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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Оренбург – 2024

Работа выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет» (ОГУ).

Научный руководитель: доктор технических наук, профессор **Аралбаев Ташбулат Захарович**

Официальные оппоненты:

Фрид Аркадий Исаакович, доктор технических наук, профессор, Закрытое акционерное общество "Республиканский центр защиты информации", зам. директора по научной работе

Соколов Александр Николаевич, кандидат технических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)», заведующий кафедрой защиты информации

Ведущая организация: Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук", г. Санкт-Петербург

Защита диссертации состоится 17 сентября 2024 года в 13^{00} часов на заседании диссертационного совета 24.2.479.07, на базе ФГБОУ ВО «Уфимский университет науки и технологий», по адресу: 450008, г. Уфа, ул. К. Маркса, д. 12.

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

Автореферат разослан «__»_____ 2024 года.

Ученый секретарь
диссертационного совета,
д-р техн. наук Вульфин Алексей Михайлович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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.., Соколова 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, в котором используются 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 обнаружения аномалий и распознавания состояния КС АСУ на основе данных монито-

ринга 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 амплитуд-

ными 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 промышленного 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.

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. 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении изложена краткая характеристика диссертации, обоснована актуальность темы, определены объект и предмет исследования, сформулированы цель и задачи работы, представлены положения, выносимые на защиту.

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 транспортировкой нефтегазового сырья одного из участков трубопровода Оренбургской области, топологическая схема которого представлена на рисунке 1.

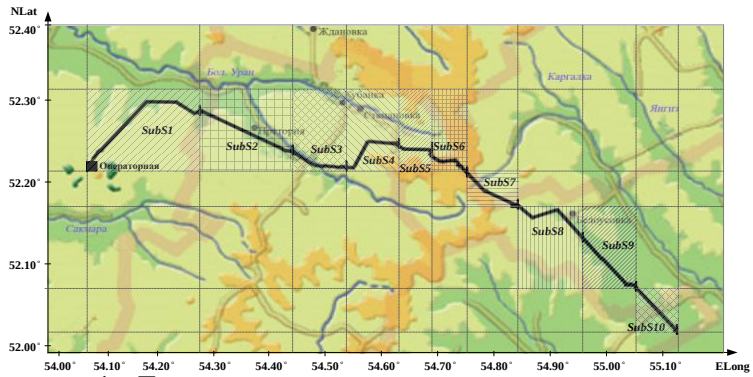

Рисунок 1 - Топологическая схема участка транспортного трубопровода

Особенностью распределенных АСУ ТП как объекта защиты является переменный в пространстве и времени характер угроз, что определяет специфичность требований к СЗИ. Каждая подсистема характеризуется индивидуальной моделью угроз (МУ), специфика которой определяется удаленностью оборудования от пунктов операторского и диспетчерского управления, рельефом местности, метеорологическими условиями и другими факторами. Это обуславливает исследование угроз БИ как на основе общей МУ, так и для каждой из подсистем АСУ. На рисунке 1 представлены 10 участков трубопровода, каждый из которых контролируется соответствующей подсистемой АСУ *(SubS1-SubS10*).

Общий вид целевой функции задачи защиты информации в АСУ представлен в выражении (1).

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

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 рассматриваемого класса АСУ характерно функционирование в условиях изменения риска и роста ущерба от атак за период времени, требующийся для обнаружения и достоверного распознавания связанных с ними аномалий. Стремление к снижению риска, необходимость обеспечения непрерывности ТП и оперативного принятия решений для предупреждения аварийных ситуаций обуславливают решение задач минимизации параметра $\boldsymbol{p}$ за счет повышения достоверности распознавания аномалии (в частности, снижения вероятностей ошибок 1-го и 2-го рода) и параметра $\boldsymbol{U}$ за счет повышения производительности (оперативности) методов и средств защиты при допустимых параметрах затрат для их достижения.

