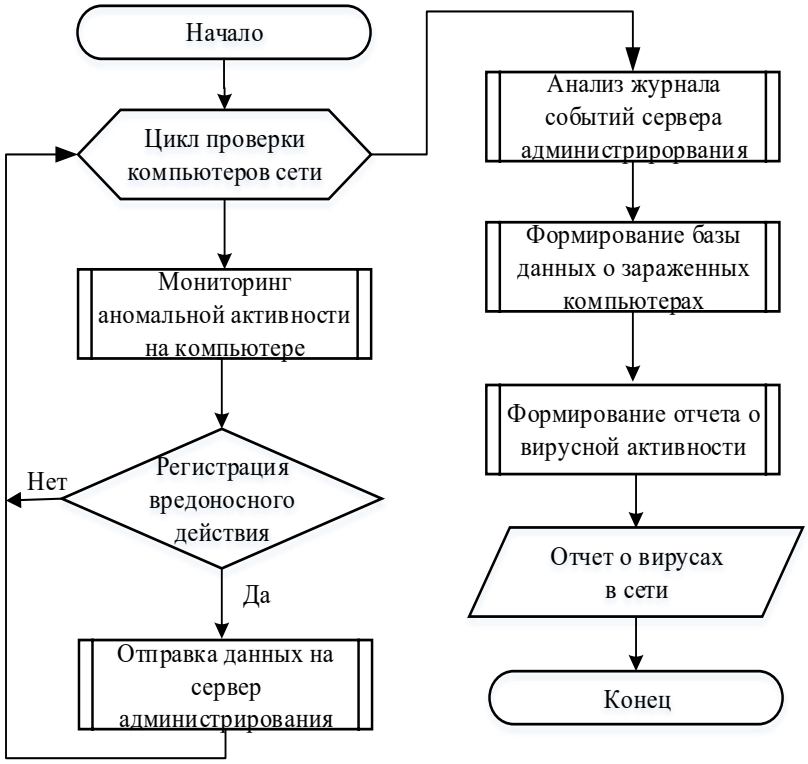
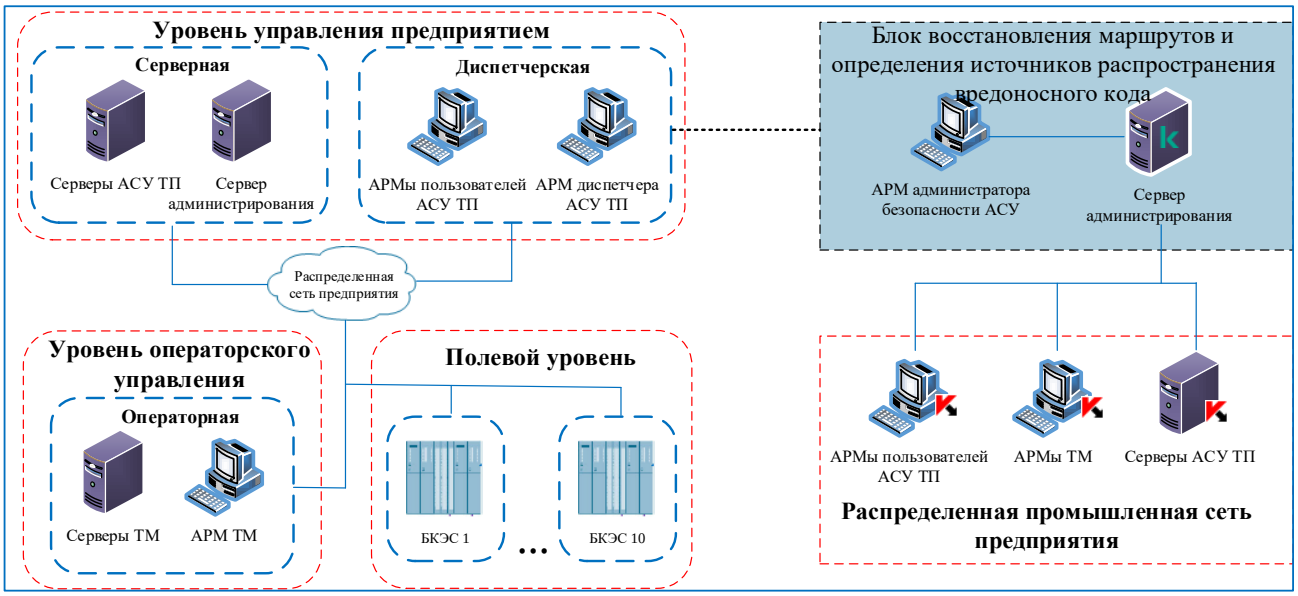


Рисунок 4.20 - Алгоритм сбора данных о зараженных компьютерах сети

Централизованный сбор данных на сервере администрирования позволяет получить первоначальную картину об адресах зараженных узлов сети, характере и времени заражения, что необходимо для дальнейшего анализа процесса распространения вредоносного кода. Особенность анализа сведений, полученных от антивируса, заключается в сложности построения полной картины распространения вируса и определения первоисточников атаки.

Модуль восстановления маршрутов и определения источников распространения вредоносного кода предназначен для оперативного построения маршрутов распространения вируса по отдельным фрагментам данных сетевого трафика. Модуль представляет собой разработанный программный комплекс [11, 13]. Структурная схема модифицированной подсистемы антивирусной защиты информации в АСУ при внедрении блока восстановления маршрутов и определения источников распространения вредоносного кода представлена на рисунке 4.21.



а) б)

Рисунок 4.21 – Структурная схема модифицированной АСУ при внедрении блока восстановления маршрутов и определения источников распространения вредоносного кода: (а) обобщенная схема АСУ транспортировкой нефтегазового сырья; (б) схема внедрения блока восстановления маршрутов и определения источников распространения вредоносного кода в подсистему антивирусной защиты информации

Программы для сбора данных устанавливаются на клиентские компьютеры КС уровня управления предприятием (АРМы пользователей, серверы АСУ) и сервер администрирования. Факт распространения вредоносного кода в сети фиксируется антивирусными средствами на конечных узлах. На сервере администрирования собирается вся информация о зараженных компьютерах.

Программы для восстановления маршрутов и определения источников распространения вредоносного кода устанавливаются на АРМ администратора безопасности АСУ на уровне управления предприятием и производит анализ данных о зараженных компьютерах, полученных с сервера администрирования, с целью выявления источников атаки и маршрутов распространения вредоносного кода. Подключение аппаратных решений на базе ассоциативных процессоров возможно через стандартные интерфейсы к оборудованию связи КС.

После восстановления маршрутов и определения источников распространения вируса диспетчеру (или администратору безопасности) выводится соответствующая информация, являющаяся основой для принятия решения по нейтрализации обнаруженной угрозы. В качестве мер по нейтрализации рекомендуется временная изоляция и восстановление работоспособности зараженных устройств, устранение уязвимостей, через которые была осуществлена атака.

Ввиду дополнительных затрат на реализацию метода, обусловленных повышением структурной сложности системы при добавлении ассоциативной памяти, рекомендуется использование метода в средних и больших сетях.

4.4.2 Разработка рекомендаций по применению метода определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС в подсистеме защиты доступности технологической информации

Целью применения метода является снижение риска потери технологической информации при ее передаче по каналам связи. В качестве исходного объекта для интеграции метода рассмотрена типовая система сбора и регистрации данных в АСУ, выполняющая функции подсистемы защиты доступности технологи-

ческой информации. В качестве метода интеграции – интеграция на функционально-прикладном и организационных уровнях [92].

Структурная схема типовой системы сбора и регистрации данных в АСУ приведена на рисунке 4.22. На рисунке приняты следующие условные обозначения:

- *БКЭС* – блочно-комплектные электростанции;
- *ВОЛС* – волоконно-оптические линии связи;
- *Д1 - Дm* – датчики;
- *Ethernet* – канал передачи данных по стандарту пакетной технологии, физическая среда передачи – витая пара;
- *RS 485* - канал передачи данных по стандарту физического уровня для асинхронного интерфейса, физическая среда передачи – витая пара;

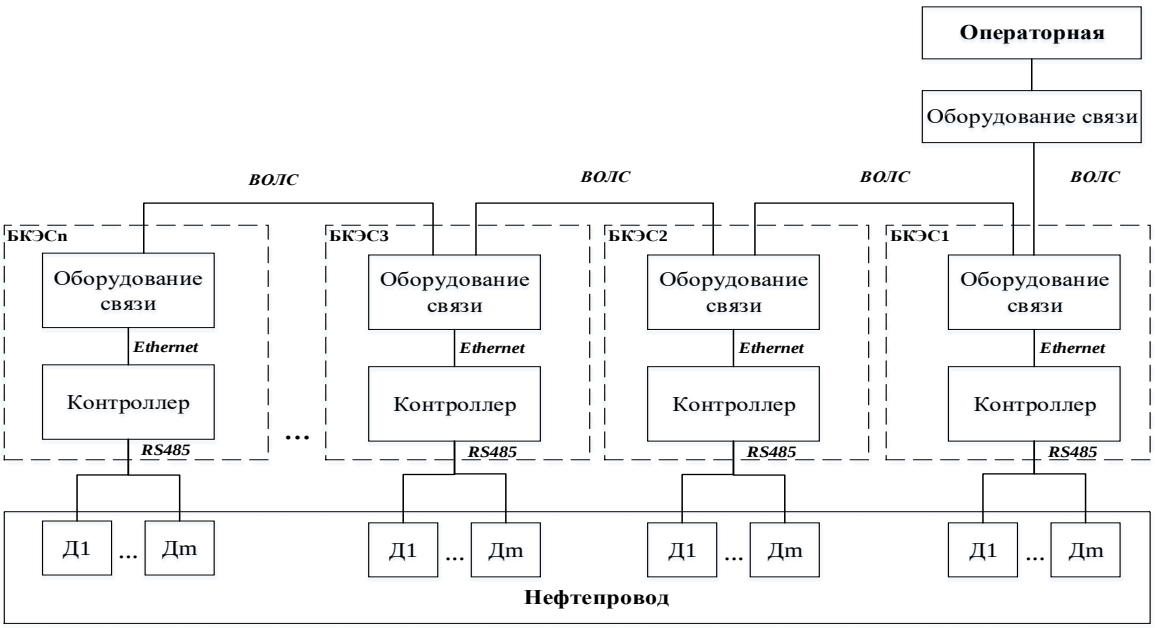


Рисунок 4.22 – Структурная схема типовой системы сбора и регистрации данных в АСУ

Источники информации - БКЭС, на которых установлено оборудование электропитания, средства собора информации о состоянии технологического объекта и оборудование связи. Источники передают данные по информационно-управляющему каналу ВОЛС оператору или диспетчеру АСУ. Подсистема сбора и регистрации данных работает в режиме мониторинга, производя периодическую

проверку связи со всеми участками АСУ. Обнаружение обрыва линии связи на объекте производится путем регистрации потери связи с контроллерами на БКЭС.

Для решения задач резервирования в исследуемой АСУ применяются технологии агрегирования каналов связи [106, 183], позволяющие объединить несколько физических каналов в один логический. Но подобный метод резервирования вносит дополнительную задержку при поднятии агрегированного канала и настройки передачи данных, что приводит к значительным задержкам при передаче данных о состоянии системы. Разработанный метод определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС позволяет снизить время передачи данных по резервному каналу за счет определения резервного маршрута за один цикл работы ассоциативного процессора.

Структурная схема модифицированной системы сбора и регистрации данных на объекте с резервным каналом связи представлена на рисунке 4.23, где *МПП* – модуль приема-передачи, *М* – модем.

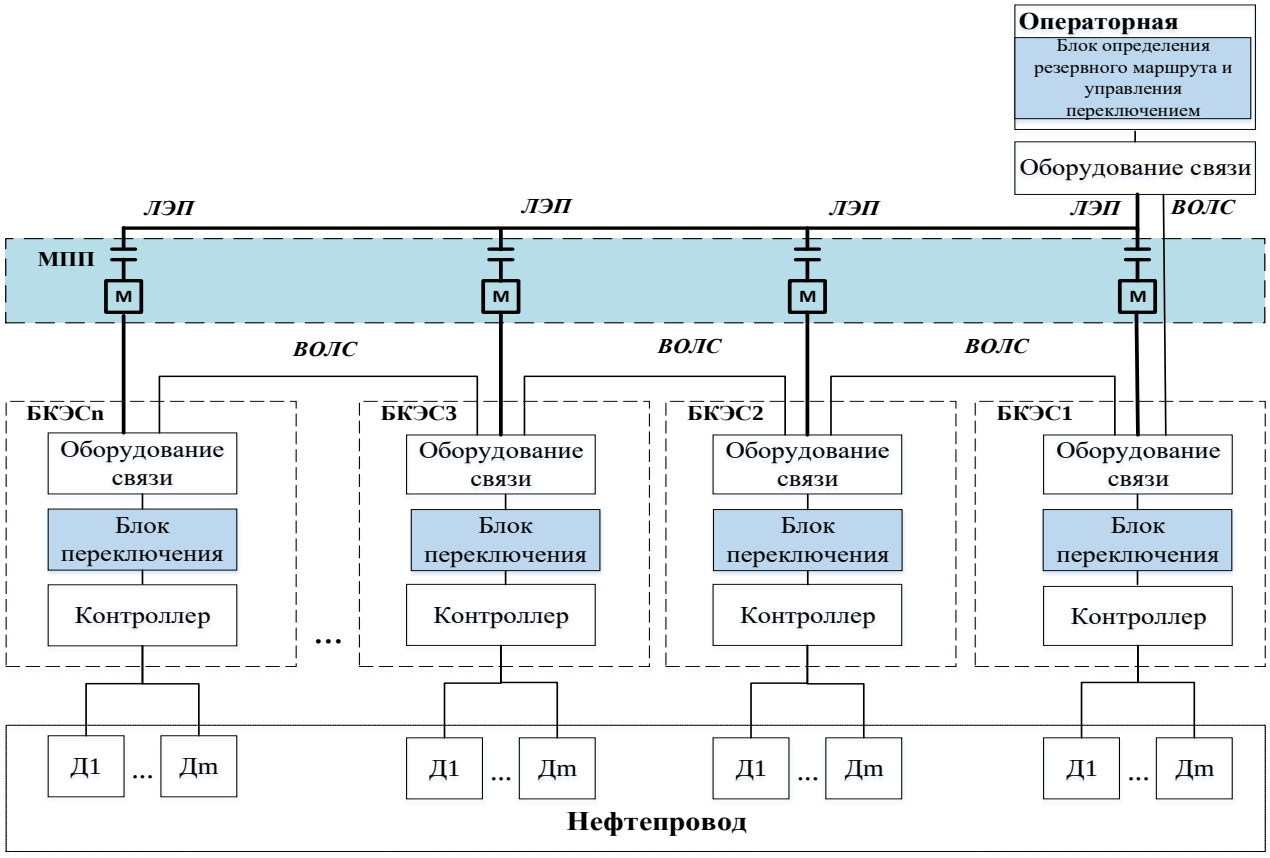


Рисунок 4.23 – Структурная схема модифицированной системы сбора и регистрации данных на объекте с резервным каналом связи

Для обеспечения надежности передачи данных основной канал ВОЛС дублируется посредством добавления резервного канала с использованием ВЛЭП. Подсистема защиты доступности технологической информации является частью подсистемы сбора и регистрации данных и состоит из следующих блоков.

1. Блока управления переключением, устанавливаемого в операторной и включающего:

- средство обнаружения нарушения целостности линии связи: в качестве такого средства может быть использована штатная система состояния мониторинга трубопровода, либо разработанное автором программное средство [11];
- разработанное автором программное средство маршрутизации сетевых потоков в режимах переключения на резервные каналы связи [5], либо устройство для определения резервного маршрута на базе ассоциативного процессора, представленного в разделе 3.4;
- утилиты удаленного администрирования сетевого оборудования связи (например, CISCO ACS), осуществляющие рассылку таблиц маршрутизации на каждый из отрезанных участков системы по резервному каналу.

2. Блока переключения на каждом участке АСУ в коммутационных шкафах БКЭС, реализуемого на базе используемого сетевого оборудования.

В случае обнаружения обрыва линии связи блок управления переключением осуществляет оперативное определение резервных маршрутов для каждого из недоступных источников информации с обходом заблокированных участков КС и передает их на соответствующие блоки переключения. Помимо маршрутов по резервному каналу связи подается управляющий сигнал, инициирующий обновление таблиц адресов коммутаторов в соответствии с полученным набором маршрутов на оборудовании связи диспетчера и каждой из БКЭС. На оборудовании связи БКЭС производится переключение всех источников, оказавших недоступными по основному каналу связи, на порты с подключенным резервным каналом.

Для обеспечения передачи данных сетевого трафика по ВЛЭП рекомендуется использовании технологии PowerLine [118]. Данная технология передает сетевую информацию путем наложения высокочастотного аналогового сигнала по-

верх стандартного переменного тока. Для организации связи система дополняется модулем приема-передачи информации по ВЛЭП.

Для подключения оборудования связи к ВЛЭП используется конденсатор связи. Для преобразования трафика Ethernet в трафик PowerLine на каждом из БКЭС и оборудовании связи диспетчера устанавливаются специализированные модемы ***M***. В работах [118, 125] представлена спецификация программного и аппаратного обеспечения, необходимого для организации резервного канала передачи информации по ВЛЭП. Вопросы построения и модернизации высокочастотных систем связи для рассматриваемых сетей подробно рассмотрены в работах [91, 118, 125, 152].

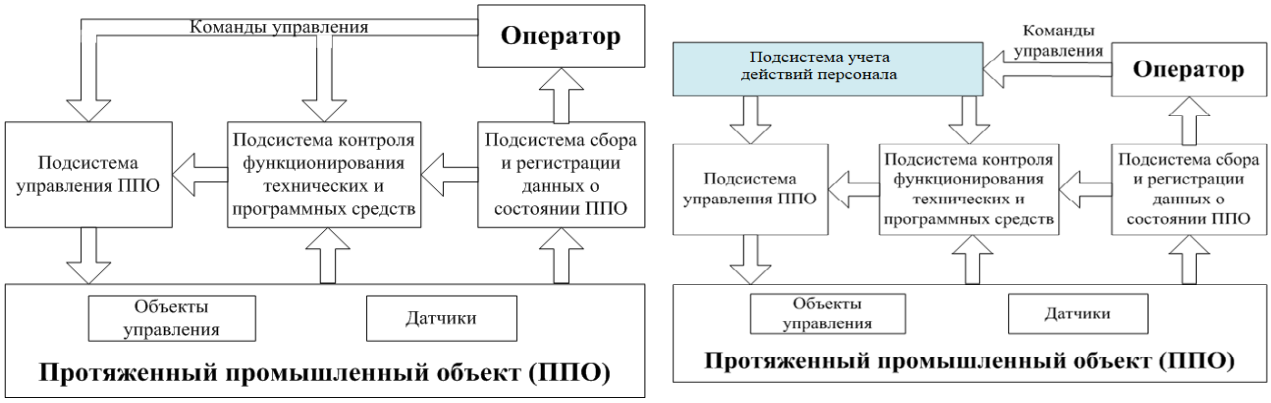
Для минимизации потерь при передаче критически важной информации о состоянии технологического объекта по ЛЭП при блокировании более 4 участков АСУ рекомендуется использование механизма управления очередями для приёмо-передающего оборудования резервного канала при дефиците пропускной способности. Механизм управления очередями подробно описан в работе [45].

При интеграции в существующую систему АС МТС разработанный метод позволит повысить надежность передачи информации о состоянии технологического объекта.

4.4.3 Разработка рекомендаций по применению метода мониторинга действий персонала в АС в подсистеме регистрации и учета действий персонала

Анализ типовой СЗИ, характерной для исследуемого класса АСУ, подтвердил актуальность мониторинга управляющих операций персонала системы, как взаимосвязанной последовательности образов (транзакции), а также его обучения по выполнению требуемой последовательности операций.

На рисунке 4.24 представлен пример применения разработанного метода для регистрации и учета действий персонала на примере подсистемы операторского управления.



(а) (б)

Рисунок 4.24 - Структурные схемы базовой (а) и модифицированной (б) подсистем операторского управления технологическим процессом

Внедрение метода мониторинга действий персонала в АС подразумевает установку разработанного программного обеспечения [20] на автоматизированных рабочих местах специалистов по ИБ и подключения устройства для контроля поведения пользователя [143] к сетевому оборудованию информационно-управляющей подсистемы, как показано на рисунке 4.19. При наличии несоответствия последовательности команд пользователя заданным политикам безопасности устройство в режиме контроля останавливает выполнение текущей команды, в режиме анализа определяет корректность всех команд транзакции и в режиме обучения представляет пользователю корректную последовательность команд.

Разработанный метод рекомендуется использовать как часть подсистемы регистрации и учета действий персонала в составе СЗИ АСУ для контроля управляющих транзакций, а также для обучения персонала.

4.5 Выводы по четвертой главе

Вычислительные эксперименты по исследованию методов обнаружения аномальных состояний сетевого трафика на базе нейронной сети, обученной по алгоритму Resilient Propagation, и мажоритарной функции с использованием экспериментальных и реальных временных рядов сетевого трафика показали, что при одинаковой достоверности функция мажоритарного вида обеспечивает на поря-

док выше оперативность обнаружения за счет меньшего числа применяемых информативных признаков.

