ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.479.07 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 17.09.2024 № 7

О присуждении Абрамовой Таисии Вячеславовне, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков» по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 02.07.2024 г., протокол № 5 диссертационным советом 24.2.479.07 на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации, 450008, г. Уфа, ул. К. Маркса, 12, созданного приказом Министерства образования и науки Российской Федерации от 24.03.2023 г. № 542/нк (с изменениями приказами от 18.12.2023 г. № 2368/нк и от 11.06.2024 г. № 581/нк).

Соискатель Абрамова Таисия Вячеславовна 22 марта 1993 года рождения, работает старшим преподавателем кафедры вычислительной техники и защиты информации Института математики и информационных технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» Министерства науки и высшего образования Российской Федерации.

В 2015 г. окончила бакалавриат ФГБОУ ВПО «Оренбургский государственный университет» по направлению подготовки 10.03.01 «Информационная безопасность». В 2017 г. окончила магистратуру ФГБОУ ВО «Оренбургский государственный университет» по направлению подготовки 09.04.01 «Информатика и вычислительная техника». В 2021 г. окончила аспирантуру ФГБОУ ВО «Оренбургский государственный университет» по направлению подготовки 09.06.01 «Информатика и вычислительная техника».

Диссертация выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет» Министерства науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, профессор, профессор кафедры вычислительной техники и защиты информации Аралбаев Ташбулат Захарович, ФГБОУ ВО «Оренбургский государственный университет».

Официальные оппоненты:

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

2. 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 **дали положительные отзывы о диссертации.**

Ведущая организация - Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук", г. Санкт-Петербург, в своем положительном отзыве, подписанным Главным научным сотрудником, заведующим лабораторией Проблем компьютерной безопасности, д.т.н, профессором, заслуженным деятелем науки РФ Котенко Игорем Витальевичем, ведущим научным сотрудником лаборатории Проблем компьютерной безопасности, к.т.н., доцентом, Чечулиным Андреем Алексеевичем, утвержденным директором СПб

ФИЦ РАН, д.т.н., профессором РАН Ронжиным Андреем Леонидовичем, указала, что диссертация Абрамовой Таисии Вячеславовны на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований разработаны методы, модели, алгоритмы и методики обнаружения аномалий и нейтрализации угроз на основе мониторинга сетевых информационных потоков, применение которых позволяет снизить риски информационной безопасности в компьютерных сетях распределенных АСУ ТП.

Диссертация соответствует требованиям пунктов 9, 10, 11, 13, 14 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (в редакции от 25.04.2024 г.), а её автор – Абрамова Таисия Вячеславовна - заслуживает присуждения ей ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Соискатель имеет более 50 опубликованных работ, из них по теме диссертации – 43, в том числе 4 статьи в научных изданиях из Перечня рецензируемых научных изданий (3 издания – К2, 1 издание – К3), рекомендованных ВАК, 1 научная публикация в издании, включенном в базу Scopus (Q2), 26 статей в других изданиях, 1 коллективная монография, 1 учебно-методическое пособие. Получен 1 патент и 9 свидетельств о регистрации программ. 4 публикации выполнены соискателем единолично, остальные – при непосредственном участии соискателя.

Общий объем публикаций – 21,5 п.л., авторский вклад – 11,5 п.л.

Наиболее значимые работы по теме диссертации:

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.

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.

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.

7 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.

8 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.

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации; соискатель ссылается на авторов и источники заимствования.