Анализ публикаций специалистов в исследуемой области, требований соответствующей нормативно-правовой базы и современных решений задачи ис-

следования показал возможности повышения оперативности и достоверности методов и средств обнаружения, распознавания аномальных состояний АСУ на основе исследования и интеллектуальной обработки сетевых информационных потоков и позволил разработать концепцию снижения рисков ИБ на объектах КИИ, определенную следующими аспектами. 1. Разработка метода кластерного анализа угроз и моделей угроз 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 в сетевом трафике АСУ, как проявлений инцидентов ИБ вследствие реализации угроз, на основе дихотомического принципа и разделяющей функции мажоритарного вида; для идентификации вида аномалии в АСУ за счет поиска ассоциативных связей между признаками и образами аномальных состояний и процессов. 3. Разработка алгоритмов, методик и программной реализации методов и средств обнаружения аномалий и нейтрализации угроз по данным сетевого трафика на основе ассоциативного подхода и мажоритарного принципа принятия решений.

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. Для анализа актуальных угроз и определения приоритетности их нейтрализации проведено исследование общей модели угроз для распределенной АСУ процессом транспортировки нефтегазового сырья, показавшее переменный в пространстве и времени характер угроз для каждой из подсистем АСУ. Это привело к необходимости дифференцированного подхода к построению СЗИ и исследования частных МУ, дополненных оценкой рисков, для подсистем, контролирующих отдельные участки технологического объекта (рис. 1). 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 на основе матрицы, представленной на рисунке 2.

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

Рисунок 2 - Матрица кластеризации угроз и частных моделей угроз для подсистем АСУ

Мера сходства при объединении объектов в кластеры определяется по совокупным бинарным классификационным кодам (КД)**.** Составляющие КД 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 позволяет судить о степени актуальности и приоритетности нейтрализации конкретной угрозы. 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.

Проведенный анализ статистических данных научных публикаций, материалов Интернет-источников, моделей угроз промышленных объектов АСУ транспортировкой нефтегазового сырья - с использованием разработанного метода кластеризации, актуальной методики оценки и реестра угроз ФСТЭК - выявил 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 АСУ, нерегламентированных действий персонала системы.

Под аномальными понимаются состояния КС, отраженные в СТ, соответствующие нерегламентированным режимам работы сетевых узлов, режимам обмена информацией между узлами и режимам передачи данных с нарушением заданных ограничений по защите информации. Характерным признаком проявления аномалий является нерегламентированные отклонения параметров СТ от «нормального» профиля, характеризующего штатную ситуацию работы АСУ. В качестве таких параметров могут быть использованы статистические характеристики сетевых сессий, например, изменение интенсивности сетевых пакетов определенных протоколов, четко дифференцируемые в промышленной сети.

Задача обнаружения аномалий в сетевом трафике АСУ, как проявлений инцидентов ИБ вследствие реализации угроз, в работе решается на основе последовательного разделения сетевых информационных потоков системы на «нормальный» и «аномальный» трафик на базе дихотомической модели (ДМ) с использованием разделяющей функции мажоритарного вида, аргументами которой являются амплитудные оценки спектров временных рядов сетевого трафика. Выбор информативных признаков для мажоритарной функции (МФ) определяется по величине рассогласования (разности) оценок математического ожидания амплитудных характеристик соответствующих гармоник спектров, рассчитанных для временных рядов СТ нормального и аномального состояния. В качестве разделяющей 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 состояния АС на этапе обучения модели.

Вычисление оценок вероятности *P(x)* принадлежности значения амплитудной оценки спектра *x* информативной гармоники к одному из образов *A* (аномального) или *B* (регламентированного состояния) производится с помощью формулы нормального распределения (функции Гаусса). Бинаризация значений аргументов X_i (i=1, n) для разделяющей функции осуществляется согласно выражениям (2):

$$X = 1, \text{если } P_A(x) \geq P_B(x), \qquad (2)$$
$$X = 0, \text{если } P_A(x) < P_B(x).$$

Формулы разделяющей функции от трех аргументов и правила принятия решения относительно распознаваемого состояния q_x представлены соответственно выражениями (3) и (4).

$$F(X_1, X_2, X_3) = X_1X_2 \vee X_1X_3 \vee X_2X_3 \vee X_1X_2X_3 \quad (3)$$

$$q_x \in A, \text{если } F(X_1, \dots, X_n) = 1;\ q_x \in B, \text{если } F(X_1, \dots, X_n) = 0; \quad (4)$$

Вычислительные эксперименты по исследованию моделей обнаружения аномальных состояний на базе нейронной сети, обученной по алгоритму Resilient Propagation, и мажоритарной функции с использованием экспериментальных и реальных временных рядов СТ с вирусными атаками показали, что при одинаковой достоверности функция мажоритарного вида обеспечивает на порядок выше оперативность обнаружения за счет меньшего числа применяемых информативных признаков, определенных на этапе обучения модели. Представленная модель положена в основу метода обнаружения аномалий в сетевом трафике АС на основе дихотомического подхода.