Анализ результатов экспериментальной оценки эффекта от применения разработанных методов показал: снижение риска от угрозы распространения вредоносного кода в КС не менее чем на 80 тыс. рублей за счет оперативного обнаружения источников и исключения возможности дальнейшего распространения вредоносного кода в КС; снижение риска потери информации о состоянии объекта защиты не менее чем на 14% за счет использования принципов горячего резервирования и оперативного определения резервного маршрута передачи данных; снижение риска от угрозы несанкционированных действий персонала АСУ не менее чем в 2 раза за счет контроля последовательности и очередности подачи управляющих команд. При одинаковых функциональных и технических характеристиках суммарные затраты на разработку программных средств для реализации трех методов значительно ниже стоимости коммерческих аналогов.

Апробация разработанных методов и средств, проведенная в условиях лабораторного эксперимента с использованием сетевого стенда лаборатории кафедры ВТиЗИ Оренбургского государственного университета, программного комплекса SCADA TRACE MODE и эмуляторов промышленного сетевого протокола ModBus TCP, показала возможность интеграции результатов диссертационной работы в реальную СЗИ в АСУ промышленными объектами.

В результате апробации разработаны рекомендации по применению результатов диссертационной работы в СЗИ на предприятиях нефтегазовой отрасли.

Достоверность использования результатов подтверждена свидетельствами о регистрации программных средств, патентом на изобретение, актами о внедрении в ООО «Уральский центр систем безопасности», ООО «Газпромнефть-Оренбург», в учебный процесс ФГБОУ ВО «Оренбургский государственный университет» [22, 51], АНО ДО «Просвещение» (г. Оренбург). Акты о внедрении результатов диссертационной работы представлены в приложении А.

ЗАКЛЮЧЕНИЕ

1. В результате анализа современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой разработана концепция снижения риска ИБ за счет высокопроизводительных методов и средств оперативного и достоверного обнаружения, распознавания аномальных состояний АСУ, как проявлений инцидентов ИБ, нейтрализации связанных с ними угроз на основе исследования и интеллектуальной обработки данных сетевого трафика.

2. Разработан метод матричной кластеризации угроз и моделей угроз на основе статистической обработки значений рисков, позволивший определить характер изменения угрозы на последовательности подсистем распределенной АСУ ТП, оценить степень актуальности угроз и приоритетности их нейтрализации, в частности, необходимость совершенствования средств защиты в задачах определения источников и восстановления маршрутов распространения вредоносного кода, определения резервных маршрутов передачи данных для нейтрализации блокировки доступа к источникам информации, мониторинга действий персонала в распределенных АС.

3. Предложен метод построения математических и имитационных моделей и разработаны модели для обнаружения аномалий и распознавания состояния КС АСУ на основе данных мониторинга сетевого трафика, позволяющие повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз. Сопоставительный анализ показал, что разработанные модели по достоверности не уступают аналогичными, в частности, нейросетевым, при этом обладают большей оперативностью и меньшей вычислительной сложностью на этапе распознавания образа не менее чем на порядок.

4. Разработаны алгоритмы, методики и программно-аппаратная реализация методов и средств: восстановления маршрутов распространения вредоносного кода по данным сетевого трафика, позволяющие оперативно выявлять маршруты и источники распространения вредоносной информации в КС и принимать превентивные меры по нейтрализации угрозы дальнейшего распространения; определе-

ния резервного маршрута с обходом аномальных участков промышленных КС, позволяющие снизить риски от угроз потери информации о состоянии объекта защиты при ее передаче по каналам связи распределенной АСУ и повысить оперативность реагирования на возникновение аварийной ситуации; мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций, позволяющие снизить риски от угроз нерегламентированных управляющих воздействий на систему.

5. Анализ результатов экспериментальной оценки эффекта от использования разработанных методов показал: увеличение оперативности поиска данных о распространении вредоносной информации в СТ не менее чем в 2 раза за счет принципов ассоциативности, что позволяет снизить риски от угрозы распространения вредоносного кода в КС; снижение риска потери информации о состоянии объекта защиты не менее чем на 14% за счет использования принципов горячего резервирования и оперативного определения резервного маршрута передачи данных; снижение риска от угрозы несанкционированных действий персонала АСУ не менее чем в 2 раза за счет контроля последовательности и очередности подачи управляющих команд. Даны рекомендации по практическому применению результатов диссертационной работы в СЗИ на предприятиях нефтегазовой отрасли.

Перспективы дальнейшей разработки темы. В рамках дальнейших исследований планируется рассмотреть возможности совершенствования разработанных методов и средств на основе нейронных сетей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Абдулин, А.А. Исследование программных решений для обеспечения информационной безопасности промышленных сетей автоматизированных систем управления технологическими процессами / А. А. Абдулин, А. Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 1(39). – С. 43-53.

2. Абрамова Т.В. Многоаспектный анализ частных решений в задаче защиты информации на основе мониторинга сетевого трафика/ Т.В. Абрамова // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 1(51). – С. 30–38.

3. Абрамова Т.В. Научно-исследовательский сетевой стенд как многофункциональный комплекс средств изучения сетевых методов защиты информации/ Т.В. Абрамова, Т.З. Аралбаев, Е.В. Каменева, Ю.И. Синицын // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всероссийской научно-методической конференции; Оренбург: ОГУ, 2018.− С. 1719–1725.

4. Абрамова Т.В. Обнаружение сетевых аномалий на основе дихотомической модели распознавания образов/Т.В. Абрамова, Е.Г. Александров, Т.З. Аралбаев// Технологические инновации и научные открытия/Сборник научных статей по материалам XII Международной научно-практической конференции / В 2 ч. Ч.1 – Уфа: Изд. НИЦ Вестник науки, 2023. – с. 54 – 62

5. Абрамова Т.В. Применение макросов табличного процессора в задаче исследования имитационной модели маршрутизации сетевых потоков/ Т.В. Абрамова, Т.З. Аралбаев// Университетский комплекс как региональный центр образования, науки и культуры: материалов Всероссийской научно-методической конференции; Оренбург: ОГУ, 2020. – с. 1389 – 1395.

6. Абрамова Т.В. Применение методологии IDEF0 в задаче изучения процесса разработки модели угроз информационной безопасности/ Т.В. Абрамова // Университетский комплекс как региональный центр образования, науки и культу-

ры: материалов Всероссийской научно-методической конференции; Оренбург: ОГУ, 2022. – с. 1245 – 1250.

7. Абрамова Т.В. Распознавание сценария развития аномальной ситуации в распределенных управляющих системах на основе ассоциативно-мажоритарного подхода // Science in the modern information society XIX: Proceedings of the Conference. North Charleston, 28-29.05.2019, Vol. 1 —Morrisville, NC, USA: Lulu Press, 2019, p. 80-81 p.

8. Абрамова Т.В., Аралбаев Т.З. Прикладная программа «Метод кластеризации моделей угроз для распределенной АСУ процессом транспортировки нефтегазового сырья». Свидетельство о регистрации электронного ресурса. Рег. № 2022. Дата регистрации: 18.11.2019. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

9. Абрамова Т.В., Аралбаев Т.З., Галимов Р.Р., Каменева А.В. Программное средство «Ранжирование рисков от угроз на основе ассоциативного принципа». Свидетельство о регистрации электронного ресурса. Рег. № 1646. Дата регистрации: 01.10.2018. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

10. Абрамова Т.В., Аралбаев Т.З., Галимов Р.Р., Программный комплекс «Моделирование сетевого трафика на базе протокола TCP/ModBUS». Свидетельство о регистрации электронного ресурса. Рег. № 1657. Дата регистрации: 10.11.2018. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

11. Абрамова Т.В., Аралбаев Т.З., Прикладная программа «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности компьютерной сети». Свидетельство о регистрации электронного ресурса. Рег. № 1109. Дата регистрации: 20.05.2015. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

12. Абрамова Т.В., Аралбаев Т.З., Прикладная программа «Синергетическая имитационная модель сетевых атак на ресурсы вычислительных систем». Свидетельство о регистрации электронного ресурса. Рег. № 970. Дата регистрации:

03.06.2014. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

13. Абрамова Т.В., Галимов Р.Р., Аралбаев Т.З. Прикладная программа «Комбинаторная семантическая модель генерации гипотез». Свидетельство о регистрации электронного ресурса. Рег. № 1236. Дата регистрации: 29.03.2016. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

14. Абрамова, Т.В. Исследование эффективности метода оперативного поиска информации о сетевом трафике на основе ассоциативного принципа / Т.В. Абрамова, Т.З. Аралбаев // Компьютерная интеграция производства и ИПИ-технологии: материалы VII Всероссийской научно-практической конференции. – Оренбург, 2015. – С. 235-239.

15. Абрамова, Т.В. Метод оперативного прогнозирования и ранжирования рисков информационной безопасности на основе ассоциативного подхода/ Т.В. Абрамова, Т.З. Аралбаев, Г.Г. Аралбаева, Р.Р. Галимов // Вопросы развития современной науки и практики в период становления цифровой экономики: Материалы международной научно-практической конференции (18 октября 2018 г.). – Санкт-Петербург: Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова. 2018. - С. 9-11.

16. Абрамова, Т.В. Моделирование аномалий в информационной системе мониторинга состояния нефтепровода по данным сетевого трафика/ Т.В. Абрамова, Т.З.Аралбаев, Р.Р. Галимов, А.В. Манжосов, М.Д. Хатеев // Безопасность: Информация, Техника, Управление: Материалы международной научной конференции. – Санкт-Петербург: ГНИИ «НАЦРАЗВИТИЕ». 2018. – С. 127-130.

17. Абрамова, Т.В. Моделирование процессов защиты передачи технологической информации по резервному каналу на основе анализа сетевого трафика / Т.В. Абрамова, Т.З. Аралбаев, А.В. Манжосов // Инновационные, информационные и коммуникационные технологии. – 2019. – № 1. – С. 246-251.

18. Абрамова, Т.В. Моделирование сетевых атак на ресурсы вычислительных систем с использованием принципов самоорганизации / Т. В. Абрамова, Т. З.

Аралбаев // Современные информационные технологии в науке, образовании и практике: Материалы XI Всероссийской научно-практической конференции, Оренбург, 11–13 ноября 2014 года / Оренбургский государственный университет. – Оренбург: ООО ИПК Университет, 2014. – С. 109-114.

19. Абрамова, Т.В. Модель контроля транзакций пользователя АСУ ТП на основе сигнатурного принципа/Т.В. Абрамова, Т.З. Аралбаев, //«Инновационные, информационные и коммуникационные технологии: сборник трудов XVI международной научно-практической конференции; Сочи. - 2020. – с. 181 - 185.

20. Абрамова, Т.В. Модифицированная имитационная модель контроля управляющих действий персонала на основе данных сетевого трафика / Т.В. Абрамова, Т.З. Аралбаев, И.Д. Зайчиков // Защита информации. Инсайд, 2022. - № 6 (108). - С. 32-35.

21. Абрамова, Т.В. Номограммный метод анализа эффективности ассоциативно - последовательного подхода в задаче распознавания сценария вирусной атаки / Т. В. Абрамова // ОБЩЕСТВО - НАУКА - ИННОВАЦИИ: сборник статей Международной научно-практической конференции, Калуга, 17 февраля 2021 года. – Уфа: ОМЕГА САЙНС, 2021. – С. 30-39.

22. Абрамова, Т.В. Основы информационной безопасности (09.03.01 очн.): электронный учебный курс в системе Moodle / Т.В. Абрамова; Оренбург. гос. ун-т. - Оренбург: ОГУ, 2023. - 9 с.

23. Абрамова, Т.В. Разработка и исследование метода анализа сетевого трафика на основе ситуационно-ассоциативного подхода с мажоритарным принципом принятия решения: выпускная квалификационная работа: направление подготовки (специальность) 09.04.01 Информатика и вычислительная техника / Т.В. Абрамова. - Оренбург. - 2017. - 161 с.

24. Абрамова, Т.В., Моделирование аномалий в информационной системе мониторинга состояния нефтепровода по данным сетевого трафика / Т. В. Абрамова, Т. З. Аралбаев, Р. Р. Галимов [и др.] // Сборник избранных статей по материалам научных конференций ГНИИ "Нацразвитие", Санкт-Петербург, 27–31.10. 2018 года. Том 1. – Санкт-Петербург: ГНИИ «Нацразвитие», 2018. – С. 127-130.

25. Абрамова, Т.В., Аралбаев, Т.З. Анализ пространственно-временной модели угроз для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья. Вестник УГАТУ, n. 1 (87), p. 76-84.

26. Агеев С.А., Саенко И.Б., Котенко И.В. Методы и алгоритмы обнаружения аномалий в трафике мультисервисных сетей связи, основанные на нечётком логическом выводе//Информационно-управляющие системы. 2019. № 3. С. 61.

27. Ажмухамедов И.М., Марьенков А.Н. Поиск и оценка аномалий сетевого трафика на основе циклического анализа // ИВД. 2012. №2. URL: https://cyberleninka.ru/article/n/poisk-i-otsenka-anomaliy-setevogo-trafika-na-osnove-tsiklicheskogo-analiza (дата обращения: 05.01.2022).

28. Алгоритм обучения RProp — математический аппарат [Электронный ресурс]. – URL: https://basegroup.ru/community/articles/rprop (дата обращения 31.03.2023)

29. Аналитическая служба компании «Код безопасности» [Эл. ресурс]. / Российский разработчик программных и аппаратных средств защиты информации. 2008-2018 «Код Безопасности». – Режим доступа: https://www.securitycode.ru/documents/analytics/. - 12.03.2021.

30. Аномалия [Электронный ресурс]: Википедия. Свободная энциклопедия. – Режим доступа: https://ru.wikipedia.org/wiki/Аномалия (дата обращения: 06.11.2022)

31. Анохин, А.Н. Сбор данных о надежности выполнения управляющих действий оператором АСУ ТП/ А.Н. Анохин, Р.И. Машковцева, Ю.Н. Анохин, А.Ю. Захаркив / Обнинск: Обнинский институт атомной энергетики Национального исследовательского ядерного университета «МИФИ». – 2016. – С. 141-146.

32. Антонов А.П., Заборовский В.С., Полянский В.А. Нейровычисления в задачах управления: аспекты вычислимости и пространственно-временной характеризации когнитивных функций// Информационные технологии в управлении. Материалы конференции. Санкт-Петербург, 2020. С. 165-168

33. Аралбаев Т.З. Геоинформационное взаимодействие мобильных средств в задаче мониторинга распределенных промышленных объектов [Электронный

ресурс] / Т.З. Аралбаев, Т.В. Абрамова, Р.Р. Галимов, А.И. Сарайкин // Прогрессивные технологии в транспортных системах : материалы XVII междунар. науч.-практ. конф., Оренбург, 17-18 янв. 2022 г. / отв. ред. В. И. Рассоха. - Оренбург: ОГУ,2022. - . - С. 5-13.

34. Аралбаев Т.З. Кластерный анализ как инструмент построения и исследования пространственно-временных моделей угроз/ Т.З. Аралбаев, Т.В. Абрамова, М.А. Гетьман// Университетский комплекс как региональный центр образования, науки и культуры: материалов Всероссийской научно-методической конференции; Оренбург: ОГУ, 2020. – с. 1401 – 1404.

35. Аралбаев Т.З. Применение макросов табличного процессора в задаче изучения имитационной модели мониторинга перемещения мобильного объекта в трехмерном пространстве/ Т.З. Аралбаев, Р.Р. Галимов, Е.В. Каменева, Т.В. Абрамова, Е.Ю. Захаров// Университетский комплекс как региональный центр образования, науки и культуры: материалов Всероссийской научно-методической конференции; Оренбург: ОГУ, 2019. – с. 1813 - 1820.

36. Аралбаев Т.З. Сопоставительный анализ методов реализации дихотомического разделения состояний сетевого трафика на основе мажоритарной и нейросетевой моделей/ Т.З. Аралбаев, Т.В. Абрамова, Е.Г. Александров // Fundamental science and technology / Сборник научных статей по материалам XII Международной научно-практической конференции (14 апреля 2023 г., г. Уфа). / В 3 ч. Ч.1 – Уфа: Изд. НИЦ Вестник науки, 2023. – с. 137 – 147.

37. Аралбаев Т.З., Абрамова Т.В., Александров Е. Г. Прикладная программа «Метод дихотомического распознавания аномалий в сетевом трафике». Свидетельство о регистрации электронного ресурса. Рег. № 4023. Дата регистрации: 10.04.2023. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

38. Аралбаев Т.З., Александров Е.Г. Анализ ситуационно-признакового пространства на основе дихотомической модели в задаче распознавания образов по данным сетевого трафика // Университетский комплекс как региональный

центр образования, науки и культуры: сборник статей конференции. — ОГУ, 2023. — С. 287-302.

39. Аралбаев Т.З., Галимов Р.Р., Абрамова Т.В. Прикладная программа «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа». Свидетельство о регистрации электронного ресурса. Рег. № 1972. Дата регистрации: 24.09.2019. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

40. Аралбаев, Т.З. Выбор базовой функции при автоматизированной идентификации временных рядов на основе ассоциативно-мажоритарного подхода / Т.З. Аралбаев, Т.В. Абрамова, Р.Р. Галимов, Д.А. Гайфулина, Э.Р. Хакимова// Вестник Ижевского государственного технического университета имени М.Т. Калашникова. – 2018. – Т. 21. – № 4. – с. 194 – 199.

41. Аралбаев, Т.З. Исследование эффективности методов мониторинга сетевого трафика на основе последовательного и ассоциативно последовательного принципов поиска актуальной информации/ Т.З. Аралбаев, Т.В. Абрамова // СТИН. – 2017. – № 11. – С. 2-5.

42. Аралбаев, Т.З. Комбинаторная семантическая модель генерации гипотез / Т.З.Аралбаев, Т.В. Абрамова, Р.Р. Галимов // Информация и безопасность: научный журнал. – 2016. – Т. 19. – №. 3. – С. 379-384.

43. Аралбаев, Т.З. Контроль пользователя в АСУ ТП на основе принципов ассоциативности и мажоритарности / Аралбаев Т.З., Абрамова Т.В. // Актуальные задачи фундаментальных и прикладных исследований : материалы Междунар. науч.-практ. конф., 20 нояб. 2018 г., Оренбург / М-во образования и науки Рос. Федер., Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбургский гос. ун-т". - Оренбург : ОГУ,2018. - . - С. 37-40.

44. Аралбаев, Т.З. Концепция оптимизации системы контроля технического состояния распределенных автоматизированных систем на основе мониторинга сетевых информационных потоков / Аралбаев Т.З., Абрамова Т.В. // Актуальные задачи фундаментальных и прикладных исследований : материалы Междунар. науч.-практ. конф., 20 нояб. 2018 г., Оренбург / М-во образования и науки

Рос. Федер., Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбургский гос. ун-т". - Оренбург: ОГУ,2018. - . - С. 40-46.

45. Аралбаев, Т.З. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография /Т.З. Аралбаев, Г.Г. Аралбаева, Т.В. Абрамова, Р.Р. Галимов, А.В. Манжосов; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2018. -160 с. ISBN – 978-5-7410-2202-3 2.

46. Аралбаев, Т.З. Особенности оперативного поиска информации о сетевом трафике по первичным данным аномальной активности компьютерной сети / Т.З. Аралбаев, Т. В. Абрамова // Информационная безопасность 2015: сб. материалов XIV международной научно-практической конференции. Таганрог: Изд-во ИКТИБ ЮФУ, 2015. − С. 76 – 81.

47. Аралбаев, Т.З. Построение адаптивных систем мониторинга и диагностирования сложных промышленных объектов на основе принципов самоорганизации/ Т.З. Аралбаев. – Уфа : Гилем. 2003. – 248 с.

48. Аралбаев, Т.З. Сигнатурный метод контроля поведения пользователя на основе теории автоматов/ Т.З. Аралбаев, И.И. Каскинов // Наука и мир, –2017. – № 1(41). – С. 27-30.

49. Аралбаев, Т.З. Структурно-параметрический и структурно-топологический синтез распределённых систем контроля и управления объектами нефтегазодобычи/ Т.З. Аралбаев, Р.Р. Галимов. – Уфа: Гилем. 2010. – 144с.

50. Ароян, З.А. Мониторинг магистральных нефтепроводов с помощью беспилотных летательных аппаратов/ З.А. Ароян, О.А. Коркишко, Г.В. Сухарев. – URL: https://russiandrone.ru (дата обращения 10.11.2018).

51. Ассоциативно-мажоритарный подход к решению задач распознавания образов в системах защиты информации: учебно-методическое пособие для обучающихся по образовательным программам высшего образования по направлениям подготовки 09.03.01 Информатика и вычислительная техника и 10.03.01 Информационная безопасность /Т.З. Аралбаев [и др.]; М-во науки и высш. образова-

ния Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург: ОГУ, 2023. - ISBN 978-5-7410-3150. – 150 с

52. Асяев, Г.Д. Обнаружение вторжений на основе анализа аномального поведения локальной сети с использованием алгоритмов машинного обучения с учителем / Г.Д. Асяев, А. Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. – 2020. – № 1(35). – С. 77-83.

53. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/ (дата обращения 31.01.2023).

54. Белов, Е.Б. Основы информационной безопасности: Уч. пособие для вузов. / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов.— М.: Горячая линия — Телеком, 2006.— 544 с

55. Берхольц, В.В. Модель угроз информационной безопасности при передаче телеметрической информации о состоянии мобильного объекта на предприятие-разработчик / В.В. Берхольц, А.М. Вульфин, А. И. Фрид // Приоритетные направления развития науки и технологий : XXVIII Международная научно-практическая конференция, Тула, 12 марта 2021 года. – Тула: Инновационные технологии, 2021. – С. 128-132.

56. Болохонов Е.С., Репинский В.Н. Информационная безопасность АСУ с использованием машинного обучения [Электронный ресурс]. – URL: https://scilead.ru/article/86-informatsionnaya-bezopasnost-asu-s-ispolzovanie (дата обращения 10.12.2023)

57. Бояркин, М.А., Моделирование деятельности операторов АСУ ТП НГК/ М.А. Бояркин, В.А. Шапцев // Вестник кибернетики. – 2006. – № 5. – С.77-87.