На диссертацию и автореферат поступили **положительные** отзывы, в которых содержатся ряд замечаний:

- ведущей организации Федерального государственного бюджетного учреждения науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук", г. Санкт-Петербург. *Замечания:* 1. Для четвертого положения, выносимого на защиту, касающегося результатов оценки эффективности предложенных решений, во введении отсутствует описание научной новизны. 2. Список литературы содержит достаточно небольшое количество публикаций на иностранных языках. Учитывая, что представленная в диссертации проблема также активно исследуется на международном уровне, целесообразно было бы рассмотреть больше зарубежных источников, чтобы обеспечить более широкий обзор и учесть достижения мировой науки в данной области. 3. На странице 131 представлен численный эксперимент для оценки возможного ущерба от вирусной атаки. При этом, для оценки ущерба используется стоимость установленного на АРМ ПО (таблица 4.2). Необходимо отметить, что заражение АРМ вирусом-шифровальщиком не уничтожает лицензии на ПО, а лишь временно делает его недоступным. ПО можно переустановить с использованием тех же лицензий без покупки новых. Более значимым является ущерб от нарушения бизнес-процессов, который далеко не всегда зависит от стоимости конкретного ПО. 4. В Приложении Г в разделе «Оценка экономического эффекта от применения разработанных методов» сравнение Kaspersky Industrial CyberSecurity for Networks с разработанным подходом выглядит некорректным. Сравнивать стоимость коммерческой лицензии и собственную разработку недостаточно обоснованно, поскольку не учитывается различие в функциональности и масштабируемости решений. Продукт от Kaspersky, вероятно, обладает более широкой функциональностью и зрелостью, что требует учитывать не только стоимость, но и качество защиты, поддержку, обновления и другие аспекты, которые влияют на реальную экономическую эффективность. 5. Оформление отдельных элементов диссертационной работы не соответствует ГОСТ Р 7.0.11-2011, а оформление библиографических записей не полностью соответствует ГОСТ 7.1 и ГОСТ 7.80.

- официального оппонента доктора технических наук, профессора Фрида Аркадия Исааковича, заместителя директора по научной работе, ЗАО

«Республиканский центр защиты информации». *Замечания*: 1. В главе 1, на мой взгляд, к перечисленным основным видам рисков следовало бы добавить риски от разрушения инфраструктуры, т.к. исследуемые системы относятся к системам критической информационной инфраструктуры (КИИ). 2. Неясно, как учитывается при оценке рисков взаимодействие участков сети, так как наверняка существует влияние изменения состояния одних участков сети на состояние других. 3. Неясно, как учитывается при оценке рисков возможность одновременного негативного воздействия на нескольких участках сети. 4. На рис. 2.4 приведен пример классификационного кода угрозы 1011100. Неясно, как получилось это выражение, поскольку не указаны исходные данные для его построения. 5. На стр. 69 предлагается проводить бинаризацию значений аргументов X_i по правилам (2.8, 2.9). Хотя математически эти неравенства не оставляют места для сомнений в принятии решений, при учете неточностей измерений и помех может возникнуть зона неопределенности, приводящая к ошибкам первого и второго рода. Как учитывать это обстоятельство? 6. На стр. 80 говорится, что дихотомический подход позволяет повысить оперативность и достоверность определения аномалии. По сути, дихотомический подход – это округление, и вряд ли эта операция может повысить достоверность. 7. Разработанный метод кластеризации угроз и моделей угроз БИ для подсистем распределенных объектов КИИ ориентирован на АСУ ТП транспортировки нефтегазового сырья. В тексте диссертации недостаточно четко показана возможность распространения полученных результатов на распределенные технические системы иной природы. 8. Замечания по представлению работы: нет списка условных обозначений, часто одни и те же понятия сопровождаются уже введенными ранее аббревиатурами, есть повторы.

- официального оппонента кандидата технических наук, доцента, Соколова Александра Николаевича, заведующего кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». *Замечания*: 1. В главе 1 диссертации автор рассматривает целевую функцию задачи защиты информации, в определении которой фигурируют элементы p_{ij} и U_{ij}, после чего говорит о минимизации

параметров p и U, явно их не определяя. Видимо, речь идет о матрицах P и U, составленных из этих элементов. Из текста не ясно, что понимается под минимизацией матрицы, может быть, минимизация ее элементов? 2. В главе 2 диссертации говорится, что вычисление вероятности $P(x)$ производится с помощью функции Гаусса. На основании чего можно считать, что в этом случае имеет место нормальное распределение? 3. Экспериментальная оценка эффективности результатов исследований проводилась на примере характеристик АСУ ТП транспортировки нефтегазового сырья. Вместе с тем, в работе не уделено достаточно внимания вопросам эффективности предложенных решений в составе СЗИ других промышленных объектов. 4. В диссертации недостаточно подробно раскрыт вопрос выбора и обоснования инструментария и средств разработки программных решений. 5. В главе 4 представлено большое количество иллюстративного материала, часть которого можно перенести в Приложение без потери информативности и понимания результатов исследования.