Идентификация аномального состояния АС в работе осуществляется с использованием обобщенной математической модели распознавания образов по данным временного ряда СТ, в которой: $Q=\{Q_1, Q_2, \dots, Q_j, \dots Q_N\}$ – множество классов распознаваемых аномальных состояний системы; q^x – состояние, подлежащее распознаванию; Q^* – класс состояний, к которому отнесено q^x; $P = \{p_1, p_2, \dots p_i, \dots, p_M\}$ – 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; $D=\{D_1, D_2, \dots, D_M\}$ – множество диапазонов изменения признаков для различных состояний; $V\{q^x, Q_j\}$ – 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; $\Phi\{<S^x>, Q_i\}$ – разделяющая функция для вычисления $V\{q^x, Q_j\}$. Математическое описание модели имеет следующий вид:

$$V\{q^x, Q_j\} = \Phi\{< S^x >, Q_j\}, j = 1, N; \quad (5)$$

$$\Phi\{< S^x >, Q_j\} = \sum_{i=1}^{M} v_{ij}\{< s_i{}^x >, Q_j\}, i = 1, M; \quad (6)$$

$$A\{<S^x, Q>\} = (v_{ij}); \quad (7)$$

$$v_{ij}\{< s_i{}^x >, Q_j\} = \begin{cases} 1, & \text{если} \quad < s_i{}^x > \in D_{ij}; \\ 0, & \text{если} \quad < s_i{}^x > \notin D_{ij}; \end{cases} \quad (8)$$

$$q^x \in Q^* \in Q: V\{q^x, Q^*\} \equiv max V\{q^x, Q_j\}, Q_j \in Q. \quad (9)$$

Выражение (9) представляет собой правило отнесения q^x к одному из образов множества Q по мажоритарному принципу. Представленная модель положена в основу методов обнаружения аномалий и нейтрализации актуальных угроз по данным сетевого трафика, в частности: метода для восстановления маршрутов распространения вредоносного кода, метода определения резервного маршрута пере-

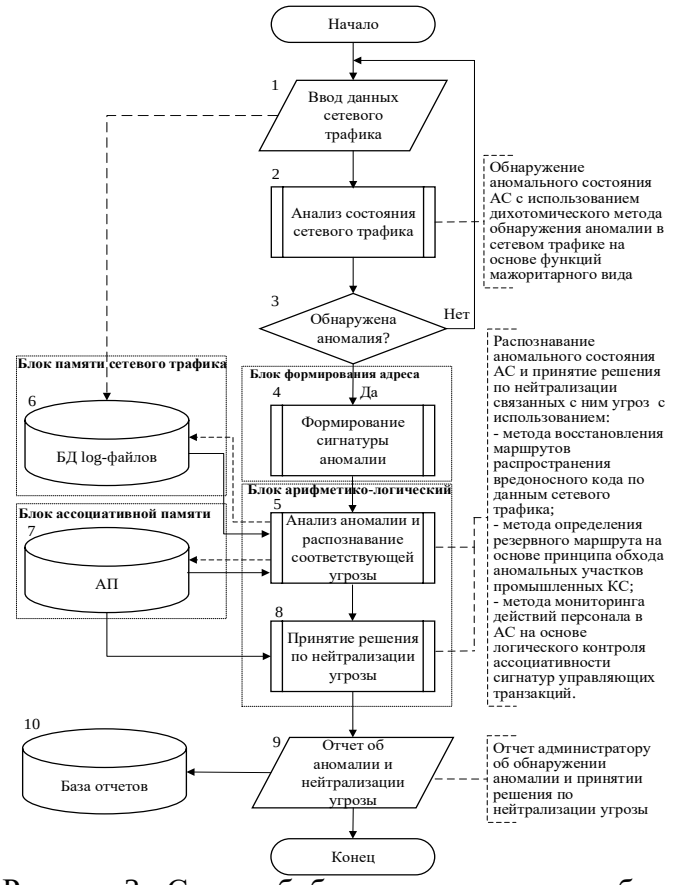

Рисунок 3 - Схема обобщенного алгоритма обнаружения аномалий и нейтрализации угроз по данным сетевого трафика

дачи данных в КС, метода для мониторинга нерегламентированных управляющих действий персонала АС.