58. Браницкий А.А., Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта: диссертация ... кандидата технических наук: 05.13.19 [Место защиты: С.-Петерб. ин-т информатики и автоматизации РАН]/ А. А. Браницкий. – Санкт-Петербург, 2018. – 305 с.

59. Будько, М.Б. Обнаружение аномалий сетевого трафика: основные аспекты, проблемы и методы / М. Б. Будько, А. Д. Малько, Д. Д. Стародубова, Р. Д. Стародубов // Современная наука: актуальные проблемы теории и практики. Се-

рия: Естественные и технические науки. – 2020. – № 8. – С. 46-49. – DOI 10.37882/2223-2966.2020.08.05. – EDN KOPRHT.

60. Бухарев, Д.А. Применение иерархического кластерного анализа для кластеризации данных информационных процессов АСУ ТП, подвергающихся воздействию кибератак / Д.А. Бухарев, А.Н. Соколов, А.Н. Рагозин //Вестник УрФО. Безопасность в информационной сфере.–2023 № 1 (47).– С.59-68

61. Васильев В.И. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт/ В.И. Васильев, А.М. Вульфин, И.Б. Герасимова, В.М. Картак//Вопросы кибербезопасности. 2020. № 2 (36). С. 11-21.

62. Васильев В.И. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции). / В.И. Васильев, А.Д. Кириллова, С.Н. Кухарев// Вестник УрФО. Безопасность в информационной сфере. 2018. № 4(30). С. 66- 74.

63. Васильев В.И. Комплексная оценка выполнения требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами/ В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, А.Д. Кириллова// Инфокоммуникационные технологии. 2017. Т. 15. № 4. С. 319-325.

64. Васильев В.И., Вульфин А.М., Гвоздев В.Е., Картак, В.М., Атарская Е.А. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий состояния // Системы управления, связи и безопасности, N6, 2021.- С. 90-119.

65. Васильев, В.И. Система проактивной защиты промышленного объекта на основе алгоритмов машинного обучения / В.И. Васильев, А.Д. Кириллова, А.М. Вульфин, А.И. Фрид // FISP-2021: Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации: Сборник докладов III Всероссийской научной конференции (с приглашением зарубежных ученых). – Ставрополь: Северо-Кавказский федеральный университет, 30 ноября, 2021. – С. 24–3

66. Веревкин А.П. Проблемы повышения эффективности управления процессами добычи и переработки нефти и газа / А.П. Веревкин, О.В. Кирюшин // Территория нефтегаз. 2009. №5. С. 12-15.

67. Вишнякова Т.О., Васильев В.И. Анализ эффективности систем физической защиты при помощи марковской сетевой модели // Вестник УГАТУ = Vestnik UGATU. 2007. №7. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-sistem-fizicheskoy-zaschity-pri-pomoschi-markovskoy-setevoy-modeli (дата обращения: 23.12.2022).

68. Воронцов А., АСУ ТП. Вопросы безопасности/ А. Воронцов// Jet Info – 2011. –№ 5.

69. Гаспарянц, Р.С. Организационно-технологическая система обеспечения эксплуатационной надёжности магистральных нефтепроводов: автореф. дис. … д-ра техн. наук/Р. С. Гаспарянц. — Уфа 2008. — 50 с.

70. Гетьман А.И. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений/ А.И. Гетьман, Е.Ф. Евстропов, Ю.В. Маркин. – Москва, 2015. – 52 с. – (Препринт ИСП РАН; № 28)

71. Годовой отчет о деятельности федеральной службы по экологическому, технологическому и атомному надзору в 2018 году: Федеральная служба по экологическому, технологическому и атомному надзору [Электронный ресурс]. – URL: http://www.gosnadzor.ru/public/annual_reports (дата обращения 10.12.2019).

72. Голиков, Ю.А. Г604 Экономическая эффективность системы защиты информации: учеб.-метод. пособие / Ю.А. Голиков, Л.Ю. Сульгина. – Новосибирск: СГГА, 2012. – 41 с.

73. Горбачев И.Е., Моделирование процессов нарушения информационной безопасности критической инфраструктуры:/ И.Е. Горбачев, А.П. Глухов. - Санкт-Петербург: ТРУДЫ СПИИРАН, 2015. — с. 112 – 135.

74. ГОСТ 21.408-2013 Система проектной документации для строительства. Правила выполнения рабочей документации автоматизации технологических процессов [Электронный ресурс]. – URL: https://internet-law.ru/gosts/gost/56653/ (дата обращения 31.01.2023).

75. ГОСТ Р (проект, первая редакция) Защита информации. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты. Термины и определения [Электронный ресурс]. – URL: https://fstec.ru/en/component/attachments/download/2770 (дата обращения 5.11.2022).

76. ГОСТ Р (проект, первая редакция) Управление инцидентами, связанными с безопасностью информации. Руководство по планированию и подготовке к реагированию на инциденты (ISO/IEC 27035-2:2016, NEQ) [Электронный ресурс]. – URL: https://fstec.ru/en/component/attachments/download/3038 (дата обращения 5.11.2022).

77. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. [Электронный ресурс]. – URL: https://itsec2012.ru/gosudarstvennyy-standart-rossiyskoy-federacii-gost-r-51624-2000-zashchita-informacii (дата обращения 23.12.2022).

78. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем [Электронный ресурс]. – URL: https://allgosts.ru/35/020/gost_r_56546-2015 (дата обращения 15.12.2020).

79. ГОСТ Р 59503-2021 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации [Электронный ресурс]. – URL: https://internet-law.ru/gosts/gost/76197/ (дата обращения 01.03.2023).

80. ГОСТ Р 59505-2021 Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации [Электронный ресурс]. – URL: https://allgosts.ru/13/110/gost_r_59505-2021 (дата обращения 15.12.2020).

81. ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения [Электронный ресурс]. – URL: https://allgosts.ru/35/020/gost_r_59547-2021 (дата обращения 15.12.2020).

82. ГОСТ Р 59793-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания [Электронный ресурс]. – URL: https://www.astoni.ru/upload/iblock/2d4/GOST-34.601_90.pdf (дата обращения 23.12.2022).

83. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200102762 (дата обращения 5.11.2022).

84. ГОСТ Р ИСО/МЭК 27033-2-2021 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей систем [Электронный ресурс]. – URL: https://allgosts.ru/35/040/gost_r_iso!mek_27033-2-2021 (дата обращения 15.12.2020).

85. ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска [Электронный ресурс]. – URL: https://gostrf.com/normadata/1/4293791/4293791964.pdf - 01.03.2023

86. ГОСТ Р МЭК 62443-3-3-2016 "Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. N 469-ст) [Электронный ресурс]. – URL: https://base.garant.ru/71663438 (дата обращения 5.11.2022).

87. Гудов А.М., Семехина М.В. Имитационное моделирование процессов передачи трафика в вычислительных сетях // Управление большими системами. М.: ИПУ РАН, 2010г. Выпуск 31; с.130-161

88. Десять возможных причин повреждения оптического кабеля [Электронный ресурс] – URL: https://nag.ru/articles/article/30149/desyat-vozmojnyih-prichin-povrejdeniya-opticheskogo-kabelya.html (дата обращения 23.01.2019).

89. Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации [Электронный ресурс]. - URL: http://citforum.ru/security/articles/model_proc. (дата обращения 23.12.2022).

90. Дроботун Е.Б., Построение модели угроз безопасности информации в автоматизированной системе управления Критически важными объектами на основе сценариев действий нарушителя/ Е.Б. Дроботун, О.В. Цветков,// Программные продукты и системы / Software & Systems. – 2016. – Т.29, № 3. – с. 42 – 50.

91. Дубровин В.С., Мариниченко А.А. Модернизация системы передачи данных по ЛЭП на участке «Рузаевка-Арзамас»// Электроника и информационные технологии. 2009, №2

92. Думченков, И.А. Обзор методов интеграции информационных систем, их преимуществ и недостатков / И.А. Думченков. — Текст : непосредственный // Молодой ученый. — 2018. — № 23 (209). — С. 176-177. — URL: https://moluch.ru/archive/209/51296/ (дата обращения: 13.07.2020).

93. Ежов, А.В. Натурное моделирование процесса многомерной маршрутизации пакетов в TCP/IP сети // Вестник науки и образования. 2017. №2 (26). URL: https://cyberleninka.ru/article/n/naturnoe-modelirovanie-protsessa-mnogomernoy-marshrutizatsii-paketov-v-tcp-ip-seti (дата обращения: 18.12.2019).

94. Загоруйко, Н.Г. Когнитивный анализ данных / Н.Г. Загоруйко; Рос. акад. наук, Сиб. отд-ние, Ин-т математики им. С.Л. Соболева. - Новосибирск: ГЕО, 2013. - 183, [3] с., [1] л. портр.: ил., цв. ил.; 22 см. - Библиогр.: с. 178-183

95. Зегжда Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. – М.: Горячая ЛинияТелеком, 2020. – 560 с.

96. Зегжда, Д.П. Информационная безопасность: учебник для вузов. / Д.П. Зегжда; М.: МГТУ им. Н.Э. Баумана, 2010. — 236 с. - ISBN 5-935170-18-3 .

97. Зегжда, П.Д. Подход к построению обощенной функционально-семантической модели кибербезопасности/ Зегжда П.Д., Зегжда Д.П., Степанова Т.В. // Методы и средства обеспечения информационной безопасности. – 2015. – № 2. – С. 17-25.

98. Ивахненко, А.Г. Моделирование сложных систем по экспериментальным данным [Текст] / А.Г. Ивахненко, Ю.П. Юрачковский. - Москва: Радио и связь, 1987. - 117 с.

99. Канаев, М.М.. Аппаратная поддержка систем искусственного интеллекта в виде нечеткого регулятора на распределенной ассоциативной ПАМЯТИ/ М.М.. Канаев, Г.Х. Ирзаев. - Интеллект. Инновации. Инвестиции. 2017. № 1. С. 54-57.

100. Касимов А.Ф. Автоматизация проектирования систем защиты информации с использованием методов многоальтернативной оптимизации : автореферат дис. ... кандидата технических наук : 05.13.12 / Воронеж. гос. техн. ун-т. - Воронеж, 2005. - 17 с.

101. Каскинов И.И. Сигнатурный метод контроля поведения пользователя на основе теории автоматов // Science and world. 2017. № 1 (41). Vol. 1. URL: http://scienceph.ru/d/413259/d/science_and_world_no_1_41_january_vol_i.pdf (дата обращения: 18.03.2020)

102. Каскинов, И.И. Ассоциативно-мажоритарная модель системы контроля поведения пользователя на основе теории автоматов/ И.И. Каскинов // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. XXII междунар. студ. науч.-практ. конф. № 11(22). URL: https://sibac.info/archive/meghdis/11(22).pdf (дата обращения 11.11.2018).

103. Качков, В.П. Ассоциативная память и ассоциативные процессоры в интеллектуальных системах / В.П. Качков, И.Я. Доморадов, Р.Е. Сердюков// Под науч. ред. В.В. Голенкова. – Минск : БГУИР, 2009. – 188 с.

104. Коломойцев В.С. Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации : автореферат дис. ... кандидата технических наук : 05.13.19 / Коломойцев Владимир Сергеевич; [Место защиты: С.-Петерб. гос. ун-т телекоммуникаций им. М.А. Бонч-Бруевича]. - Санкт-Петербург, 2018. - 20 с.

105. Комашинский Н.А., Котенко И.В. Модель системы обнаружения вредоносной активности с использованием сигнатурных методов с учетом технологии больших данных// Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 556-561.

106. Концепция параллельного и кольцевого резервирования// Промышленные сети. URL: http://www.promseti.ru/knowledge/ (дата обращения: 28.09.2019).

107. Корниенко А.А., Никитин А.Б., Диасамидзе С.В., Кузьменкова Е.Ю. Моделирование компьютерных атак на распределенную информационную систему // Известия Петербургского университета путей сообщения. 2018. Т. 15. № 4. С. 613-628.

108. Коробкина, Н.Н. Исследование и разработка информационно-поисковых интерфейсов на основе типологии поведения пользователей: автореф. дис. … канд. тех. наук./ Н. Н. Коробкина; Рос. гос. гуманитар. ун-т (РГГУ). 2014. - 18 с.

109. Котенко, И.В. Аналитическое моделирование атак для управления информацией и событиями безопасности / И. В. Котенко, А. А. Чечулин // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT 2012»: в 4 томах. – Дивноморское, 02–09 сентября, 2012. – Том 2. – С. 385–391

110. Крыжановский, Б.В. Ассоциативная память, способная распознавать сильно скоррелированные образы/ Б.В. Крыжановский // Доклады Академии наук – 2003. Доклады АН, информатика, т 390, №1, с.27-31, 2003

111. Кузин Д.А. Применение методов машинного обучения для классификации акустических сигналов по спектральным характеристикам / Кузин Д.А., Стаценко Л.Г., Анисимов П.Н., Смирнова М.М. // Известия СПбГЭТУ "ЛЭТИ", №3, 2021, стр. 48-54.

112. Кукса П.П. Применение ассоциативных ЗУ и ассоциативных процессоров в сетевых устройствах. [Эл. ресурс]. – Режим доступа: http://pkuksa.org/~pkuksa/publications/am-c-01.pdf (дата обращения 20.07.2023).

113. Курилов Ф.М. Моделирование систем защиты информации. Приложение теории графов // Технические науки: теория и практика: материалы III Междунар. науч. конф. — Чита: Издательство Молодой ученый, 2016. — С. 6-9.

114. Курицын Е.М. Сценарии организации цифровых трактов для ВЧ-связи по высоковольтным линиям электропередачи / В.В. Пантелеев; Техническая политика, 2006. – 10 с.

115. Лаборатория Касперского. Ландшафт угроз для систем промышленной автоматизации. – URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ (дата обращения 20.07.2019)

116. Леонович, И.А. Разработка методики прогнозирования возникновения аварийных ситуаций на компрессорных станциях магистральных газопроводов. Диссертация на соискание учёной степени кандидата технических наук/ И.А. Леонович. – Москва: Российский государственный университет нефти и газа имени И.М. Губкина, 2016. – 181 с.

117. Манжосов А.В., Аралбаев Т.З., Абрамова Т.В. Организация системы передачи информации в распределенной системе мониторинга протяженного технологического объекта // «Инновационные, информационные и коммуникационные технологии: сборник трудов XV международной научно-практической конференции; Сочи, 2018. − С. 386 – 390.

118. Мартынов, А. Использование PLC-технологии для мониторинга и управления СУ ЭНЦ на нефтедобывающих предприятиях/А. Мартынов// Автоматизация нефтегазовой отрасли. Control engineering Россия, 2016. - Т. 62, № 2. - С. 59-62.

119. Машечкин, И.В. Мониторинг и анализ поведения пользователей компьютерных систем/ И. В. Машечкин, М. И. Петровский, С.В. Трошин // Проблемы программирования. – 2008. – № 2-3. – С. 541-549.

120. Машкина И.В. Концепция построения модели угроз информационной среде объекта информатизации / И.В. Машкина, В.И. Васильев, Е.А. Рахимов // Информационные технологии. 2007. №2. С. 24 – 32.

121. Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP: свидетельство о гос. регистрации программы для ЭВМ / Т.В. Абрамова, И.Д. Зайчиков; правообладатель Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т".- 2022.

122. Методика оценки угроз безопасности информации (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). URL: https://www.garant.ru/products/ipo/prime/doc/400325044/. (дата обращения 11.11.2021).

123. Методология функционального моделирования IDEF0. Руководящий документ РД IDEF0-2000 М.: Госстандарт России, 2000.

124. Мониторинг аномалий сетевой активности в промышленных системах/ Инженерные и промышленные решения нового поколения [Электронный ресурс]. – Режим доступа: https://automation.croc.ru/press-center/media/55792/ - 04.06.2020.

125. Наинг, Л.З. Исследование и разработка методов передачи данных в системах управления технологическими процессами с использованием PLC сети: диссертация ... кандидата технических наук : 05.13.06 [Место защиты: Нац. исслед. ун-т МИЭТ]/ Л.З. Наинг. – Москва, 2015. – 132 с.

126. Нуруллаев М.М. Моделирование информационных процессов в интегрированных системах безопасности // Молодой ученый. - 2018. - №17. - С. 26-27.

127. О безопасности критической информационной инфраструктуры Российской Федерации [Текст]: федеральный закон от 26.07.2017 г. № 187-ФЗ // Собр. законодательства Рос. Федерации. – 2017. – № 31. Ст. 4736.

128. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования / Приказ ФСТЭК от 21.12.2017 № 235 [Электронный ресурс]. URL: https://fstec.ru/index?id=1606:prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235. (дата обращения 25.07.2022).

129. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 5.11.2022).

130. Обеспечение целостности телеметрической информации о состоянии сложного технического объекта / А. И. Фрид, А. М. Вульфин, М. Б. Гузаиров, В.

В. Берхольц // Моделирование, оптимизация и информационные технологии. – 2023. – Т. 11, № 1(40). – С. 17-18.

131. Обнаружение сетевых атак на основе стохастических контекстно-независимых грамматик // Вестник МГТУ им. Н.Э. Баумана. 2006. Т. 1, № 4. с. 94 - 101. [N.V. Medvedev and V.A. Grishin, “Modeling scenarios of network attacks based on stochastic context-independent grammars”, (in Russian), in Vestnik MGTU im. N.E. Baumana”. vol. 1, no. 4, pp. 94-101, 2006.]

132. Оладько, В.С. Причины и источники сетевых аномалий/ В.С. Оладько, С.Ю. Микова, М.А. Нестеренко, Е.А. Садовник // Молодой ученый. — 2015. — №22. — С. 158-161.

133. Осипов В.Ю. Аналоговые ассоциативные интеллектуальные системы // Труды СПИИРАН. 2013. Вып. 30. С. 141-155.

134. Остапенко А.Г. Эпидемии в телекоммуникационных сетях/ А.Г. Остапенко, Н.М. Радько, А.О. Калашников, О.А. Остапенко, Р.К. Бабаджанов. М.: Горячая линия - Телеком, 2017. – 282 с.

135. Остапенко А.Г., Калашников А.О., Остапенко Г.А., Плотников Д.Г., Доросевич О.В., Стародубцева Ю.Г., Чернышова С.В. Теория сетевых войн. Живучесть атакуемых сетей: учеб. пособие [Электронный ресурс]. 1 электрон. опт. диск (CD-ROM). Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2016. – 157 с.

136. Пат. 2012156444 Российская Федерация, МПК G06F21/50, G06F21/62, G06Q90/00. Система и способ адаптивного управления и контроля действий пользователя на основе поведения пользователя/ Леденев Александр Вячеславович (RU), Колотинский Евгений Борисович (RU), Игнатьев Константин Сергеевич (RU); заявитель и патентообладатель Закрытое акционерное общество "Лаборатория Касперского" (RU). - 2012156444/08; заявл. 25.12.2012; опубл.27.06.2014

137. Патент 2193797 Российская Федерация, G06G007/60, Устройство ассоциативной памяти и способ распознавания образов / Сутерланд Дж. МПК. / заявитель и патентообладатель Сутерланд Дж. № 92016491/14; опубл. 27.11.2002.

138. Патент 2306605 Российская Федерация, МПК 7 G11C15/00. Ассоциативная память / Кабак И.С., Суханова Н.В: заявитель и патентообладатель Кабак И. С., Суханова Н. В; заявл. 2007-12-24; опубл. 20.10.2008.

139. Патент 2306605 Российская Федерация. Устройство для распознавания образов / Аралбаева Г.Г., Аралбаев Т.З., Хасанова С.В., Хасанов Р.И.; заявитель и патентообладатель ОГУ. – № 2014102726/08; заявл. 28.01.2014; опубл. 10.12.2014, Бюл. №34. – 18 с.

140. Патент 2430415 Российская Федерация, МПК G 06 K 9/00. Устройство для распознавания образов / Р.И. Хасанов, М.З. Масягутов, Т.З. Аралбаев; заявитель и патентообладатель Оренбургский государственный университет. – №2010116601/08; заявл. 26.04.2010 – опубл. 27.09.2011, Бюл. № 27. – 21 с.

141. Патент 2533064 Российская Федерация, МПК G 06 K 9/62. Устройство для распознавания образов / Сарайкин А.И., Хасанов Р.И., Аралбаев Т.З.; заявитель и патентообладатель Оренбургский государственный университет. – № 2013149729/08; заявл. 06.11.2013 – опубл. 20.11.2014, Бюл. № 32. – 16 с.

142. Патент 2540818 Российская Федерация. Устройство для распознавания образов / Аралбаев Т.З., Хасанов Р.И., Сарайкин А.И., Закревский Г.В. / заявитель и патентообладатель ОГУ. – № 2013138762/08; заявл. 20.08.2013; опубл. 10.02.2015, Бюл. № 4. – 19 с.

143. Патент 2675896 Российская Федерация, МПК G06K9/62. Устройство для контроля поведения пользователя / Абрамова Т.В., Аралбаев Т.З., Каскинов И.И., Хатеев М.Д./ заявитель и патентообладатель ОГУ. – № 2018100997/08; заявл. 10.01.2018; опубл. 25.12.2018, Бюл. № 36. – 17 с.

144. Патент № 2738460 C1 Российская Федерация, МПК H04L 1/00, G06F 21/00. Способ выявления аномалий в работе сети автоматизированной системы : № 2020108174 : заявл. 26.02.2020 : опубл. 14.12.2020 / А. С. Антипинский, Н. А. Домуховский, Д. Е. Комаров, А. Н. Синадский ; заявитель Общество с ограниченной ответственностью "Сайберлимфа".