Получено **семь положительных** отзывов на автореферат:

1. **ФГБОУ ВО «Поволжский государственный технологический университет»** (г. Йошкар-Ола), доктор технических наук, профессор, заведующая кафедрой информационной безопасности, **Сидоркина Ирина Геннадьевна.** Замечание: в содержании текста автореферата отсутствуют сведения о возможностях использования результатов работы применительно к квантовым компьютерным сетям.

2. **ФГБОУ ВО «Ижевский государственный технический университет имени М.Т. Калашникова»** (г. Ижевск), доктор технических наук, доцент, заведующий кафедрой информационной безопасности, **Вологдин Сергей Валентинович**. Замечания: в тексте автореферата не представлено обоснование выбора ассоциативно-мажоритарной модели для идентификации аномального состояния автоматизированных систем; в автореферате не раскрыты детали внедрения предложенных решений в подсистемы сетевой защиты, учета действий персонала и защиты доступности технологической информации.

3. **ФГБОУ ВО «Тамбовский государственный технический**

университет» (г. Тамбов), доктор технических наук, профессор, профессор кафедры информационных систем и защиты информации, **Алексеев Владимир Витальевич**. Замечания: 1. В тексте автореферата при описании третьей главы диссертации представлена блок-схема алгоритма обнаружения аномалий и нейтрализации угроз по данным сетевого трафика, то время как в результатах работы говорится о трех разработанных методах и алгоритмах. 2. Экспериментальная оценка эффективности результатов исследований проводится на примере характеристик АСУ транспортировкой нефтегазового сырья одного из месторождений Оренбургской области, в этой связи было целесообразно представить в автореферате хотя бы обобщенную структуру КС этой системы, для получения наглядного представления о ней.

4. **Общество с ограниченной ответственностью «Уральский центр систем безопасности»** (г. Екатеринбург), кандидат технических наук, директор корпоративного центра мониторинга информационной безопасности средств и систем информатизации, **Мушовец Константин Владимирович**. Замечания: 1. В автореферате не раскрыты подробно детали реализации комплекса разработанных программных средств. 2. Не приводятся характеристики требуемых вычислительных ресурсов для применения результатов работы.

5. **ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова» (г. Магнитогорск)**, доктор технических наук, доцент, заведующая кафедрой информатики и информационной безопасности, **Баранкова Инна Ильинична**. Замечания: 1. В тексте автореферата явно не указано, какие меры обеспечения безопасности значимого объекта реализуют разработанные решения, согласно требованиям Приказа ФСТЭК № 239. 2. В автореферате приводится математическая модель, положенная в основу метода обнаружения аномального состояния распределенных АС на базе дихотомического подхода, но не приведена блок-схема соответствующего алгоритма, что позволило бы получить наглядное представление о его работе.

6. **ФГБОУ ВО «Пензенский государственный университет»** (г. Пенза), доктор технических наук, профессор, профессор кафедры №1 Военного учебного

центра имени Героя Советского Союза полковника Шишкова В.Ф. **Малыгин Александр Юрьевич**. Замечания: 1. Обозначения географических объектов и надписи на рисунке 1 автореферата выполнены слишком мелко, что затрудняет его читабельность. 2. При оценке снижения уровня риска недостаточно ясен механизм работы получения численных значений вероятностей (глава 4).