В третьей главе представлены результаты разработки алгоритмов, методик и программно-аппаратных средств для реализации перечисленных методов. Схема обобщенного алгоритма обнаружения аномалий и нейтрализации угроз по данным сетевого трафика представлена на рисунке 3. В основу работы средств защиты положены принципы построения ассоциативных процессоров, в которых адресная часть ассоциативной памяти (АП) соответствует контролируемым признакам аномалии, информационная часть – характеристикам исследуемых образов, а структура и архитектура арифметико-логических блоков определяется назначением этих средств (рис. 3). Отличительной особенностью средств защиты является то, что признаки аномалии составляют адресную часть ассоциативной базы информации, а в информационной части содержатся сведения, необходимые для распознавания и нейтрализации соответствующей угрозы.

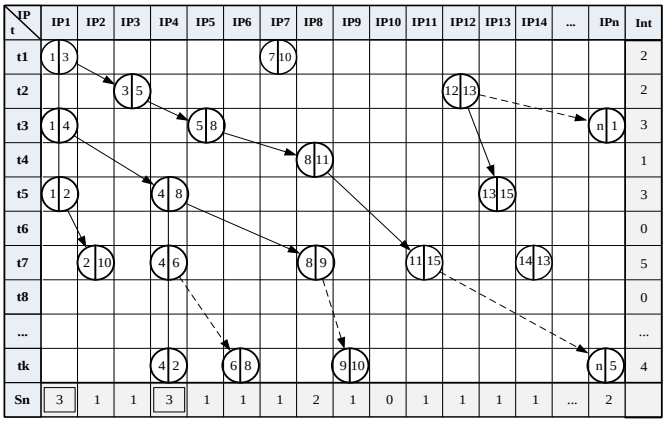

Рисунок 4 – Графо-аналитическая модель восстановления маршрутов распространения вредоносного кода

1. Метод и методика восстановления маршрутов распространения вредоносного кода в распределенной КС построены на базе графо-аналитической модели (рис. 4), где вершины графов, в отличие от традиционной матрицы смежности, обозначают адресную часть пакетов сетевого трафика в виде IP-адресов источников и получателей, ребра – направления их передачи. Модель позволяет описывать динамику маршрута по левой вертикальной 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. Адресом строки в АП (рис. 3) является адрес сетевого узла, а содержимое ячеек каждой строки включает адреса всех узлов, обменивающихся информацией с искомым, и время их взаимодействия. Источники распространения вируса определяются на основе мажоритарной функ-

ции (9) в арифметико-логическом блоке. Оперативное выявление источников и зараженных хостов позволяет принять превентивные меры по нейтрализации угрозы дальнейшего распространения вредоносного кода в КС (УБИ.1), такие как временная изоляция и восстановление работоспособности зараженных устройств.

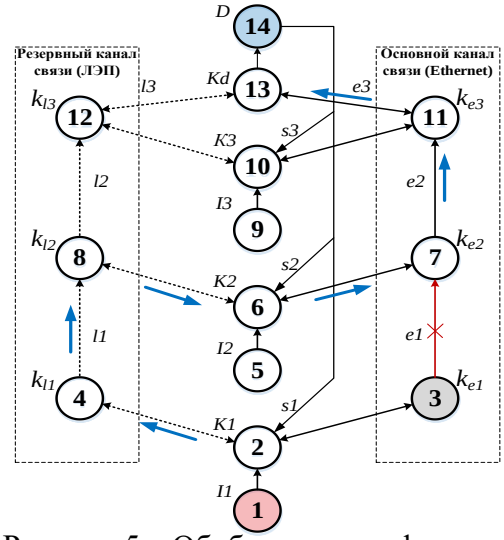

Рисунок 5 – Обобщенная графовая модель переключения потоков сетевого трафика в системе передачи данных с резервным каналом связи