145. Патент на полезную модель 77483 Российсая Федерация МПК 7 G11C15/00 Ассоциативная память [Текст]/ Кабак И. С., Суханова Н. В. - № 2007147587; заявл. 24.12.2007; опубл 20.10.2008, Бюд №29 – 2 с.: ил.

146. Пищик, Б.Н. Безопасность АСУ ТП/ Б.Н. Пищик // Вычислительные технологии Том 18, Специальный выпуск, – 2013. – С. 170-175.

147. Подопросветов, А.В. Сравнительный анализ метода геометризированных гистограмм и нейросетевого метода для распознавания дорожной разметки/А.В. Подопросветов, Д.А. Анохин, К.И. Кий, И.А. Орлов. // Сравнительный анализ метода геометризированных гистограмм и нейросетевого метода для распознавания дорожной разметки / А.В. Подопросветов [и др.] // Препринты ИПМ им. М.В. Келдыша. 2021. № 104. 22 с.

148. Подробное описание протокола Modbus TCP с примерами команд [Электронный ресурс]. –URL: https://ipc2u.ru/articles/prostye-resheniya/modbus-tcp/. (дата обращения 10.11.2018).

149. Положение о Реестре ключевых систем информационной инфраструктуры (утв. приказом ФСТЭК России от 04.03.2009). URL: https://www.securitylab.ru/blog/personal/zlonov/144489.php. (дата обращения 11.11.2018).

150. Попов, Г.А. Алгоритм маршрутизации сетевых потоков с учетом требований по безопасности/Г.А. Попов, Е.А. Попова // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2016. №2. URL: https://cyberleninka.ru/article/n/algoritm-marshrutizatsii-setevyh-potokov-s-uchetom-trebovaniy-po-bezopasnosti (дата обращения: 25.12.2019).

151. Приказ ФСТЭК России от 14 марта 2014 года № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». URL: https://docs.cntd.ru/document/499084780. (дата обращения 25.07.2021).

152. Принципы организации PCL-сетей и используемое оборудование [Электронный ресурс]. – Режим доступа: https://studbooks.net/2275465/informatika/printsipy_organizatsii_setey_ispolzuemoe_oborudovanie – 23.05.2019.

153. Промышленная безопасность. Надзор за объектами нефтегазового комплекса. Нормативные правовые и правовые акты. URL: https://www.gosnadzor.ru/industrial/oil/acts/ (дата обращения 11.11.2021).

154. Пьявченко, Т.А. Проектирование АСУТП в SCADA-системе: учебное пособие. – Таганрог: Изд-во Технологического института ЮФУ. 2007. – 78 с.

155. Рахматуллин, Р.Р. Расчет технико-экономических показателей и определение экономического эффекта программного продукта [Электронный ресурс]: метод. указания / Р. Р. Рахматуллин, Л.Ф. Давлетбаева; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. экономики и орг. пр-ва. - Оренбург : ГОУ ОГУ. - 2008. - 30 с

156. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 19.11.2007). URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 11.11.2018).

157. Репозиторий инцидентов промышленной безопасности [Электронный ресурс]. - URL: https://www.risidata.com/ (дата обращения 23.01.2021).

158. Романов М.П. Ассоциативная память на логических элементах. Межвузовский сборник научных трудов. Автоматическое управление и интеллектуальные системы. М.: МИРЭАД996

159. Рузавин Г.И. Методология научного исследования : Учеб. пособие для студентов вузов / Г.И. Рузавин. - М. : ЮНИТИ, 1999. – 316 с.

160. Савина, А.В. Аварийность на отечественных и зарубежных магистральных трубопроводах // Безопасность труда в промышленности. – 2014. - № 2. – С. 14-17.

161. Саенко И.Б., Котенко И.В., Аль-Барри М.Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. 2022. №2 (48). URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennyh-neyronnyh-setey-dlya-vyyavleniya-anomalnogo-povedeniya-polzovateley-tsentrov-obrabotki-dannyh (дата обращения: 12.11.2023).

162. Симанков В.С., Луценко Е.В. Адаптивное управление сложными системами на основе теории распознавания образов. Монография (научное издание) /Техн. ун-т Кубан. гос. технол. ун-та. – Краснодар, 2019. – 318 с.

163. Скакун, С.В. Математическое моделирование поведения пользователей компьютерных систем // Математические машины и системы, - 2005. - № 2. - С. 122–129.

164. Сравнение промышленных средств обнаружения вторжений (СОВ для АСУ ТП) [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/compare/Intrusion-Detection-Systems#part52 - 04.06.2021.

165. Суханов, А.В. Метод нахождения аномалий при диагностике верхнего строения пути / А.В. Суханов, С.М. Ковалев// Программные системы и вычислительные методы — № 2(3) – Москва, NOTA BENE (ООО "НБ-Медиа"), 2013. С. 176 – 180.

166. Тенденции развития киберинцидентов АСУ ТП за 2023 год [Электронный ресурс]. — URL: https://www.infowatch.ru/sites/default/files/analytics/files/tendentsii-razvitiya-kiberintsidentov-asu-tp-za-dve-tysyachi-dvadtsat-tretiy-god.pdf (дата обращения: 15.05.2024).

167. Тимофеев А.В., Браницкий А.А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевых атак – International Journal INFORMATION TECHNOLOGIES & KNOWLEDGE VOLUME 6/2012, с. 257–265.

168. Титов, С. Системы автоматизации и контроля в нефтегазовом комплексе // Control Engineering Россия. – 2015. - № 3(57). – С. 28 - 31.

169. Трошин, С.В. Мониторинг работы корпоративных пользователей // Вопросы современной науки и практики. Университет им. В.И. Вернадского,- 2009. - № 2(16). - С. 59-72.

170. Трубопроводный транспорт нефти / С.М. Вайншток, В.В. Новоселов, А.Д. Прохоров, А.М. Шаммазов и др.; Под ред. С.М. Вайнштока: Учеб. для вузов: В 2 т. – М.: ООО «Недра-Бизнесцентр». 2004. – Т.2. – 621 с.

171. Ту Дж., Гонсалес Р. Принципы распознавания образов// М.: Мир, 1978. — 412 с.

172. Ужинский, А.В. Методы и средства мониторинга сервисов передачи данных в глобальных распределенных инфраструктурах : автореф. дис. … канд. техн. наук: автореферат дис. ... кандидата технических наук : 05.13.01 / Ужинский Александр Владимирович; [Место защиты: Междунар. ун-т природы, общества и человека «Дубна»]. – Дубна. 2010. – 20 с.

173. Университетский фонд электронных ресурсов. Оренбургский государственный университет. - URL: https://ufer.osu.ru/ (дата обращения 23.12.2022).

174. Устройство поиска информации Десницкий В.А., Котенко И.В., Паращук И.Б., Саенко И.Б., Чечулин А.А., Дойникова Е.В. Патент на изобретение 2724788 C1, 25.06.2020. Заявка № 2019132407 от 14.10.2019.

175. Филиппович, А.Ю. Интеграция ситуационного, имитационного и экспертного моделирования. автореф. дис. на соиск. учен. степ. канд. техн. наук специальность 05.13.11 <Автоматизация и управление технологическими процессами и производствами>// А.Ю. Филиппович; [Моск. гос. ун-т печати (техн. ун-т)]. - Москва, 2009 . - 25 с. : ил. ; 21 см. - Библиогр.: с. 25.

176. Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты // Программные продукты и системы (SOFTWARE&SYSTEMS). – 1998. – №2. – С.6-9.

177. ЦЭР: Обзор программ анализа и мониторинга сетевого трафика [Электронный ресурс]. – Наука, техника, образование, 1999-2015 – Режим доступа: http://pi.314159.ru/volotka/volotka1.htm - 04.06.2019

178. Черноруцкий, И.Г. Методы принятия решений/ И. Г. Черноруцкий. – СПб.: БХВ – Петербург. 2005. – 736 с.

179. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. М.: Горячая линия-Телеком, 2019. - 448 с.

180. Шелухин О.И., Ерохин С.Д., Полковников М.В. Технологии машинного обучения в сетевой безопасности. Горячая линия–Телеком, 2021. -353 с.

181. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : Учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – Москва: Горячая линия–Телеком, 2013. – 220 с. – ISBN 9785991203234.

182. Шипулин А. Мониторинг аномалий сетевой активности в промышленных системах [Электронный ресурс]. URL: https://automation.croc.ru/press-center/media/55792/. (дата обращения 11.07.2019). [A. Shipulin (2019, Jul. 11). Monitoring network activity anomalies in industrial systems [Online]. Available: https://automation.croc.ru/press-center/media/55792/]

183. Энциклопедия АСУ ТП : Аппаратное резервирование: Резервирование промышленных сетей [Электронный ресурс]. – Режим доступа: https://www.bookasutp.ru/Chapter8_3 - 04.06.2021.

184. Aralbaev T. Z., Abramova T.V. Network Traffic Monitoring on the Basis of Sequential and Associative–Sequential Search Principles // Russian Engineering Research. – 2018. Vol. 38, - №. 5, - pp. 381–383. © Allerton Press, Inc., 2018. ISSN 1068-798X Original Russian Text © T.Z. Aralbaev, T.V. Abramova, 2017, published in STIN, - 2017, №. 11. - pp. 2–5.

185. Architecture of the security access system for information on the state of the automatic control systems of aircraft / A. I. Frid, A. M. Vulfin, V. V. Berholz [et al.] // Acta Polytechnica Hungarica. – 2020. – Vol. 17, No. 8. – P. 151-164.

186. Asyaev, G. Anomaly Detection Model in APCS Using AutoML / G.. Asyaev, A.. Sokolov //Proceedings - 2022 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2022.–2022.– P.305-308

187. DATAPK: программный комплекс для полноценной защиты АСУ ТП. [Электронный ресурс]: – URL: http://www.pressreader.com/russia/ekspert-ural/20140929/281947426075740 (дата обращения: 24.03.2023).

188. Eric D. Knapp, Joel Thomas Langill, Industrial Network Security (Second Edition), Syngress, 2015. ISBN 9780124201149

189. Index of /publicDatasets/CTU-Malware-Capture-Botnet-253-1 [Электронный ресурс]. — URL: https://mcfp.felk.cvut.cz/publ icDatasets/CTU-Malware-Capture-Botnet-253-1/ (дата обращения: 24.03.2023).

190. Kaspersky Administration Kit 8.0. Справочное руководство [Электронный ресурс]. – URL: https://kaspersky.antivirus.lv/files/10258_kasp8.0_ak_refguideru.pdf (дата обращения 27.09.2019)

191. Kaspersky Industrial CyberSecurity [Электронный ресурс]. — URL: https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity (дата обращения: 24.11.2022).

192. Kaspersky Industrial CyberSecurity for Networks. [Электронный ресурс]. – Режим доступа: https://support.kaspersky.com/KICSforNetworks/4.0/ru-RU/104127.htm (дата обращения 25.08.2023).

193. Khairul Azizan Suda, Nazatul Shima Abdul Rani, Hamzah Abdul Rahman, Wang Chen. A Review on Risks and Project Risks Management: Oil and Gas Industry // International Journal of Scientific and Engineering Research 6(8) – 2016. – Vol. 6.– pp. 938-943.

194. Kotenko I., Saenko I., Kushnerevich A., Branitskiy A. ATTACK DETECTION IN IOT CRITICAL INFRASTRUCTURES: A MACHINE LEARNING AND BIG DATA PROCESSING APPROACH// Proceedings - 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2019. 27. 2019. С. 340-347.

195. Malware Capture Facility Project [Электронный ресурс]. — URL: https://www.stratosphereips.org/datasets-malware (дата обращения: 24.03.2023).

196. ModBus TCP. Промышленный протокол для TCP/IP-сетей. [Электронный ресурс]. – LAZY SMART, 2015–2018 – URL: http://lazysmart.ru/osnovy-avtomatiki/modbus-tcp-promy-shlenny-j-protokol-dlya-tcp-ip-setej/ (дата обращения 22.10.2018).

197. Mohsen Imani, Tajana Rosing “CAP: Configurable Resistive Associative Processor for Near-Data Computing”, IEEE International Symposium on Quality Electronic Design (ISQED), 2017

198. Neuro TECHLAB [Электронный ресурс]. – URL: https://www.neurotechlab.ru/software/neural-excel (дата обращения 05.04.2023).

199. Niv Goldenberg, Avishai Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013, - pp. 63-75.

200. Parashchuk Igor, Doynikova Elena, Saenko Igor, Kotenko Igor. Selection of Countermeasures against Harmful Information based on the Assessment of Semantic Content of Information Objects in the Conditions of Uncertainty // 2020 International Conference on innovations in Intelligent systems and Applications INISTA 2020. Novi Sad, August 24-26 2020 P. 9194680

201. PT Industrial Security Incident Manager [Электронный ресурс]. — URL: https://www.ptsecurity.com/ru-ru/products/isim/ (дата обращения: 24.11.2022).

202. Rafael Ramos, Regis Barbosa, Ramin Sadre, Aiko Pras, Flow whitelisting in SCADA networks, International Journal of Critical Infrastructure Protection, Volume 6, Issues 3–4, December. - 2013, - pp. 150-158.

203. Ramakrishnan P. Self-Similar Traffic Models. Technical research report. Available at: http://www.isr.umd.edu/TechReports/ISR/1999/TR_99-12/TR_99-12.phtml , accessed 09.07.2018.

204. Song X. Conditional anomaly detection / X. Song et al. //Knowledge and Data Engineering, IEEE Transactions on. – 2007. – Vol. 19, - №. 5. – pp. 631-645.

205. STAFFCOP. Атаки на АСУ ТП. [Электронный ресурс]. - Режим доступа: https://www.anti-malware.ru/threats/APCS-attacks (дата обращения 20.02.2020).

Приложение А. Акты о внедрении результатов диссертационной работы

Уральский Центр Систем Безопасности
Технологии защиты бизнеса.
Аудит. Проектирование.
Внедрение. Сопровождение.

620100
г. Екатеринбург
ул. Ткачей, д. 6

тел.: +7(343) 379-98-34
факс: +7(343) 382-05-63

info@ussc.ru
www.USSC.ru

УТВЕРЖДАЮ

Заместитель Генерального директора
ООО «УЦСБ»
_____ *В. Ёркин*
«10» _____ 2024 г.

АКТ
о внедрении результатов диссертационной работы
Абрамовой Таисии Вячеславовны на тему
«Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков»

Настоящим Актом подтверждается, что в ООО «УЦСБ» используется пакет прикладных программ, разработанный на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет» аспирантом Абрамовой Таисией Вячеславовной, доктором технических наук, профессором Аралбаевым Ташбулатом Захаровичем, кандидатом технических наук, доцентом Галимовым Ринатом Равилевичем.

Пакет программ включает:

– прикладная программа «Метод кластеризации моделей угроз для распределенной АСУ процессом транспортировки нефтегазового сырья» (программа зарегистрирована в университетском фонде электронных ресурсов ОГУ, регистрационный номер №2022 от 18.11.2019);

– прикладная программа «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (программа зарегистрирована в университетском фонде электронных ресурсов ОГУ, регистрационный номер №1972 от 24.09.2019);

– программный комплекс «Моделирование сетевого трафика на базе протокола TCP/ModBUS» (программный комплекс зарегистрирован в университетском фонде электронных ресурсов ОГУ, регистрационный номер №1657 от 12.11.2018);

– прикладная программа «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности компьютерной сети» (программа зарегистрирована в университетском фонде электронных ресурсов ОГУ, регистрационный номер №1109 от 20.05.2015).

Перечисленные программы используются в рамках реализации перспективных проектов по обеспечению информационной безопасности АСУ нефтегазового комплекса Оренбургской области.

Заместитель генерального директора
по научно-технической работе Н.А. Домуховский

Рисунок А.1 – Акт о внедрении результатов диссертационной работы в ООО «УЦСБ»

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ГАЗПРОМНЕФТЬ-ОРЕНБУРГ»
(ООО «ГАЗПРОМНЕФТЬ-ОРЕНБУРГ»)

УТВЕРЖДАЮ
Заместитель генерального директора
по корпоративной защите

ПОДРАЗДЕЛЕНИЕ КОРПОРАТИВНОЙ ЗАЩИТЫ

_____ В.А. Подгорнов

«14» апреля 2024 г.

АКТ
о передаче результатов диссертационной работы
Абрамовой Таисии Вячеславовны на тему
«Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков»

Настоящим подтверждается, что результаты диссертационного исследования на тему «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков», полученные при проведении научно-исследовательской работы аспиранта кафедры вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет» Абрамовой Таисии Вячеславовны, переданы для ознакомления и возможного внедрения в ООО «Газпромнефть-Оренбург». Переданные результаты включают:

– алгоритмы и программы для моделирования аномалий в информационной системе мониторинга состояния нефтепровода по данным сетевого трафика;
– алгоритмы и программы для обнаружения аномалий и нейтрализации угроз в распределенных автоматизированных системах управления;
– алгоритм и программа кластеризации угроз и моделей угроз для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья.

Практическая ценность разработанных алгоритмов и программ заключается в снижении рисков от угроз безопасности информации при их применении в подсистемах защиты информации распределенных автоматизированных систем управления транспортировкой нефтегазопродуктов.

Начальник отдела по
информационно-аналитической работе
УЭБ ООО «Газпромнефть-Оренбург» **Р.Э. Галиев**

Профессор кафедры вычислительной техники
и защиты информации ФГБОУ ВО
«Оренбургский государственный университет» **Т.З. Аралбаев**

Рисунок А.2 – Акт о передаче результатов диссертационной работы в ООО «Газпромнефть-Оренбург»

Автономная некоммерческая организация дополнительного образования «Просвещение»
460014, г. Оренбург, ул. Лениская 59/1, офис 1
тел. +7 (3532) 26-65-70
e-mail: educatio56@yandex.ru

УТВЕРЖДАЮ

Директор
АНО ДО «Просвещение»
_____ А.В. Панова
«27» _____ 2024 г.

АКТ
о внедрении результатов диссертационного исследования
Абрамовой Таисии Вячеславовны на тему
«Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков»

Настоящий акт подтверждает, что в учебном процессе АНО ДО «Просвещение» используется пакет прикладных программ, разработанный на кафедре. вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет», аспирантом Абрамовой Таисией Вячеславовной.

Пакет программ включает:

– прикладная программа «Синергетическая имитационная модель сетевых атак на ресурсы вычислительных систем» (программа зарегистрирована в университетском фонде электронных ресурсов ОГУ, регистрационный номер №970 от 03.06.2014);

– прикладная программа «Комбинаторная семантическая модель генерации гипотез» (программа зарегистрирована в университетском фонде электронных ресурсов ОГУ, регистрационный номер №1236 от 29.03.2016);

– прикладная программа «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (программа зарегистрирована в университетском фонде электронных ресурсов ОГУ, регистрационный номер №1972 от 24.09.2019).

Указанные программы используются в учебном процессе при изучении курсов «Информатика» и «Программирование».

Директор А.В. Панова

Заместитель директора Н.П. Панов

Рисунок А.3 – Акт о внедрении результатов диссертационного исследования в учебный процесс АНО ДО «Просвещение» (г. Оренбург)

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет» (ОГУ)

АКТ

_____ № _____

г. Оренбург

УТВЕРЖДАЮ
Первый проректор
ФГБОУ ВО «Оренбургский государственный университет»
профессор С.В. Нотова
_____
«25» июня 2021 г.

АКТ
о внедрении результатов кандидатской диссертации
Абрамовой Таисии Вячеславовны в учебный процесс

Экспертная комиссия федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» (ОГУ) в составе: председателя комиссии — проректора по научной работе ОГУ, доктора физико-математических наук, профессора Летуты С.Н., членов комиссии:
начальника управления научной и инновационной деятельности, кандидата технических наук Болдырева П.А., директора аэрокосмического института, доктора технических наук, профессора Сердюка А.И., декана факультета математики и информационных технологий, кандидата физико-математических наук, доцента Герасименко С.А. - составили настоящий акт о том, что в учебном процессе факультета математики и информационных технологий ОГУ и аэрокосмического института ОГУ используются следующие разработки и учебно-методические материалы старшего преподавателя кафедры «Вычислительной техники и защиты информации» Абрамовой Т.В.:

- алгоритмы и программы обнаружения и нейтрализации аномалий в распределенных автоматизированных системах на основе мониторинга сетевых информационных потоков;
- монография «Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков» (авторы: Т.З. Аралбаев, Г.Г. Аралбаева, Т.В. Абрамова, Р.Р. Галимов, А.В. Манжосов; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2018).

Указанные результаты используются в учебном процессе при изучении студентами дисциплин «Защита информационных процессов в компьютерных системах», «Основы информационной безопасности», «Проектирование систем информационной безопасности» и «Комплексная защита в распределенных информационно-вычислительных системах» по направлениям подготовки 10.03.01 - Информационная безопасность и 09.03.01 – Информатика и вычислительная техника.

Председатель комиссии -
проректор по научной работе ОГУ С.Н. Летута

Члены комиссии:
начальник управления научной и инновационной деятельности П.А. Болдырев

директор аэрокосмического института А.И. Сердюк

декан факультета математики и информационных технологий С.А. Герасименко

Рисунок А.4 – Акт о внедрении результатов кандидатской диссертации в учебный процесс ФГБОУ ВО «ОГУ»

УТВЕРЖДАЮ

Директор ООО «Пластик»

Кубиц А.А.

« 22 » июня 2021 г.

АКТ
о передаче результатов диссертационной работы
Абрамовой Таисии Вячеславовны

Настоящим Актом подтверждается, что результаты диссертационного исследования Абрамовой Т.В., включающие алгоритмы и программы обнаружения и нейтрализации аномалий в распределенных информационно-вычислительных и управляющих системах на основе мониторинга сетевых информационных потоков, являются полезными, обладают высокой производительностью и достоверностью, представляют практический интерес и могут быть использованы при решении задач, связанных с безопасным хранением, передачей и обработкой данных.

Переданные результаты включают:

– пакет программ для моделирования аномалий в распределенных информационно-вычислительных и управляющих системах.

– пакет программ для обнаружения и нейтрализации аномалий в распределенных информационно-вычислительных и управляющих системах.

Специалист по информационной безопасности Ковальский К.А.

Рисунок А.5 – Акт о передаче результатов диссертационной работы

в ООО «Пластик»

Приложение Б. Определение информативных признаков аномалии по данным протокола Modbus TCP

Таблица Б.1 – Распределение сетевых протоколов в промышленных АСУ по уровням модели OSI

Уровень модели OSI	Функции	Тип данных	Основные протоколы
Прикладной уровень	Обеспечение взаимодействия сети и приложений пользователя	потоки данных	HTTP, gopher, Telnet, DNS, SMTP, SNMP, CMIP, FTP, TFTP, SSH, IRC, AIM, NFS, NNTP, NTP, SNTP, XMPP, FTAM, APPC, X.400, X.500, AFP, LDAP, SIP, ITMS, Modbus TCP, BACnet IP, IMAP, POP3, SMB, MFTP, BitTorrent, eD2k, PROFIBUS
Уровень представления	Операции с формой представления данных (преобразование протоколов, сжатие/распаковка, кодирование/декодирование данных), перенаправление запросов		HTTP, ASN.1, XML-RPC, TDI, XDR, SNMP, FTP, Telnet, SMTP, NCP, AFP
Сеансовый	Управление сеансом связи, созданием/завершением сеанса, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений		ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, NWLink, Printer Access Protocol, Zone Information Protocol, SSL, TLS, SOCKS
Транспортный	Надежная доставка данных без ошибок, потерь и дублирования в нужной последовательности, разделение данных на сегменты	сегменты	TCP, UDP, NetBEUI, AEP, ATP, IL, NBP, RTMP, SMB, SPX, SCTP, DCCP, RTP, TFTP
Сетевой	Логическая адресация, определение маршрутов пересылки пакетов от источника к приемнику	пакеты	IP, IPv6, ICMP, IGMP, IPX, NWLink, NetBEUI, DDP, IPSec, ARP, RARP, DHCP, BootP, SKIP, RIP
Канальный	Канальная адресация, проверка доступности канала передачи, проверка целостности данных и коррекция ошибок передачи	кадры	STP, ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, FDDI, Frame Relay, LocalTalk, Token ring, StarLan, L2F, L2TP, PPTP, PPP, PPPoE, PROFIBUS
Физический	Передача потока данных в виде электрических и оптических сигналов по каналам связи	биты (эл. сигналы)	RS-232, RS-422, RS-423, RS-449, RS-485, ITU-T, xDSL, ISDN, T1, E1, 10BASE-T, 10BASE2, 10BASE5, 100BASE-T, 1000BASE-T, 1000BASE-TX, 1000BASE-SX

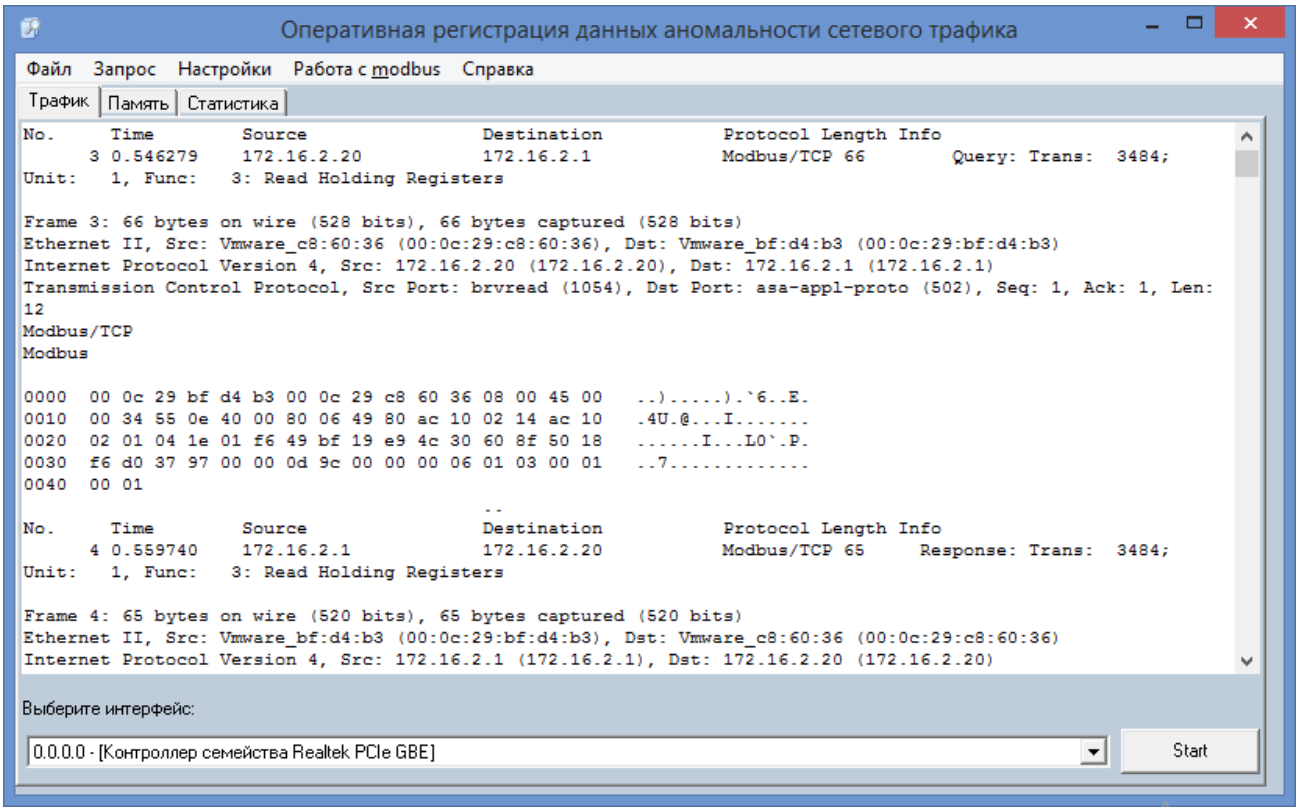


Рисунок Б.1 – Экранная форма регистрации трафика Modbus TCP

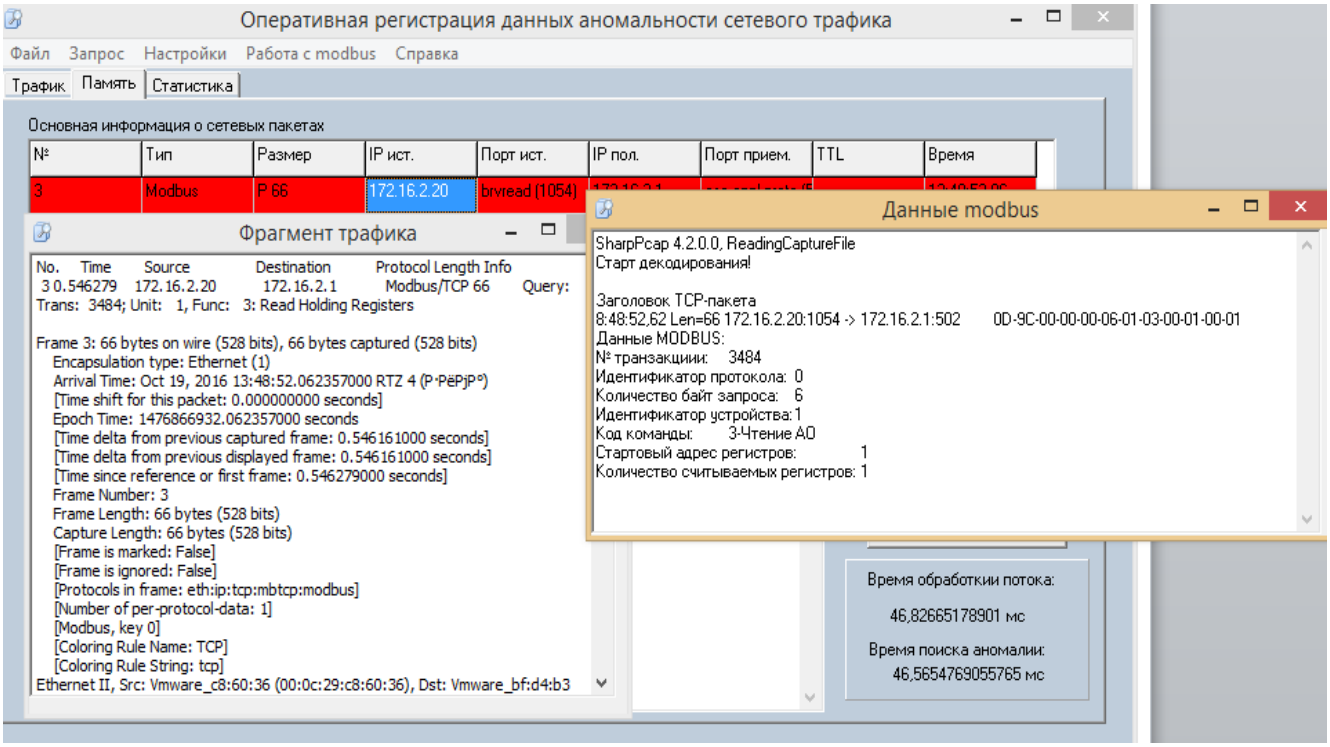


Рисунок Б.2 – Экранная форма поиска и декодирования пакета запроса на чтение регистров по протоколу Modbus TCP

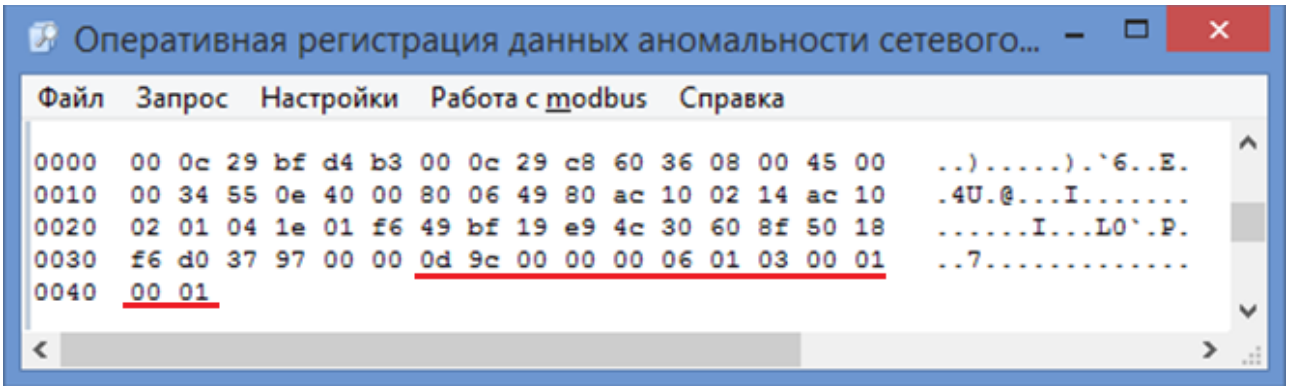
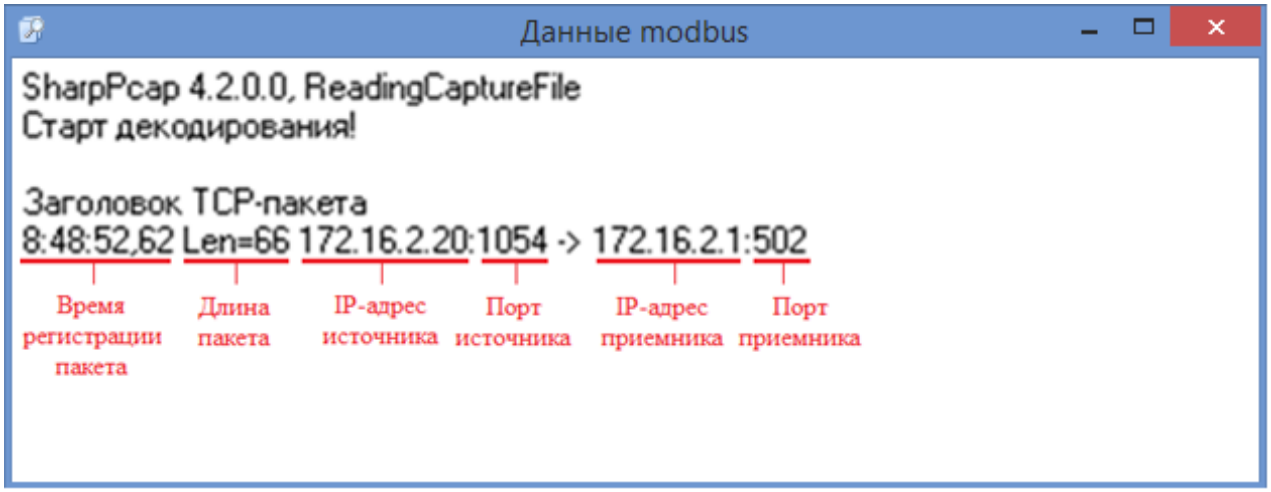
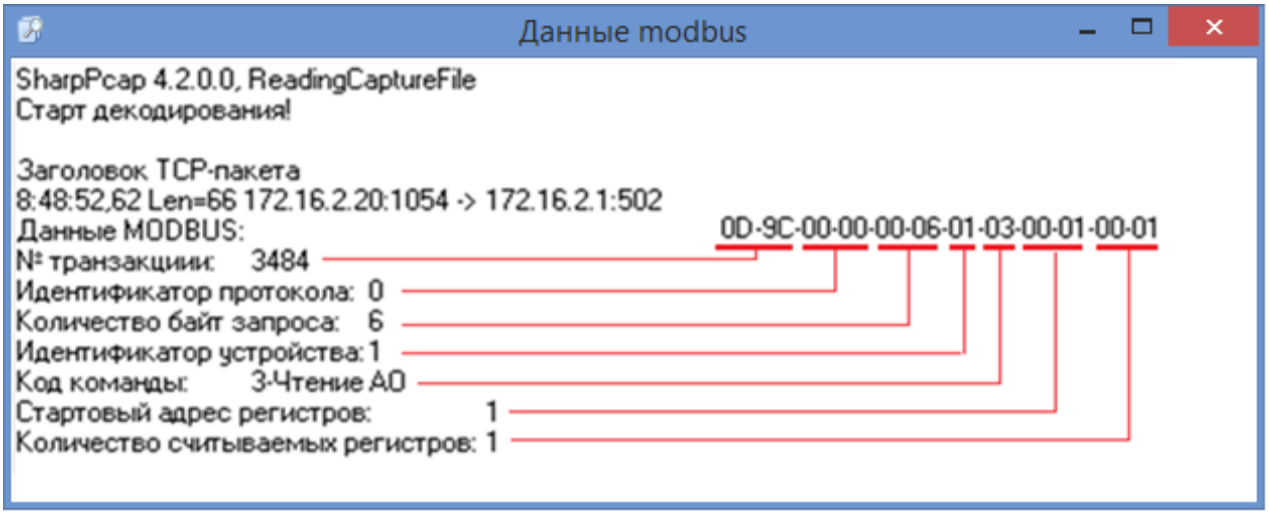


Рисунок Б.3 - Экранная форма содержимого пакета запроса на чтение регистров по протоколу Modbus TCP



а)



б)

Рисунок Б.4 - Определение информативных признаков аномалии: (а) в заголовке TCP-пакета; (б) в данных протокола Modbus

Приложение В. Анализ методов обнаружения аномалий в сетевом трафике АСУ

Таблица В.1 - Сравнительный анализ методов обнаружения аномалий в сетевом трафике АСУ

Группы методов	Методы обнаружения аномалий в СТ АСУ	Достоинства	Недостатки
Поведенческие методы	- вейвлет-анализа	- возможность проанализировать сигнал СТ в частотно-временной области и исследовать аномальный процесс на фоне остальных компонент; - высокая достоверность; - возможность обнаружения аномалий в режиме реального времени; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- большая вычислительная сложность; - наличие ложноположительных срабатываний.
	- статистического анализа	- возможность обнаружения широкого спектра аномалий; - высокая адаптивность к новым видам аномалий; - способность обнаруживать распределённые в пространстве и времени аномалии; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- наличие ложноположительных срабатываний; - сложность задания пороговых значений; - неспособность обнаружить атаки со стороны субъектов, для которых отсутствуют шаблоны типичного поведения; - нечувствительность к порядку следования событий.
	- спектрального анализа	- возможность описать частотный состав исследуемого трафика и выявить скрытые закономерности; - способность обнаруживать циклические аномалии в СТ; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- в наличие ложноположительных срабатываний.
	- кластерного анализа	- выявление закономерностей и взаимосвязей в данных СТ; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- сложность интерпретация результатов кластеризации; - чрезмерное обобщение данных; - кластеризация больших массивов данных может быть дорогостоящей и трудоёмкой.
	- фрактального анализа	- возможность обнаружения аномалий в разных типах СТ; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- снижение оперативности работы при увеличении количества обрабатываемых параметров.

Продолжение таблицы В.1

Группы методов	Методы обнаружения аномалий в СТ	Достоинства	Недостатки
	- анализа энтропии	- масштабируемость; - легкость в реализации; - чувствительность к изменениям распределений характеристик СТ; - отсутствие необходимости в данных для обучения.	- низкая достоверность при обнаружении мелкомасштабных атак; - затруднена диагностика в сетях с малыми объёмами передаваемого трафика; **- неэффективны при обнаружении аномалий в СТ АСУ ТП.**
Методы вычислительного интеллекта и машинного обучения	- нейронных сетей	- оперативность; - достоверность; - способность к обучению; - гибкость; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- требуется большой объем данных для обучения; - природа «черного ящика»; - высокая ресурсоемкость.
	- нечеткой логики	- возможность обнаружения новых типов атак; - позволяют относить аномалию к нескольким классам одновременно в разной степени принадлежности; **- применимы для обнаружения аномалий в СТ.**	- сложность определения границ аномальных состояний; - невысокая достоверность.
	- иммунных систем	- способность обнаруживать неизвестные аномалии при низком уровне ошибок; - способность постоянно самообучаться в процессе анализа; - способность к самоорганизации; **- применимы для обнаружения аномалий в СТ.**	- большое количество ложных срабатываний; - сложность интерпретации результатов.
	- метод опорных векторов	- эффективность для многомерных данных; - интерпретируемость; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- чувствительность к шуму; - вычислительная сложность.
	- Байесовских сетей	- высокая эффективность для сложных систем; - возможность учета как статистических данных, так и экспертных оценок; - простота интерпретации и наглядность; **- эффективны при обнаружении аномалий в СТ АСУ ТП.**	- требуют знания множества условных вероятностей; - трудность определения всех взаимодействий в сетях Байеса для сложных систем.