2. Метод и методика определения резервного маршрута на основе принципа обхода аномальных участков промышленных КС построены на базе графовой модели переключения потоков сетевого трафика в системе передачи данных с резервным каналом связи (рис. 5), где *I* - источники информации, *D* - диспетчер, *K* – узлы переключения. В качестве резервного канала для обхода заблокированного участка используются линии передачи электроэнергии промышленного объекта, в данном случае – транспортного трубопровода. Отличительной особенностью методики является то, что адрес ячейки АП, по которому хранится адрес каждого следующего узла маршрута, формируется на основе адреса текущего узла и сигнала доступности от следующего узла. В случае доступности информация передается на следующий узел основного канала связи, иначе – резервного. В блоке арифметико-логическом (рис. 3) осуществляется сравнение адресов текущего и конечного узлов маршрута и, в случае их совпадения, процедура определения резервного маршрута завершается. В отличие от известных средств маршрутизации на основе сетевых протоколов, определение резервного маршрута производится за один цикл за время обращения к АП. Кроме того, предложенный принцип обхода недоступных участков позволяет снизить объем данных, передаваемых по резервному каналу. 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.

3. В основу метода и методики мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций положен принцип проверки соответствия порядка следования команд пользователя в виде сигнатур, составляющих адресную часть АП системы мониторинга, эталонам сигнатур, хранящимся в АП. Вариант организации потоков данных в ассоциативном процессоре в режиме мониторинга представлен на рисунке 6 в виде графовой модели, демонстрирующей процесс последовательного контроля операций пользователя АС ***O11 – O14*** по сигнатурам ***S*** на каждом узле обработки запроса ***M*** на вы-

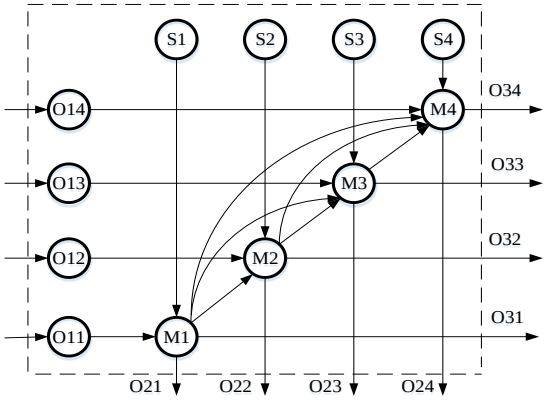

Рисунок 6 – Графовая модель контроля управляющих транзакций персонала

полнение операции. На рисунке 6: ***O31 - O34*** – сигналы легитимности выполнения операции и разрешения на выполнение следующей операции, ***O21 – O24*** – сигналы блокировки операций. В блоке арифметико-логическом (рис.3) проверяется последовательность и соответствие кодов всех операций в адресной части и в ячейке АП. В случае несоответствия - осуществляется блокирование операций и транзакций пользователей, не соответствующих политикам безопасности, что позволяет нейтрализовать угрозы, связанные с нерегламентированными действиями персонала АС. Отличительной особенностью методики является оперативное распознавание и анализ операций пользователя, как взаимосвязанной последовательности образов, что снижает вероятность принятия неправомерных управляющих решений.

Разработан комплекс программных и аппаратных средств [8, 9, 18, 24, 27, 28], реализующих представленные методы.

Четвертая глава посвящена экспериментальной оценке эффективности результатов исследований и разработке рекомендаций их практического применения на примере характеристик АСУ транспортировкой нефтегазового сырья одного из месторождений Оренбургской области. Эффективность оценивалась по критерию снижения уровня риска ИБ (согласно МУ) по отношению к базовым СЗИ с учетом затрат на реализацию средств защиты на основе разработанных методов.