Продолжение таблицы В.1

Группы методов	Методы обнаружения аномалий в СТ	Достоинства	Недостатки
Методы вычислительного интеллекта и машинного обучения	- деревьев решений	- возможность выявления закономерностей в проявлении аномалии; - возможность учёта динамики аномального процесса для прогнозирования и ретроспективного анализа; - **эффективны при обнаружении аномалий в СТ АСУ ТП.**	- необходимость подготовки большого объёма данных для обучения; - наличие ложных срабатываний.
	Мар-сплайнов	- возможность решения задачи при неизвестных закономерностях; - устойчивость к шумам во входных данных; - адаптация к изменениям в среде. - **эффективны при обнаружении аномалий в СТ АСУ ТП.**	- зависимость от выбранного алгоритма кластеризации.
	- алгоритмов кластеризации	- возможность выявлять ранние признаки развития аномалий в динамических процессах; - **эффективны при обнаружении аномалий в СТ АСУ ТП.**	- потребность в больших объёмах размеченных данных для обучения алгоритмов.
	- алгоритмов регрессии	- способность выявлять сложные и малозаметные аномалии; - возможность адаптации к изменениям в инфраструктуре АС и характере трафика; - **эффективны при обнаружении аномалий в СТ АСУ ТП.**	- потребность в больших объёмах размеченных данных для обучения алгоритмов; - наличие ложных срабатываний; - сложность интерпретации результатов.
Методы на основе знаний	**Методы на основе экспертных систем**	- низкая вероятность ложных тревог.	- низкая оперативность; - сложность построения нормального профиля работы АС; - потребность в больших объёмах знаний и опыта; - неэффективны при обнаружении неизвестных видов атак; - **неэффективны при обнаружении аномалий в СТ АСУ ТП.**

Приложение Г. Результаты вычислительных экспериментов по исследованию эффективности применения разработанных методов

Таблица Г.1. - Результаты вычислительного эксперимента по оценке производительности (*Ts/Tas*) ассоциативного подхода в задаче идентификации маршрутов распространения вредоносного кода (*Ts* и *Tas* – время поиска при использовании базового и ассоциативного подходов к анализу сетевого трафика соответственно)

Nz	***V=200***			***V=500***			***V=1000***		
	***Ts* (мс)**	***Tas* (мс)**	***Ts/Tas***	***Ts* (мс)**	***Tas* (мс)**	***Ts/Tas***	***Ts* (мс)**	***Tas* (мс)**	***Ts/Tas***
1	100	1	100	250	1	250	500	1	500
2	100	2	50	250	2	125	500	2	250
3	100	3	33,33	250	3	83,33	500	3	166,67
4	100	4	25	250	4	62,5	500	4	125
5	100	5	20	250	5	50	500	5	100
6	100	6	16,67	250	6	41,67	500	6	83,33
7	100	7	14,28	250	7	35,71	500	7	71,43
8	100	8	12,5	250	8	31,25	500	8	62,5
9	100	9	11,11	250	9	27,78	500	9	55,55
10	100	10	10	250	10	25	500	10	50
…	…	…	…	…	…	…	…	…	…
20	100	20	5	250	20	12,5	500	20	25
30	100	30	3,33	250	30	8,33	500	30	16,67
40	100	40	2,5	250	40	6,25	500	40	12,5
50	100	50	2	250	50	5	500	50	10
60	100	60	1,67	250	60	4,17	500	60	8,33
70	100	70	1,43	250	70	3,57	500	70	7,14
80	100	80	1,25	250	80	3,125	500	80	6,25
90	100	90	1,11	250	90	2,78	500	90	5,55
100	100	100	1	250	100	2,5	500	100	5

Таблица Г.2 – Результаты расчета рисков информационных потерь в режимах переключения на резервные каналы связи при вероятностях потери связи на каждом участке p=0,1

Число недоступных участков	**Объем недоступной информации (Мбит/сек)**	**Риск в базовом варианте (Мбит/сек)**	**Риск при резервировании (Мбит/сек)**	**Эффект**
N=10	50	5	4,3	14,00%
N=9	45	4,5	3,8	15,56%
N=8	40	4	3,3	17,50%
N=7	35	3,5	2,8	20,00%
N=6	30	3	2,3	23,33%
N=5	25	2,5	1,8	28,00%
N=4	20	2	1,3	35,00%
N=3	15	1,5	0	100,00%
N=2	10	1	0	100,00%
N=1	5	0,5	0	100,00%

Таблица Г.3 – Результаты расчета вероятностей реализации несанкционированной транзакции в базовом $\boldsymbol{Pt_1}$ и новом $\boldsymbol{Pt_2}$ вариантах при различном числе рубежей защиты $\boldsymbol{N}$ в системе

P / N	**$Pt_1(N)$, p_i=0,01**	**$Pt_1(N)$, p_i=0,02**	**$Pt_1(N)$, p_i=0,04**	**$Pt_1(N)$, p_i=0,06**	**$Pt_2(N)$, p_i=0,01**	**$Pt_2(N)$, p_i=0,02**	**$Pt_2(N)$, p_i=0,04**	**$Pt_2(N)$, p_i=0,06**
1	0,01	0,02	0,04	0,06	0,00000001	0,00000016	0,00000256	0,00001296
2	0,0001	0,0004	0,0016	0,0036	0,00000001	0,00000016	0,00000256	0,00001296
3	0,000001	0,000008	0,000064	0,000216	0,00000001	0,00000016	0,00000256	0,00001296
4	0,00000001	0,00000016	0,00000256	0,00001296	0,00000001	0,00000016	0,00000256	0,00001296

Оценка экономического эффекта от применения разработанных методов

Для оценки экономической эффективности разработанных методов обнаружения аномалий и нейтрализации угроз использована формула (4.1), в которой эффективность оценивается по критерию снижения уровня риска ИБ по отношению к базовым СЗИ с учетом затрат на реализацию средств защиты на основе разработанных методов.

В качестве средств защиты информации рассмотрены разработанные программные средства, представленные в таблице Г.4.

Таблица Г.4 – Программные средства (ПС) для обнаружения аномалий и нейтрализации угроз

Программное средство	Наименование	Ссылка
1. Программы для восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС»; - ПС «Комбинаторная семантическая модель генерации гипотез»	[11] [13]
2. Программа определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	- ПС «Маршрутизация сетевых потоков в режимах переключения на резервные каналы связи»	[5]
3. Программа мониторинга действий персонала в АС	- ПС «Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP»	[121]

Для расчета себестоимости программных продуктов использована методика [155], согласно которой себестоимость рассчитывается по формуле (1):

$$C = \text{М}_{\text{ВС}} + \text{Э} + \text{З}_{\text{ЗП}}^{\text{О}} + \text{З}_{\text{ЗП}}^{\text{Д}} + \text{З}_{\text{СН}} + H, \quad (1)$$

где M_{BC} – затраты на вспомогательные материалы, руб.;

Э – затраты на электроэнергию на технологические цели, руб.;

$\text{З}_{\text{ЗП}}^{\text{О}}$ – основная зарплата разработчика, руб.;

$\text{З}_{\text{ЗП}}^{\text{Д}}$ – дополнительная зарплата разработчика, руб.;

Зсн – взнос на социальное страхование и обеспечение, руб.;

H – накладные расходы, руб.

Общая трудоёмкость разработки программного продукта рассчитывается по формуле (2):

$$T_{\text{ОБЩ}} = t_{\text{ТЗ}} + t_{\text{ЭП}} + t_{\text{ТП}} + t_{\text{РП}} + t_{B}, \quad (2)$$

где $t_{ТЗ}$ – затраты труда на стадии технического задания (в днях);

$t_{ЭП}$ – затраты труда на стадии эскизного проекта (в днях);

$t_{ТП}$ – затраты труда на стадии технического проекта (в днях);

$t_{РП}$ – затраты труда на стадии рабочего проекта (в днях);

t_{B} – затраты труда на стадии внедрения (в днях).

Расчет $T_{\text{ОБЩ}}$ для каждого из разработанных программных средств с учётом поправочных коэффициентов представлен в таблице Г.5.

Таблица Г.5 - Общая трудоёмкость разработки программных продуктов

Программное средство	**Расчет трудозатрат**
1. Программы для определения и восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	$T_{\text{ОБЩ}} = 14 + 20 + 30 + 14 + 7 = 85$ дней
2. Программа для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	$T_{\text{ОБЩ}} = 14 + 20 + 30 + 7 + 7 = 78$ дней
3. Программа мониторинга действий персонала в АС	$T_{\text{ОБЩ}} = 15 + 20 + 30 + 16 + 8 = 89$ дней

Необходимое число исполнителей - 1 человек.

Затраты на вспомогательные материалы для разработки каждой из программ приведены в таблице Г.6.

Таблица Г.6– Затраты на вспомогательные материалы

Наименование затрат	Количество, шт.	Сумма, руб.
Доступ в Интернет	≈3 месяца	2100
Бумага офисная, А4	500 листов	300
Тонер для картриджа	1	400
Канцелярский набор	1	500
Память USB	1	300
Всего		3600

Затраты на электроэнергию рассчитываются по формуле (3):

$$Э = Р * С_Э * T_{ОБЩ} * R_{ЗАГ}, \quad (3)$$

где P – мощность потребляемой электроэнергии, Кватт;

$C_Э$ – стоимость одного киловатт-часа электроэнергии, руб.;

$T_{ОБЩ}$ – общие затраты труда на разработку программного продукта, час;

$R_{ЗАГ}$, – коэффициент загрузки компьютера.

В таблице Г.7 представлены результаты расчета затрат на электроэнергию для каждого программного средства по формуле (3).

Таблица Г.7 – Затраты на электроэнергию

Программное средство	**Расчет затрат на электроэнергию**
1. Программы для определения и восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	$Э = 0{,}3 * 3{,}77 * (85 * 8) * 0{,}9 = 692{,}2$ руб
2. Программа для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	$Э = 0{,}3 * 3{,}77 * (78 * 8) * 0{,}9 = 635{,}2$ руб
3. Программа мониторинга действий персонала в АС	$Э = 0{,}3 * 3{,}77 * (89 * 8) * 0{,}9 = 724{,}7$ руб

Основная заработная плата разработчика рассчитывается по формуле (4):

$$З^0_{ЗП} = С_{ЧТС} * T_{ОБЩ} \quad (4)$$

где $C_{ЧТС}$ – часовая тарифная ставка разработчика, руб.;

$T_{ОБЩ}$ – общие затраты труда на разработку программного продукта, час.

Дополнительная заработная плата разработчика составляет 10% от основной зарплаты. В таблице Г.8 представлены результаты расчета основной и дополнительной заработной плат разработчика для каждого программного средства.

Таблица Г.8 – Расчет основной и дополнительной заработной платы разработчика

Программное средство	Расчет основной и дополнительной заработной платы
1. Программы для определения и восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	$З_{ЗП}^{О} = 60 * 85 * 8 = 40800$ руб $З_{ЗП}^{Д} =$ 4080 руб$З_{ЗП}^{Д} =$руб.
2. Программа для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	$З_{ЗП}^{О} = 60 * 78 * 8 = 37400$ руб $З_{ЗП}^{Д} =$ 3740 руб
3. Программа мониторинга действий персонала в АС	$З_{ЗП}^{О} = 60 * 89 * 8 = 42720$ руб $З_{ЗП}^{Д} =$ 4272 руб

Взносы на социальное страхование и обеспечение определяются по формуле (5):

$$З_{СН} = (З_{ЗП}^{О} + З_{ЗП}^{Д}) * R_{СН}, \quad (5)$$

$R_{СН}$ – коэффициент взноса на социальное страхование и обеспечение;

$R_{СН}$ = 0,35.

В таблице Г.9 представлены результаты расчета взносов на социальное страхование.

Таблица Г.9 – Взносы на социальное страхование

Программное средство	Расчет взносов на социальное страхование
1. Программы для определения и восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	$З_{СН} = (40800 + 4080) * 0{,}35 = 15708$ руб
2. Программа для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	$З_{СН} = (37400 + 3740) * 0{,}35 = 14399$руб
3. Программа мониторинга действий персонала в АС	$З_{СН} = (42720 + 4272) * 0{,}35 = 16447{,}2$ руб

Накладные расходы рассчитываются по формуле (6):

$$Н = 0{,}1 * (З_{ЗП}^{О} + З_{ЗП}^{Д}). \quad (6)$$

В таблице Г.10 представлены результаты расчета накладных расходов.

Таблица Г.10 – Накладные расходы

Программное средство	Накладные расходы
1. Программы для определения и восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	$H = 0{,}1 * (40800 + 4080) =$4488 руб
2. Программа для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	$H = 0{,}1 * (37400 + 3740) =$4114 руб
3. Программа мониторинга действий персонала в АС	$H = 0{,}1 * (42720 + 4272) = 4699{,}2$ руб

В таблице Г.11 представлены результаты расчета полной себестоимости разработанных программных средств.

Таблица Г.11 – Полная себестоимость разработанных программных средств

Программное средство	Себестоимость
1. Программы для определения и восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	$C = 3600 + 692{,}2 + 40800 + 4080 + 15708 + 4488 =$ 69368 руб
2. Программа для определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС	$C = 3600 + 635{,}2 + 37400 + 3740 + 14399 + 4114 = 63888$ руб
3. Программа мониторинга действий персонала в АС	$C = 3600 + 724{,}7 + 42720 + 4272 + 16447{,}2 + 4699{,}2 = 72463$ руб
Итого:	205719 руб

Одним из наиболее популярных аналогов разработанных программных средств, представленных на отечественном рынке, является программное решение Kaspersky Industrial CyberSecurity for Networks [192], реализующий функции:

- отображения сетевых взаимодействий между устройствами промышленной сети в виде карты сети;

- мониторинга технологического процесса с помощью анализа значений передаваемых тегов и обнаружения попыток нелегитимного вмешательства в технологический процесс, мониторинга команд к ПЛК;

- контроля целостности промышленной сети.

Стоимость годовой лицензии на программное обеспечение Kaspersky Industrial CyberSecurity for Networks составляет 834720 рублей для 2 – 33 рабочих станций (на 2023 год).

Таким образом, суммарная стоимость разработанных программных средств более чем в 4 раза ниже стоимости коммерческих аналогов. Особенностью разработанных ПС является возможность их бессрочного использования для неограниченного числа рабочих станций.

Стоимость аппаратного обеспечения для разработанных методов зависит от числа узлов в КС и рассчитывается для каждого конкретного случая. Исследования, проведенные на основе вычислительных экспериментов в работах [21, 41] показали высокую эффективность разработанных методов на базе ассоциативных процессоров в больших и средних сетях.

Значение рисков информационной безопасности зависят от ущерба и вероятностей реализации угрозы и рассчитываются для каждой системы индивидуально. Результаты вычислительных экспериментов, представленные в разделе 4.2, показали, что вероятность и ущерб при внедрении разработанных методов снижаются. Согласно отчету компании Dragos, занимающейся вопросами кибербезопасности АСУ ТП, средняя стоимость одного инцидента ИБ в АСУ ТП обходится организации почти в 3 миллиона долларов (U ≈ 284 000 000 руб.). Таким образом, риск от нейтрализуемых угроз БИ значительно превышает стоимость разработанного программного обеспечения, что также свидетельствует об экономической эффективности разработанных методов.

Приложение Д. Многоаспектный анализ результатов диссертационной работы в задаче защиты информации

Одним из факторов успешного создания систем защиты информации (СЗИ) является наличие и рациональное использование инструментальной базы средств поиска технических решений (ТР) и оценка их эффективности на всех стадиях и этапах построения системы. Большая организационная и техническая сложность проектных работ обусловила использование наряду с традиционными новых решений для повышения качества проекта, а вместе с этим – и необходимость оценки эффективности этих решений.

В научной литературе известен представительный ряд публикаций, посвященных данной тематике. В частности, в статьях [67, 176] рассматриваются вопросы поиска адекватных оценок проектов и внедряемых систем, в [104] представлены результаты исследований вкладов отдельных технических решений в общую эффективность разработки, в [89, 100] приводятся результаты разработки систем автоматизации проектных работ по созданию СЗИ.

Однако представленные работы не позволяют в полной мере оценить эффективность результатов конкретных решений в совокупности других результатов разработок сложных проектов. Эти вопросы нередко возникают в процессе выявления актуальных стратегий при управлении проектами, а также в процессе обсуждения и принятия решений о соответствии результатов научных исследований системе требований к научно-квалификационным работам.

Целью настоящего раздела является повышение качества процесса разработки СЗИ на основе системного анализа эффективности частных технических решений с использованием многоаспектной матричной модели процесса создания СЗИ. Для достижения цели решены следующие задачи:

- разработана структура многоаспектной интерактивной матричной модели (МИМ) для системного анализа характеристик технических решений по созданию СЗИ;

- представлен вариант применения МИМ для анализа эффективности разработанных методов и средств в задаче построения СЗИ на основе мониторинга сетевого трафика [2].

Согласно [159], метод - некоторая специфическая процедура, состоящая из последовательности определенных действий или операций, применение которых приводит либо к достижению поставленной цели, либо приближает к ней. Предметом исследования в настоящей работе являются множество методов **M** и множество средств **C,** являющихся техническими решениями для построения и совершенствования СЗИ на основе мониторинга сетевого трафика.

Ниже представлена структура многоаспектной матричной модели декомпозиции процесса создания СЗИ по стадиям, структуре СЗИ и ее компонентам. Множество аспектов ***A,*** позволяющих определить систему оценок качества технических решений, содержит следующие элементы.

1. Структурный аспект ***S***, определяющий уровень детализации СЗИ: система, подсистема, функциональный блок. Выбор перечня функциональных блоков обусловлен особенностями решения задачи, требованиями нормативных документов к СЗИ для рассматриваемого класса систем, а так же необходимостью расширения функциональной полноты существующих средств защиты в соответствии с требованиями проекта.

2. Технологический аспект ***T***, определяющий стадии создания СЗИ или ее компонентов.

3. Аспект ***K***, определяющий качество ТР на основе показателей технической, экономической и социальной эффективности.

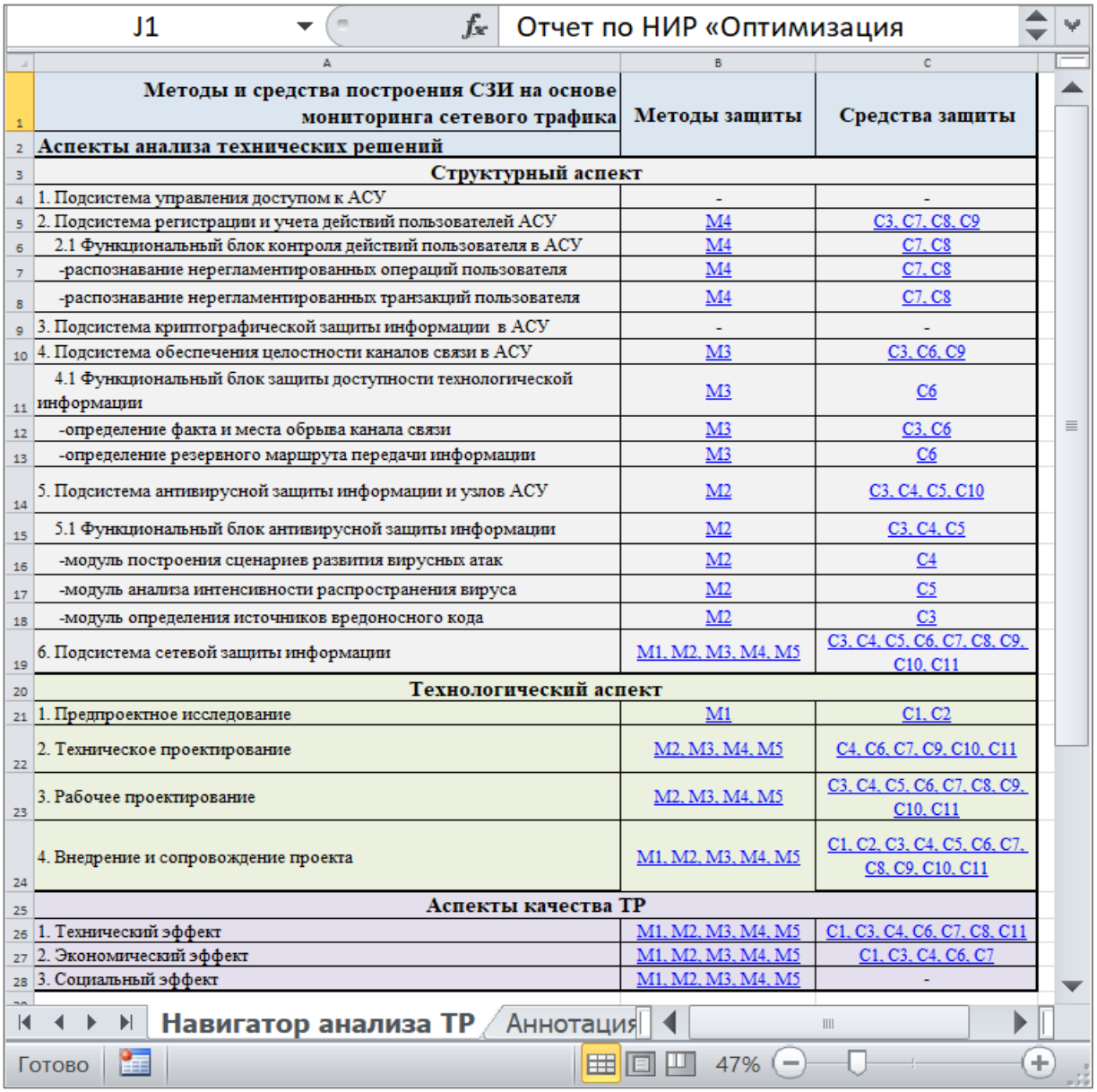
Таким образом, каждое техническое решение может быть описано фасетным кодом ***Ф*** (1):

$$\Phi=\{S;\ T;\ K\}. \qquad (1)$$

В зависимости от задачи анализа результатов исследований и разработки перечень составляющих фасетного кода дополняется такими компонентами, как: уровень актуальности ***R***, достоверности ***D***, практической значимости ***Z*** или другими атрибутами результатов.

Для систематизации разработанных методов и средств в модели использован способ классификации и кодирования по методике, представленной в [9]. Согласно предложенному способу, разработанному решению присваивается код, каждый блок которого характеризует определенный аспект анализа ТР и содержит номера подсистем СЗИ, стадий проектирования и видов эффекта, относящихся к анализируемому методу или средству.

Для реализации модели разработано приложение для многоаспектного анализа эффективности частных решений в задаче защиты информации на основе табличного процессора MS Excel.



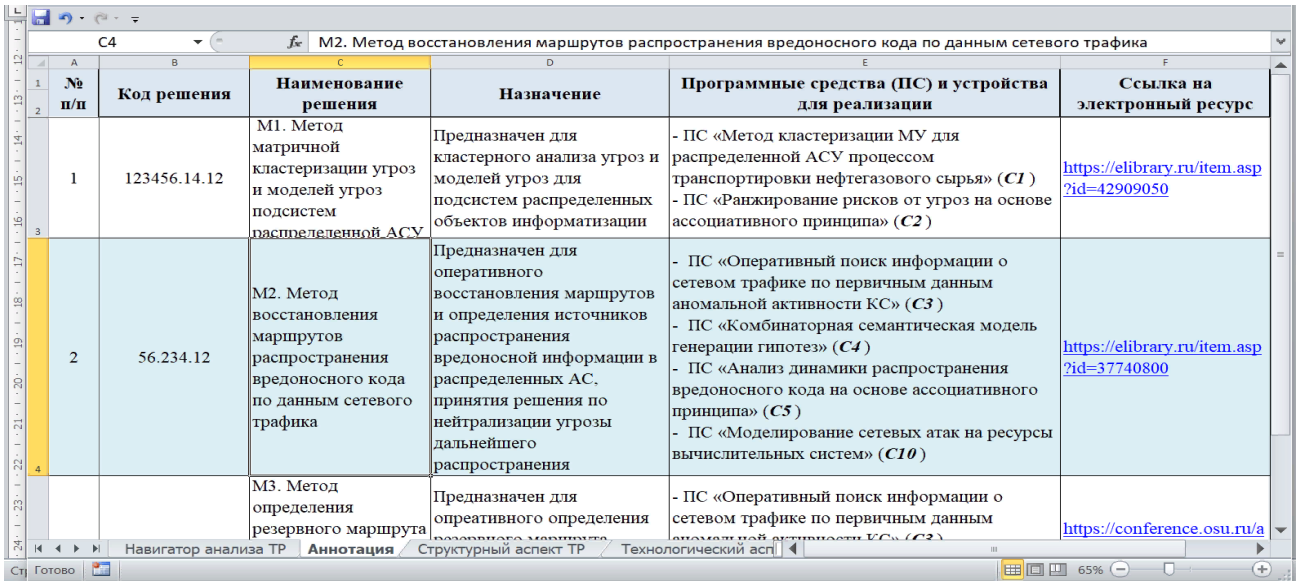
Методы и средства построения СЗИ на основе мониторинга сетевого трафика	Методы защиты	Средства защиты
Аспекты анализа технических решений		
Структурный аспект		
1. Подсистема управления доступом к АСУ	-	-
2. Подсистема регистрации и учета действий пользователей АСУ	M4	C3, C7, C8, C9
2.1 Функциональный блок контроля действий пользователя в АСУ	M4	C7, C8
-распознавание нерегламентированных операций пользователя	M4	C7, C8
-распознавание нерегламентированных транзакций пользователя	M4	C7, C8
3. Подсистема криптографической защиты информации в АСУ	-	-
4. Подсистема обеспечения целостности каналов связи в АСУ	M3	C3, C6, C9
4.1 Функциональный блок защиты доступности технологической информации	M3	C6
-определение факта и места обрыва канала связи	M3	C3, C6
-определение резервного маршрута передачи информации	M3	C6
5. Подсистема антивирусной защиты информации и узлов АСУ	M2	C3, C4, C5, C10
5.1 Функциональный блок антивирусной защиты информации	M2	C3, C4, C5
-модуль построения сценариев развития вирусных атак	M2	C4
-модуль анализа интенсивности распространения вируса	M2	C5
-модуль определения источников вредоносного кода	M2	C3
6. Подсистема сетевой защиты информации	M1, M2, M3, M4, M5	C3, C4, C5, C6, C7, C8, C9, C10, C11
Технологический аспект		
1. Предпроектное исследование	M1	C1, C2
2. Техническое проектирование	M2, M3, M4, M5	C4, C6, C7, C9, C10, C11
3. Рабочее проектирование	M2, M3, M4, M5	C3, C4, C5, C6, C7, C8, C9, C10, C11
4. Внедрение и сопровождение проекта	M1, M2, M3, M4, M5	C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11
Аспекты качества ТР		
1. Технический эффект	M1, M2, M3, M4, M5	C1, C3, C4, C6, C7, C8, C11
2. Экономический эффект	M1, M2, M3, M4, M5	C1, C3, C4, C6, C7
3. Социальный эффект	M1, M2, M3, M4, M5	-

Рисунок Д.1 - Экранная форма навигатора анализа технических решений

На рисунках Д.1 – Д.3 приводится вариант реализации МИМ для многоаспектного анализа решений, полученных по итогам научных исследований по теме гранта РФФИ № 18-47-560012 «Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков» [45].

В частности, на рисунке Д.1 представлена экранная форма навигатора анализа технических решений, отображающего общую структуру многоаспектной матричной модели и позволяющего определить место разработанного решения в структуре СЗИ, этапы проектирования и вид получаемого эффекта.

Ввод сведений о технических решениях осуществляется с использованием специальных опросных анкет, реализованных в табличном процессоре MS Excel. На рисунке Д.2 представлен фрагмент аннотации ТР, содержащей общие сведения о решении и ссылки на соответствующие электронные ресурсы в сети Internet.



№ п/п	Код решения	Наименование решения	Назначение	Программные средства (ПС) и устройства для реализации	Ссылка на электронный ресурс
1	123456.14.12	М1. Метод матричной кластеризации угроз и моделей угроз подсистем распределенной АСУ	Предназначен для кластерного анализа угроз и моделей угроз для подсистем распределенных объектов информатизации	- ПС «Метод кластеризации МУ для распределенной АСУ процессом транспортировки нефтегазового сырья» (***С1***) - ПС «Ранжирование рисков от угроз на основе ассоциативного принципа» (***С2***)	https://elibrary.ru/item.asp?id=42909050
2	56.234.12	М2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Предназначен для оперативного восстановления маршрутов и определения источников распространения вредоносной информации в распределенных АС, принятия решения по нейтрализации угрозы дальнейшего распространения	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (***С3***) - ПС «Комбинаторная семантическая модель генерации гипотез» (***С4***) - ПС «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (***С5***) - ПС «Моделирование сетевых атак на ресурсы вычислительных систем» (***С10***)	https://elibrary.ru/item.asp?id=37740800
		М3. Метод определения резервного маршрута	Предназначен для опреативного определения	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным	https://conference.osu.ru/a

Рисунок Д.2 - Экранная форма аннотации технических решений

Переход к сведениям о ТР и результатам анализа их эффективности осуществляется со страницы навигатора по гиперссылкам, обеспечивающим интерактивность модели и быструю навигацию между сведениями о решении, результатами анализа по различным аспектам и соответствующими электронными ресурсами сети Internet. Например, при нажатии на ссылку М2 в поле навигатора,

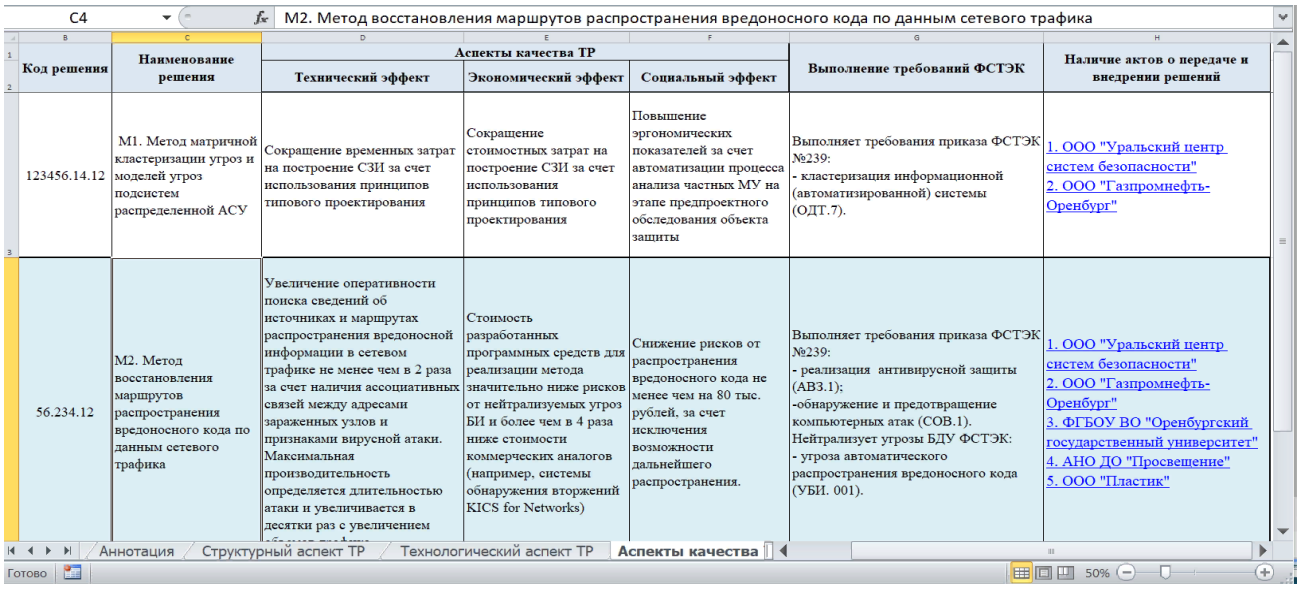
характеризующего определенный аспект анализа, выводится информация об эффективности метода М2 «Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика» по соответствующему аспекту. Строка сведений об анализируемом методе выделяется цветом.

Анализ решений по структурному аспекту осуществляется согласно требованиям стандарта [77] и приказа [129]. Относительно представленного в примере метода М2 можно сделать вывод, что метод относится к подсистемам антивирусной и сетевой защиты информации и позволяет повысить функциональную полноту средств антивирусной защиты за счет функций построения сценариев, анализа интенсивности и определения источников сетевой вирусной атаки.

Анализ решений по технологическому аспекту осуществляется согласно стандарту [82]. В результате анализа делается вывод о том, на каком этапе проекта используется разработанное решение. Например, модели, разработанные при реализации метода метод М2, используются на этапе технического проектирования, а программное обеспечение – на этапах рабочего проектирования, внедрения и сопровождения проекта.

Анализ решений по аспектам качества ТР проводится с учетом технического, экономического и социального эффекта от его использования. На рисунке Д.3 в качестве примера представлена экранная форма результатов анализа эффективности метода М2 по аспектам качества ТР.

Оценка технической эффективности в представленном примере проводилась по методу [21], где в качестве основного критерия для оценки выбрана оперативность анализа сетевого трафика. Такой выбор обусловлен необходимостью оценки производительности разработанных методов и средств поиска информации об атаке в больших объемах сетевого трафика. Например, метод М2 позволяет повысить производительность поиска фрагментов маршрутов распространения вредоносной информации в сетевом трафике за счет использования принципов ассоциативности, а также достоверность определения источников и сценариев сетевой атаки на основе мажоритарного подхода.



C4 | M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика

Код решения	Наименование решения	Аспекты качества ТР			Выполнение требований ФСТЭК	Наличие актов о передаче и внедрении решений
		Технический эффект	Экономический эффект	Социальный эффект		
123456.14.12	M1. Метод матричной кластеризации угроз и моделей угроз подсистем распределенной АСУ	Сокращение временных затрат на построение СЗИ за счет использования принципов типового проектирования	Сокращение стоимостных затрат на построение СЗИ за счет использования принципов типового проектирования	Повышение эргономических показателей за счет автоматизации процесса анализа частных МУ на этапе предпроектного обследования объекта защиты	Выполняет требования приказа ФСТЭК №239: - кластеризация информационной (автоматизированной) системы (ОДТ.7).	1. ООО "Уральский центр систем безопасности" 2. ООО "Газпромнефть-Оренбург"
56.234.12	M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Увеличение оперативности поиска сведений об источниках и маршрутах распространения вредоносной информации в сетевом трафике не менее чем в 2 раза за счет наличия ассоциативных связей между адресами зараженных узлов и признаками вирусной атаки. Максимальная производительность определяется длительностью атаки и увеличивается в десятки раз с увеличением	Стоимость разработанных программных средств для реализации метода значительно ниже рисков от нейтрализуемых угроз БИ и более чем в 4 раза ниже стоимости коммерческих аналогов (например, системы обнаружения вторжений KICS for Networks)	Снижение рисков от распространения вредоносного кода не менее чем на 80 тыс. рублей, за счет исключения возможности дальнейшего распространения.	Выполняет требования приказа ФСТЭК №239: - реализация антивирусной защиты (АВЗ.1); -обнаружение и предотвращение компьютерных атак (СОВ.1). Нейтрализует угрозы БДУ ФСТЭК: - угроза автоматического распространения вредоносного кода (УБИ. 001).	1. ООО "Уральский центр систем безопасности" 2. ООО "Газпромнефть-Оренбург" 3. ФГБОУ ВО "Оренбургский государственный университет" 4. АНО ДО "Просвещение" 5. ООО "Пластик"

Аннотация | Структурный аспект ТР | Технологический аспект ТР | Аспекты качества

Готово | 50%

Рисунок Д.3 - Экранная форма результатов анализа эффективности метода по аспектам качества ТР

При оценке экономической эффективности в работе предполагалось, что техническое решение приносит эффект, если затраты на его реализацию меньше, либо соизмеримы с затратами на аналогичные средства защиты при снижении рисков от угроз в случае его внедрения.

При оценке социального эффекта учитывалось повышение эргономических показателей при внедрении разработанных решений за счет автоматизации процессов поиска информации об инциденте ИБ и принятия мер по нейтрализации соответствующей ему угрозы.

Анализ выполнения требований Федеральной службы по техническому и экспортному контролю (ФСТЭК России) позволил оценить общий эффект от внедрения ТР, в частности, выполнение требований приказа №239 [128], значимого при построении СЗИ для исследуемого объекта, нейтрализуемые угрозы из банка данных угроз ФСТЭК [53] и степень снижения рисков от угроз, вследствие выполнения требований. На рисунке Д.3 в столбце «Выполнение требований ФСТЭК» приведен пример результатов оценки эффективности метода М2, позволяющего снизить риски от актуальных для исследуемого объекта угроз, связанных с распространением вредоносного кода в системе. Оценка угроз в приведенном примере осуществлялась с учетом реальных характеристик АСУ транспорти-

ровкой нефтегазового сырья по методике [122]. Численные значения показателей эффективности получены на основе данных опросных анкет, заполняемых авторами разработанных решений. Новизна и достоверность работы метода и средств для его реализации подтверждены наличием актов об их передаче и внедрении на отраслевых предприятиях. Характеристика разработанных методов и средств по результатам многоаспектного анализа эффективности представлена в таблице Д.1.

Таблица Д.1 – Характеристика разработанных методов и средств по результатам многоаспектного анализа эффективности

Метод	**Результаты анализа**	**Средства для реализации метода**
Метод матричной кластеризации угроз и моделей угроз (МУ) подсистем распределенной АСУ (***М1***)	- предназначен для кластерного анализа моделей угроз (МУ) для подсистем распределенных объектов информатизации *на этапах предпроектного исследования, внедрения и сопровождения проекта*; - используется *во всех подсистемах СЗИ*; - позволяет повысить *функциональную полноту методов и средств кластеризации элементов АС*, согласно мерам *ОДТ. 7* приказа ФСТЭК [128]; - позволяет снизить временные и стоимостные затраты на построение СЗИ.	- ПС «Метод кластеризации МУ для распределенной АСУ процессом транспортировки нефтегазового сырья» (***С1***); - ПС «Ранжирование рисков от угроз на основе ассоциативного принципа» (***С2***).
Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика (***М2***)	- предназначен для оперативного восстановления маршрутов и определения источников распространения вредоносной информации в распределенных АС и принятия решения по нейтрализации угрозы дальнейшего распространения вредоносного кода в КС; - используется *на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем антивирусной и сетевой защиты информации*; - позволяет повысить *функциональную полноту методов и средств антивирусной защиты*, согласно мерам *АВ3.1* и *СОВ.1* приказа ФСТЭК [128]; - позволяет повысить оперативность поиска данных о распространении вредоносной информации в сетевом трафике не менее чем в 2 раза за счет принципов ассоциативности и снизить риски от угрозы распространения вредоносного кода в КС не менее чем на 80 тыс. рублей	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (***С3***); - ПС «Комбинаторная семантическая модель генерации гипотез» (***С4***); - ПС «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (***С5***); - ПС «Моделирование сетевых атак на ресурсы вычислительных систем» (***С10***).
Метод определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС (***М3***)	- предназначен для определения резервного маршрута передачи информации при блокировании одного или нескольких участков основного канала связи; - используется *на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем обеспечения целостности и доступности технологической информации и сетевой защиты информации*; - позволяет повысить *функциональную полноту средств защиты доступности информации в АС*, согласно мерам *ЗИС. 6* и *ДНС.4* приказа ФСТЭК [128]; - позволяет снизить риски потери информации о состоянии объекта защиты не менее чем на 14% за счет использования принципов горячего резервирования и оперативного определения резервного маршрута передачи данных.	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (***С3***); - ПС «Маршрутизация сетевых потоков в режимах переключения на резервные каналы связи» (***С6***).

Продолжение таблицы Д.1

Метод мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций (***M4***)	- предназначен для контроля управляющих операций и транзакций в системе; - используется *на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем регистрации и учета, сетевой защиты информации*; - позволяет повысить *функциональную полноту методов и средств контроля действий пользователей в АС*, согласно мерам *АУД. 9* и *ОЦЛ. 5* приказа ФСТЭК [128]; - метод позволяет снизить риски от угрозы несанкционированных действий персонала АСУ не менее чем в 2 раза за счет контроля последовательности и очередности подачи управляющих команд	- ПС «Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP» (***C7***); - ПС «Моделирование сетевого трафика на базе протокола TCP/ModBUS» (***C9***); - устройство для контроля поведения пользователя (***C8***).
Метод обнаружения аномалий в сетевом трафике на основе дихотомического подхода (***M5***)	- предназначен для обнаружения аномалий в сетевом трафике КС; - используется *на этапах технического и рабочего проектирования, внедрения и сопровождения подсистемы сетевой защиты информации*; - позволяет повысить *функциональную полноту методов и средств анализа сетевого трафика*, согласно мерам *АУД. 5* и *СОВ.1* приказа ФСТЭК [128]; - метод обладает большей оперативностью и меньшей вычислительной сложностью на этапе распознавания аномалии не менее чем на порядок по сравнению с базовыми, в частности, нейросетевыми методами.	- ПС «Метод дихотомического распознавания аномалий в сетевом трафике» (***C11***).

Предложенная модель отличается применением принципов многоаспектности и интерактивности, что позволяет оперативно проводить системный анализ эффективности частных технических решений на всех стадиях разработки СЗИ и способствует повышению качества процесса разработки. В частности, представленные решения позволяют:

- автоматизировать процедуру обоснования и доказательства применимости результатов научных исследований;

- выявить избыточность или дефицит методов и средств защиты информации для конкретного этапа проекта;

- оценить эффективность результатов конкретных решений в совокупности других результатов разработок сложных проектов;

- оценить вклад разработанных методов в общий результат проекта.

Приложение Е. Характеристика программно-аппаратного комплекса мониторинга и анализа аномалий в КС «МАКС-1»

Программно-аппаратный комплекс «МАКС-1» предназначен для обнаружения аномалий и нейтрализации угроз безопасности информации по данным сетевого трафика КС АСУ.

Архитектура ПАК «МАКС-1» включает в себя следующие модули:

- модуль сбора и регистрации данных сетевого трафика;
- модуль анализа и обнаружения аномальных состояний сетевого трафика;
- модуль анализа аномалии и распознавания соответствующей угрозы;
- модуль принятия решений по нейтрализации угрозы;
- модуль моделирования и исследования аномальных состояний КС подсистем АСУ.

Характеристика программных и аппаратных средств ПАК МАКС-1 представлена в таблице Е.1.

Таблица Е.1 – Характеристика средств ПАК МАКС-1

Модуль ПАК МАКС-1	**Средство**	**Назначение**	**Среда разработки**	**Язык программирования**
Модуль сбора и регистрации данных сетевого трафика	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (***C3***) [11]	Прикладная программа предназначена для мониторинга сетевого трафика путем регистрации и оперативного поиска актуальной информации по данным аномальной активности компьютерной сети.	Delphi	Delphi
Модуль анализа и обнаружения аномальных состояний сетевого трафика	- ПС «Метод дихотомического распознавания аномалий в сетевом трафике» (***C11***) [37]	Прикладная программа предназначена для обнаружения аномалий в сетевом трафике АС на основе дихотомического подхода	Python	Python

Продолжение таблицы Е.1

Модуль ПАК МАКС-1	**Средство**	**Назначение**	**Среда разработки**	**Язык программирования**
Модуль анализа аномалии и распознавания соответствующей угрозы **Модуль принятия решений по нейтрализации угрозы**	- ПС «Комбинаторная семантическая модель генерации гипотез» (***C4***) [13];	Прикладная программа предназначена для построения маршрутов распространения вредоносного кода в КС и принятия решений по нейтрализации источников атаки	Visual Studio	C#
	ПС «Маршрутизация сетевых потоков в режимах переключения на резервные каналы связи» [5] (***C6***)	Программа предназначена для имитационного моделирования процессов маршрутизации сетевых потоков в режиме переключения на резервные каналы связи	VBA Excel	Visual Basic
	- ПС «Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP» [121] (***C7***)	Прикладная программа предназначена для анализа сетевого трафика КС в режиме реального времени с целью поиска нерегламентированных операций и транзакций пользователя.	Visual Studio	C#
	- устройство для контроля поведения пользователя [143] (***C8***)	Устройство предназначено для защиты АСУ от несанкционированного доступа на основе контроля действий пользователя.	-	-
Модуль моделирования и исследования аномальных состояний КС подсистем АСУ	- ПС «Метод кластеризации МУ для распределенной АСУ процессом транспортировки нефтегазового сырья» [8] (***C1***)	Прикладная программа предназначена для кластеризации угроз и частных моделей угроз для распределенной автоматизированной системы управления протяженным промышленным объектом.	Delphi	Delphi
	-ПС «Ранжирование рисков от угроз на основе ассоциативного принципа» [9] (***C2***)	Прикладная программа предназначена для ранжирования рисков информационной безопасности.	Visual Studio	C#
	- ПС «Моделирование сетевого трафика на базе протокола TCP/ModBUS» [10] (***C9***)	Программный комплекс предназначен для моделирования сетевого трафика в задачах обнаружения аномального профиля поведения оператора SCADA-системы.	Visual Studio	C#
	-ПС «Моделирование сетевых атак на ресурсы вычислительных систем» [17] (***C10***)	Программа предназначена для исследования функционирования вычислительных ресурсов в условиях сетевых атак	Delphi	Delphi
	- ПС «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» [39] (***C5***)	Прикладная программа предназначена для исследования процессов распространения вредоносного кода в КС.	Visual Studio	C#

Для разработки программного обеспечения использовались следующие среды:

- Microsoft Visual Studio — интегрированная среда разработки программного обеспечения и ряд других инструментов, позволяющая разрабатывать как консольные приложения, так и приложения с графическим интерфейсом, в том числе с поддержкой технологии Windows Forms, UWP а также веб-сайты, веб-приложения, веб-службы как в родном, так и в управляемом кодах для всех платформ, поддерживаемых Windows, Windows Mobile, Windows CE, .NET Framework, .NET Core, .NET, MAUI, Xbox, Windows Phone .NET Compact Framework и Silverlight;

- Embarcadero Delphi — интегрированная среда разработки ПО для Microsoft Windows, macOS, iOS и Android на языке Delphi;

- VBA Excel, VBA LibreOffice - интегрированные среды разработки, включающие специализированные средства для создания программ на языке Visual Basic;

- Python IDE — это программное обеспечение, предназначенное для создания, отладки и выполнения программ на языке программирования Python.