Сопоставительный анализ методов реализации дихотомического разделения состояний сетевого трафика на основе мажоритарной и нейросетевой моделей, проведенный на основе натурного эксперимента с применением разработанной программы [24] и MS Excel с аналитической надстройкой Neural Excel, показал, что при одинаковых результатах по достоверности (ошибки первого и второго рода не превышали 5%) разработанный метод обладает меньшей вычислительной сложностью алгоритма на этапе распознавания аномалии не менее чем на порядок.

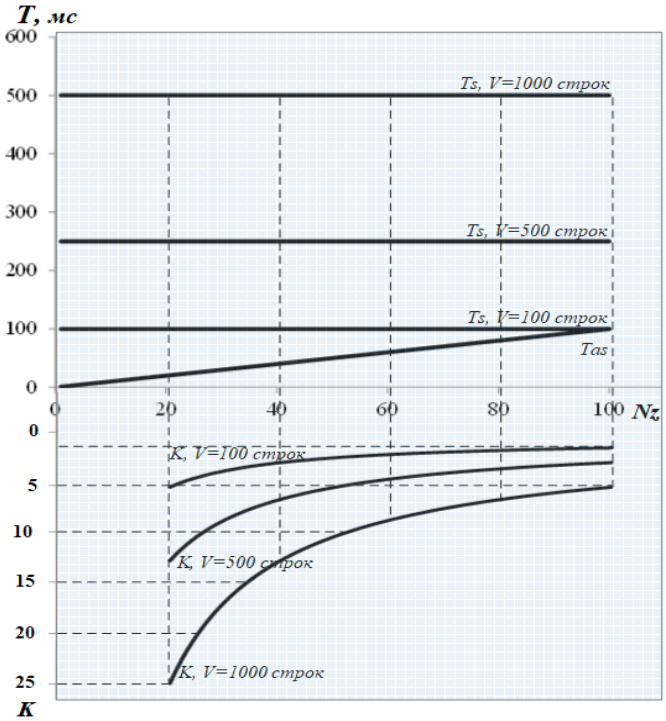

Рисунок 7 - Графики зависимости времени восстановления маршрутов распространения вируса в базовом (*Ts*) и новом (*Tas*) вариантах от числа зараженных хостов *Nz* при различных объемах *V* лог-файла СТ, где *K=Ts/Tas*

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, общим объемом около 1 Гб. Эксперимент по оценке ущерба от распространения вируса-шифровальщика показал возможность снижения рисков от угрозы УБИ.1 для исследуемой АСУ не менее чем на 80 тыс. рублей за счет оперативного обнаружения источников и исключения возможности дальнейшего распространения вредоносного кода в КС. На рисунке 7 представлены номограммы, демонстрирующие увеличение оперативности по-

иска 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.

Вычислительный эксперимент, проведенный с учетом реальных характеристик участка исследуемой АСУ (рис. 1), показал, что при использовании разработанного *метода определения резервного маршрута передачи данных* наблюдается снижение риска потери информации о состоянии технологического объекта не менее чем на 0,7 Мбит, что составляет 14% технологической информации, необходимой для управления системой. Размер предотвращенного ущерба зависит от назначения потерянной информации.

В результате оценки эффекта от применения *метода мониторинга действий персонала в АС*, проведенной на модельных данных на примере контроля команд диспетчера по управлению давлением в трубопроводе, выявлено снижение риска от угроз несанкционированных действий пользователей АСУ не менее чем в 2 раза. Эффект достигается за счет контроля последовательности и очередности подачи управляющих команд, что значительно снижает вероятность нерегламентированных транзакций. Оценка затрат на построение средств защиты показала, что при одинаковых функциональных и технических характеристиках суммарные затраты на разработку программных средств для реализации методов в 4 раза ниже стоимости коммерческих аналогов, в частности KICS for Networks.

В результате апробации разработанных программных средств, проведенной 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, выявлено повышение оперативности и достоверности распознавания аномалий в СТ как промышленного, так и корпоративного уровней КС АСУ ТП и разработаны рекомендации по применению результатов диссертационной работы в СЗИ. Разработанный комплекс программных средств позволяет повысить функциональную полноту существующих решений по ИБ в подсистемах сетевой и антивирусной защиты, учета действий персонала и защиты доступности технологической информации и может быть использован в SOC, SIEM-системах и системах поддержки и принятия решений в подразделениях ИБ 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», АНО ДО «Просвещение» (г. Оренбург).