Выбор средств разработки программного обеспечения для каждого из методов обусловлен наличием библиотек и функций, необходимых для его реализации, и возможностью интеграции со средствами регистрации, мониторинга и анализа сетевого трафика.

Тестирование и апробация разработанных программных средств производились на базе процессоров Intel и AMD x64, на основе операционных систем, Windows (XP, 7, 8, 10, 11), Linux (РЕД ОС) с использованием Windows API – Wine. Апробация программных средств, проведенная в условиях лабораторного эксперимента с использованием сетевого стенда лаборатории кафедры ВТиЗИ Оренбургского государственного университета, программного комплекса SCADA TRACE MODE и эмуляторов промышленного сетевого протокола ModBus TCP, показала возможность их интеграции в реальную СЗИ в АСУ промышленными объектами.

Приложение Ж. Листинги программных средств

Фрагмент листинга программного средства «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности компьютерной сети»

Модуль записи данных в ассоциативную память

```
procedure TfrmMain.btn1Click(Sender: TObject);
var j,i, n, n1:integer; ok: array [1..8] of boolean; finalok: boolean;
begin
  if  strngrdgrd1.cells[0,1]<>'' then begin  n:=0;  // inc(r);
  for j:=1 to strngrdgrd1.rowcount-1 do   begin
  for i:=1 to 8 do ok[i]:=false;
      if form2.edt1.enabled=false then ok[1]:=true
      else if strngrdgrd1.cells[3,j]=form2.edt1.text then ok[1]:=true;
      if form2.edt2.enabled=false then ok[2]:=true
      else if strngrdgrd1.cells[5,j]=form2.edt2.text then ok[2]:=true;
      if form2.edt3.enabled=false then ok[3]:=true
      else if strngrdgrd1.cells[4,j]=form2.edt3.text then ok[3]:=true;
      if form2.edt4.enabled=false then ok[4]:=true
      else if strngrdgrd1.cells[6,j]=form2.edt4.text then ok[4]:=true;
      if form2.edt5.enabled=false then ok[5]:=true
      else if strngrdgrd1.cells[7,j]=form2.edt5.text then ok[5]:=true;
      if form2.edt6.enabled=false then ok[6]:=true
      else if strngrdgrd1.cells[8,j]=form2.edt6.text then ok[6]:=true;
      if form2.cbb1.enabled=false then ok[7]:=true
      else if strngrdgrd1.cells[1,j]=form2.cbb1.text then ok[7]:=true;
      if form2.edt7.enabled=false then ok[8]:=true
      else if strngrdgrd1.cells[2,j]=form2.edt7.text then ok[8]:=true;       finalok:=true;
      for i:=1 to 8 do finalok:=ok[i] and finalok;
      if finalOk  then begin
       inc(count);  if n=0 then  n:=j;  n1:=j;
       end;
  end;
```

```
for j:=1 to strngrdgrd1.rowcount-1 do
 if r<>0 then  begin
strngrd1.cells[1,r]:=inttostr(count); strngrd1.cells[2,r]:=strngrdgrd1.cells[8,n];
strngrd1.cells[3,r]:=strngrdgrd1.cells[8,n1]; strngrd1.cells[0,r]:=inttostr(r);
if count=0 then begin strngrd1.cells[2,r]:='#=#=#'; strngrd1.cells[3,r]:='#=#=#'end;
end;
mmo1.Lines.Add('Признак'+inttostr(r));
if form2.edt1.enabled=true then mmo1.Lines.Add('IP источника: '+form2.edt1.text);
if form2.edt2.enabled=true then mmo1.Lines.Add('IP приемника: '+form2.edt2.text);
if form2.edt3.enabled=true then mmo1.Lines.Add('Порт источника: '+form2.edt3.text);
if form2.edt4.enabled=true then mmo1.Lines.Add('Порт приемника: '+form2.edt4.text);
if form2.edt5.enabled=true then mmo1.Lines.Add('TTL (время жизни пакета): '+form2.edt5.text);
if form2.edt6.enabled=true then mmo1.Lines.Add('Время регистрации: '+form2.edt6.text);
if form2.cbb1.enabled=true then mmo1.Lines.Add('Тип пакета: '+form2.cbb1.text);
if form2.edt7.enabled=true then mmo1.Lines.Add('Размер пакета: '+form2.edt7.text);
mmo1.Lines.Add(''); count:=0;
Strngrdgrd1.RowCount:=Strngrdgrd1.RowCount-1;
end; end.
```

Модуль ассоциативного поиска данных об аномалии

```
procedure TfrmMain.strngrdgrd1DrawCell(Sender: TObject; ACol,
ARow: Integer; Rect: TRect; State: TGridDrawState);
Var   StringGrid: TStringGrid; finalok: boolean;
Can: TCanvas; i, j, ACol1: Integer; ok: array [1..8] of boolean;
begin
  StringGrid := Sender as TStringGrid; Can := StringGrid.Canvas; Can.Font := StringGrid.Font;
  if (ARow >= StringGrid.FixedRows) and (ACol >= StringGrid.FixedCols)
   then Can.Brush.Color := StringGrid.Color else Can.Brush.Color := StringGrid.FixedColor;
  if (r>0) then  begin
  if (flag=true) and (Arow>0) then
      begin
          if ((strngrdgrd1.cells[3,Arow]=strngrdgrd1.cells[5,Arow]) or
         (strtoint(strngrdgrd1.cells[4,Arow])=0) or
         (strtoint(strngrdgrd1.cells[6,Arow])=0) or
```

```
      (strtoint(strngrdgrd1.cells[2,Arow])<40))  then
      begin if  (Arow<>strngrdgrd1.RowCount-1) then Can.Brush.Color:=clRed; end;
      for ACol1:=0 to form1.strngrd1.colcount-1 do
      if ((strngrdgrd1.cells[1,Arow]=form1.strngrd1.cells[Acol1,0]) or
      (strngrdgrd1.cells[2,Arow]=form1.strngrd1.cells[Acol1,1]) or
      (strngrdgrd1.cells[3,Arow]=form1.strngrd1.cells[Acol1,2]) or
      (strngrdgrd1.cells[4,Arow]=form1.strngrd1.cells[Acol1,3]) or
      (strngrdgrd1.cells[5,Arow]=form1.strngrd1.cells[Acol1,4]) or
      (strngrdgrd1.cells[6,Arow]=form1.strngrd1.cells[Acol1,5]) or
      (strngrdgrd1.cells[7,Arow]=form1.strngrd1.cells[Acol1,6]) )  then
      begin Can.Brush.Color:=clRed; end;
  end else
begin
  for i:=1 to 8 do ok[i]:=false;
  if form2.edt1.enabled=false then ok[1]:=true
  else if strngrdgrd1.cells[3,Arow]=form2.edt1.text then ok[1]:=true;
  if form2.edt2.enabled=false then ok[2]:=true
  else if strngrdgrd1.cells[5,Arow]=form2.edt2.text then ok[2]:=true;
  if form2.edt3.enabled=false then ok[3]:=true
  else if strngrdgrd1.cells[4,Arow]=form2.edt3.text then ok[3]:=true;
  if form2.edt4.enabled=false then ok[4]:=true
  else if strngrdgrd1.cells[6,Arow]=form2.edt4.text then ok[4]:=true;
  if form2.edt5.enabled=false then ok[5]:=true
  else if strngrdgrd1.cells[7,Arow]=form2.edt5.text then ok[5]:=true;
  if form2.edt6.enabled=false then ok[6]:=true
  else if strngrdgrd1.cells[8,Arow]=form2.edt6.text then ok[6]:=true;
  if form2.cbb1.enabled=false then ok[7]:=true
  else if strngrdgrd1.cells[1,Arow]=form2.cbb1.text then ok[7]:=true;
  if form2.edt7.enabled=false then ok[8]:=true
  else if strngrdgrd1.cells[2,Arow]=form2.edt7.text then ok[8]:=true;
  finalok:=true;
  for i:=1 to 8 do finalok:=ok[i] and finalok;
  if ((finalOk) and (Arow<>0)and (Flag1=true)) then
  begin  Can.Brush.Color:=clRed;  end;
end;
```

```
  if (gdSelected in State) then
  begin
    Can.Font.Color := clHighlightText; Can.Brush.Color := clHighlight;
  end;
  Can.FillRect(Rect);
  Can.TextOut(Rect.Left+2,Rect.Top+2, StringGrid.Cells[ACol, ARow]);
end; end;
procedure TfrmMain.strngrdgrd1SelectCell(Sender: TObject; ACol,
  ARow: Integer; var CanSelect: Boolean);
  var num, i, j: integer; find,s: string; List: TStringList; p,q: cardinal ;
begin
if strngrdgrd1.Cells[0,1]<>'' then
begin
form3.show; form3.Mmo1.ScrollBars := ssVertical;
num:=strtoint(strngrdgrd1.Cells[0,Arow]); find:='Packet ID: '+inttostr(num);
s:=mmoreport.lines.text; j:=pos(find,s); delete(s,1,j);
j:=pos('================================================================',s);
form3.mmo1.Text:='P'+copy(s,1,j-1);
end; end;
procedure TfrmMain.strngrd1SelectCell(Sender: TObject; ACol, ARow: Integer;
  var CanSelect: Boolean);
 var num1, num2, k: string; i, j, l: integer; find,s: string; List: TStringList; p,q: cardinal ;
begin
if strngrd1.Cells[0,1]<>'' then
begin
form3.show; form3.Mmo1.ScrollBars := ssVertical;
num1:=strngrd1.Cells[2,Arow]; num2:=strngrd1.Cells[3,Arow]; find:=num1;
s:=mmoreport.lines.text; j:=pos(find,s);
for i:=j downto 1 do
if mmoreport.text[i]='=' then begin l:=i; break;  end;
delete(s,1,l);
j:=pos(num2,s);
form3.mmo1.Text:=copy(s,3,j+11);
end;  end.
```

Фрагмент листинга программного средства «Метод кластеризации моделей угроз для распределенной АСУ процессом транспортировки нефтегазового сырья»

Модуль кластеризации угроз и моделей угроз

```
procedure TForm1.Button3Click(Sender: TObject);
Var Ucl, Mcl: string; n, k, r, l, m: integer;
Begin if (flag1=true) and (flag4=false) then
begin
FillChar(MidleRiskU,Sizeof(MidleRiskU),False);
FillChar(MidleRiskM,Sizeof(MidleRiskM),False);
//рассчет классификационных кодов
SetLength(MidleRiskU,i);
 SetLength(MidleRiskM,j);
 memo1.Text:='Ранж. список значимых угроз:';
 memo2.Text:='Ранж. список МУ:';
 //рассчет средних значений рисков по угрозам
 for i:= 1 to stringgrid1.rowcount-3 do
 for j:= 1 to stringgrid1.colcount-3 do
 Begin
    MidleRiskU[i]:=MidleRiskU[i]+StrTofloat(stringgrid1.Cells[j,i]);
    stringgrid1.Cells[stringgrid1.colcount-2,i] := FloatTo-
Str(RoundTo(MidleRiskU[i]/(stringgrid1.colcount-3), -2));
        end;
 //рассчет средних значений рисков по моделям угроз
 for j:= 1 to stringgrid1.colcount-3 do
 for i:= 1 to stringgrid1.rowcount-3 do
 Begin
    MidleRiskM[j]:=MidleRiskM[j]+StrTofloat(stringgrid1.Cells[j,i]);
    stringgrid1.Cells[j, stringgrid1.rowcount-2] := FloatTo-
Str(RoundTo(MidleRiskM[j]/(stringgrid1.rowcount-3), -2));
  end;
  //рассчет классификационных кодов для угроз
  for i:= 1 to stringgrid1.rowcount-3 do
  for j:= 1 to stringgrid1.colcount-3 do
```

```
  stringgrid1.Cells[stringgrid1.colcount-1,i]:='';
 for i:= 1 to stringgrid1.rowcount-3 do
  for j:= 1 to stringgrid1.colcount-3 do
   if (strtofloat(stringgrid1.Cells[j,i])<strtofloat(stringgrid1.Cells[stringgrid1.colcount-2,i])) then
stringgrid1.Cells[stringgrid1.colcount-1,i]:= stringgrid1.Cells[stringgrid1.colcount-1,i]+'0'  else string-
grid1.Cells[stringgrid1.colcount-1,i]:= stringgrid1.Cells[stringgrid1.colcount-1,i]+'1';
  //рассчет классификационных кодов для моделей угроз
  for j:= 1 to stringgrid1.colcount-3 do   for i:= 1 to stringgrid1.rowcount-3 do
  stringgrid1.Cells[j,stringgrid1.rowcount-1]:= '';
  for j:= 1 to stringgrid1.colcount-3 do   for i:= 1 to stringgrid1.rowcount-3 do
  if (strtofloat(stringgrid1.Cells[j,i])<strtofloat(stringgrid1.Cells[j,stringgrid1.rowcount-2])) then
stringgrid1.Cells[j,stringgrid1.rowcount-1]:= stringgrid1.Cells[j,stringgrid1.rowcount-1]+'0'  else
stringgrid1.Cells[j,stringgrid1.rowcount-1]:= stringgrid1.Cells[j,stringgrid1.rowcount-1]+'1';
  /// кластеризация
StringGrid2.colWidths[0] := 100; StringGrid2.colWidths[1] := 200;
stringgrid2.Cells[0,0]:='Кластеры'; stringgrid2.Cells[1,0]:='Угрозы';
StringGrid3.colWidths[0] := 100; StringGrid3.colWidths[1] := 200;
stringgrid3.Cells[0,0]:='Кластеры'; stringgrid3.Cells[1,0]:='Модели угроз';
//кластеризация угроз
if flag=true then stringgrid2.rowcount:=1;
if flag<>true then
 begin  for i:= 1 to stringgrid2.rowcount-1 do stringgrid2.Cells[1,i]:='';
  k:=1;  stringgrid2.rowcount:=1;
 for i:= 1 to stringgrid1.rowcount-3 do
 Begin
 stringgrid2.rowcount:=stringgrid2.rowcount+1;
 stringgrid2.Cells[0,k]:='Кластер'+inttostr(k);
 for n:= 1 to stringgrid1.rowcount-1 do
 begin
 if stringgrid1.Cells[stringgrid1.colcount-1,i]=stringgrid1.Cells[stringgrid1.colcount-1,n] then
 stringgrid2.Cells[1,k]:= stringgrid2.Cells[1,k] + stringgrid1.Cells[0,n]+ ', ';
 end;   inc(k);  End;
l:=1; for i:= 1 to stringgrid2.rowcount-1 do
if stringgrid2.Cells[0,i]<>'' then begin  stringgrid2.Cells[0,i]:='Кластер'+inttostr(l);
 inc(l);  end;  end;
```

```
//кластеризация моделей угроз
 for i:= 1 to stringgrid3.rowcount-1 do stringgrid3.Cells[1,i]:='';
  k:=1;
 stringgrid3.rowcount:=1;
 for j:= 1 to stringgrid1.colcount-3 do
 Begin
 stringgrid3.rowcount:=stringgrid3.rowcount+1;
 stringgrid3.Cells[0,k]:='Кластер'+inttostr(k);
 for n:= 1 to stringgrid1.colcount-1 do
 begin
 if stringgrid1.Cells[j,stringgrid1.rowcount-1]=stringgrid1.Cells[n, stringgrid1.rowcount-1] then
 stringgrid3.Cells[1,k]:= stringgrid3.Cells[1,k] + stringgrid1.Cells[n,0]+ ', ';
 end;  inc(k);  End;
l:=1; for i:= 1 to stringgrid3.rowcount-1 do
if stringgrid3.Cells[0,i]<>'' then
begin  stringgrid3.Cells[0,i]:='Кластер'+inttostr(l);  inc(l);
 end;  flag2:=true; end;  end;
```

Модуль определения актуальных угроз и наиболее уязвимых подсистем

```
procedure TForm1.Button5Click(Sender: TObject);
Var i, j, k, n, m, s, sum, Count111: integer; strtemp, st: string; temp: array of string;
begin
if (flag<>true)and(flag4=false)and(flag1=true)and(flag2=true) then
begin
//определение актуальных угроз
StringGrid4.rowcount:=1;
 for i:= 1 to stringgrid1.rowcount-3 do
 begin
 stringgrid4.rowcount:=stringgrid4.rowcount+1;
 stringgrid4.Cells[0,i]:= stringgrid1.Cells[0,i];
 stringgrid4.Cells[1,i]:= stringgrid1.Cells[stringgrid1.colcount-1,i];
 end;
 //сортировка угроз
 n := StringGrid4.RowCount - 1;
```

```
SetLength(temp, n);
for i := 0 to n - 1 do
begin strtemp := '';
for j := 1 to Length(StringGrid4.Cells[1, i + 1]) do
begin
if StringGrid4.Cells[1, i + 1][j] = '1' then Inc(sum);
end;
strtemp := IntToStr(sum) + StringGrid4.Cells[1, i + 1];
temp[i] := strtemp; sum := 0; end;
for i := 0 to n - 1 do
begin for j := i to n - 1 do
begin
if temp[i] > temp[j] then
begin
strtemp := temp[i]; temp[i] := temp[j]; temp[j] := strtemp;
end; end; end;
for i := 0 to n - 1 do
begin StringGrid4.Cells[1, i + 1] := Copy(temp[i], 2, Length(temp[i])-1); end;
for i:=stringgrid4.rowcount-1 downto 1 do
Begin for k:=1 to stringgrid1.rowcount-3 do
if StringGrid4.Cells[1, i]=StringGrid1.Cells[StringGrid1.ColCount-1,k] then
begin count111 := 0;
  st := StringGrid4.Cells[1, i];
  for s := 1 to length(st)do if (st[s] = '1') then inc(count111);
  Memo1.Lines.Add((StringGrid1.Cells[0,k])+', k='+inttostr(count111));
end; end;
//определение уязвимых участков
StringGrid5.rowcount:=1;
 for i:= 1 to stringgrid1.colcount-3 do
 begin
 stringgrid5.rowcount:=stringgrid5.rowcount+1;
 stringgrid5.Cells[0,i]:= stringgrid1.Cells[i,0];
 stringgrid5.Cells[1,i]:= stringgrid1.Cells[i,stringgrid1.rowcount-1];
 end;
```

```
 //сортировка МУ
n := StringGrid5.RowCount - 1;
SetLength(temp, n);
for i := 0 to n - 1 do
begin strtemp := '';
for j := 1 to Length(StringGrid5.Cells[1, i + 1]) do
begin
if StringGrid5.Cells[1, i + 1][j] = '1' then Inc(sum);
end;
strtemp := IntToStr(sum) + StringGrid5.Cells[1, i + 1];
temp[i] := strtemp; sum := 0; end;
for i := 0 to n - 1 do
begin for j := i to n - 1 do
begin
if temp[i] > temp[j] then
begin strtemp := temp[i]; temp[i] := temp[j]; temp[j] := strtemp;
end; end; end;
for i := 0 to n - 1 do
begin StringGrid5.Cells[1, i + 1] := Copy(temp[i], 2, Length(temp[i])-1); end;
//вывод в мемо
if flag4=false then
begin for i:=stringgrid5.rowcount-1 downto 1 do
Begin for k:=1 to stringgrid1.colcount-3 do
if StringGrid5.Cells[1, i]=StringGrid1.Cells[k, StringGrid1.rowCount-1] then
begin
count111 := 0;
   st := StringGrid5.Cells[1, i];
   for s := 1 to length(st)do
    if (st[s] = '1') then inc(count111);
   Memo2.Lines.Add(StringGrid1.Cells[k, 0]+', k='+inttostr(count111));
end; end;
//удаление лишних строк из мемо
end;
end;
```

Приложение З. Справка о получении грантов

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Оренбургский государственный университет»
(ОГУ)

Управление научных исследований

г. Оренбург 18 июня 2019года

СПРАВКА

Настоящим подтверждаем, что аспирант Аэрокосмического института группы 17ИВТ(а)АТП **Абрамова Таисия Вячеславовна** входила в состав коллективов по выполнению научных проектов:

1. Система идентификации источников распространения вредоносной рассылки в распределенных информационно-вычислительных сетях на основе комбинаторной семантической модели генерации гипотез с ассоциативно-мажоритарным принципом принятия решения» (грант Оренбургской области в сфере научной и научно-технической деятельности, соглашение № 1, руководитель, объем финансирования: 50 тыс. руб., 2017 г.).

2. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков (грант РФФИ и правительства Оренбургской области № 18-47-560012, руководитель Аралбаев Т.З., исполнитель, объем финансирования: 500 тыс. руб., 2018 г.).

Начальник управления научных исследований И.И. Лисицкий

Рисунок 3.1 – Справка о выполнении научных проектов по теме исследования