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

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; 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 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 ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Монографии

1 Оптимизация методов контроля технического состояния распределенных автоматизированных систем / Т.З. Аралбаев, Г.Г. Аралбаева, Т.В. Абрамова [и др.]. – Оренбург : Оренбургский государственный университет, 2019. – 160 с.

Статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК

2 Аралбаев, Т.З. Комбинаторная семантическая модель генерации гипотез / Т.З. Аралбаев, Т.В. Абрамова, Р.Р. Галимов // Информация и безопасность. – 2016. – Т. 19, № 3. – С. 379-384.

3 Выбор базовой функции при автоматизированной идентификации временных рядов на основе ассоциативно-мажоритарного подхода / Т.З. Аралбаев, Т.В. Абрамова, Р.Р. Галимов [и др.] // Вестник ИжГТУ имени М.Т. Калашникова. – 2018. – Т. 21, № 4. – С. 194-199. – DOI 10.22213/2413-1172-2018-4-194-199.

4 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.

5 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.

Публикации в отечественных журналах из перечня изданий ВАК, включенных в международную базу Scopus

6 Aralbaev, T.Z. Network Traffic Monitoring on the Basis of Sequential and Associative–Sequential Search Principles / T.Z. Aralbaev, T.V. Abramova // Russian Engineering Research. – 2018. – Vol. 38, No. 5. – P. 381-383. – DOI 10.3103/S1068798X18050039.

Другие публикации по теме диссертации

7 Аралбаев, Т.З. Особенности оперативного поиска информации о сетевом трафике по первичным данным аномальной активности компьютерной сети / Т.З. Аралбаев, Т.В. Абрамова // Информационное противодействие угрозам терроризма. – 2015. – № 24. – С. 76-81.

8 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.

9 Галимов Р.Р., Аралбаев Т.З., Абрамова Т.В., 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.

10 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.

11 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 развития образования, науки и культуры : материалы Всерос. науч.-метод. конф. - Оренбург: ОГУ, 2018. − С. 1719-1725.

12 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 октября 2018 года. – Санкт-Петербург: ГНИИ «Нацразвитие», 2018. – С. 127-130.

13 Аралбаев, Т.З. Контроль пользователя в АСУ ТП на основе принципов ассоциативности и мажоритарности / Т.З. Аралбаев, Т.В. Абрамова // Актуальные задачи фундаментальных и прикладных исследований : Материалы Международной научно-практической конференции, Оренбург, 20 ноября 2018 года. – Оренбург: Оренбургский государственный университет, 2018. – С. 37-40.

14 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.

15 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.

16 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.

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., 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.

19 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 : Материалы Всероссийской научно-методической конференции (с международным участием). – Оренбург: ОГУ, 2020. – С. 1389-1395.

20 Абрамова, Т.В. Анализ пространственно-временной модели угроз для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья / Т. В. Абрамова, Т. З. Аралбаев // Вестник Уфимского государственного авиационного технического университета. – 2020. – Т. 24, № 1(87). – С. 76-84.

21 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 XVII Международной научно-практической конференции. - 2020. – С. 181-185.

22 Абрамова Т.В. Номограммный метод анализа эффективности ассоциативно-последовательного подхода в задаче распознавания сценария вирусной атаки // Сборник статей Международной научно-практической конференции «ОБЩЕСТВО - НАУКА - ИННОВАЦИИ» (Калуга, 17.02.2021 г.). – Уфа: OMEGA SCIENCE, 2021. – С. 30-39

23 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 культуры : Сборник материалов Всероссийской научно-методической конференции. – Оренбург: Оренбургский государственный университет, 2022. – С. 1245-1249.

24 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.

25 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.

26 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 (11 апреля 2023 г., г. Уфа). / В 2 ч. Ч.1 – Уфа: Изд. НИЦ Вестник науки, 2023. – С. 54 – 62.

Патенты и свидетельства о регистрации программ для ЭВМ

27 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. - 2018.

28 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"..- № 2022661790 заявл. 21.06.2022 опубл. 27.06.2022. – 2022.

Диссертант  Т.В. Абрамова