7. **ФГБОУ ВО «Оренбургский государственный аграрный университет»** (г. Оренбург), кандидат технических наук, доцент, доцент кафедры цифровых систем обработки информации и управления Тарасов Андрей Дмитриевич. Замечания: 1. Частое использование коротких - двухбуквенных аббревиатур затрудняет чтение. Например, безопасность информации (БИ), компьютерные сети (КС), сетевой трафик (СТ), модели угроз (МУ). 2. Не раскрыт состав разработанных программных средств, не указаны используемые языки программирования. 3. Сказано, что разработанный комплекс программных средств позволяет повысить функциональную полноту существующих решений по ИБ, при этом не уточняется, о каких из перечисленных в работе функциях идет речь.

Выбор официальных оппонентов и ведущей организации обосновывается их достижениями в данной отрасли наук, наличием публикаций в соответствующей сфере исследования и способностью определить научную и практическую ценность диссертации. Ведущая организация и оппоненты не имеют совместных проектов и публикаций с соискателем.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– **предложены**:

- 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

автоматизированной системы управления технологическими процессами (АСУ ТП), а также применять принципы типового проектирования при построении системы защиты информации (СЗИ) для АСУ с распределенной топологией;

- метод построения математических и имитационных моделей для обнаружения аномалий и распознавания состояния компьютерной сети (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;

– **разработаны** алгоритмы, методики и осуществлена 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 безопасности информации (БИ);

– **экспериментально доказана** эффективность и целесообразность применения разработанных методов, моделей, алгоритмов и методик, а также программно-аппаратных средств обнаружения аномалий и нейтрализации угроз БИ в распределенных АСУ ТП, что позволяет повысить производительность, достоверность, универсальность средств и снизить риски от угроз БИ, в частности: от угрозы распространения вредоносного кода в КС; от угрозы

несанкционированных действий персонала АСУ; риск потери информации о состоянии объекта защиты.

Теоретическая значимость исследования обоснована тем, что:

– применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) **использованы** методы теории информационной безопасности, теории вероятности, теории принятия решений, теории распознавания образов, теории графов, методы математического, имитационного моделирования;

– **изложены** аргументы и факты, подтверждающие актуальность разработки методов, моделей и алгоритмов обнаружения аномалий и нейтрализации угроз БИ в распределенных АСУ, отличительной особенностью которых является применение дихотомического и ассоциативно-мажоритарного подходов с использованием интеллектуальной обработки данных сетевого трафика, что позволяет повысить оперативность и достоверность обнаружения аномалий в сетевом трафике и идентификации аномальных состояний АСУ.

– **раскрыты** противоречия, связанные с применением известных методов и средств обнаружения аномалий и нейтрализации угроз БИ по данным сетевого трафика, недостаточно полно учитывающих специфику КС распределенных АСУ ТП и не позволяющих оперативно и достоверно обнаруживать и идентифицировать их аномальные состояния, и, как следствие, принять превентивные меры по нейтрализации соответствующих угроз;

– **изучены** особенности структурно-функциональной организации распределенной АСУ ТП как объекта защиты, а также требования регуляторов и современные решения в области защиты информации на объектах критической информационной инфраструктуры (КИИ), на основании чего сделан вывод о необходимости совершенствования существующих СЗИ и разработки новых высокопроизводительных и достоверных методов и средств обнаружения аномалий и нейтрализации соответствующих угроз БИ с учетом современных требований;

– **проведена модернизация** известных методов защиты информации с использованием моделей и алгоритмов кластерного описания угроз и развития методов обнаружения аномалий и нейтрализации угроз БИ на основе дихотомического и ассоциативно-мажоритарного подходов с применением интеллектуальной обработки данных сетевого трафика.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– **разработаны и внедрены** в ООО «Уральский центр систем безопасности», в учебный процесс ФГБОУ ВО «Оренбургский государственный университет», АНО ДО «Просвещение» (г. Оренбург) и переданы для ознакомления и внедрения в ООО «Газпромнефть-Оренбург»: алгоритм и программа кластеризации угроз и МУ для распределенной АСУ процессом транспортировки нефтегазового сырья, алгоритмы и программы для моделирования, обнаружения аномалий и нейтрализации угроз БИ в распределенных АСУ 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»;

– **определены** рекомендации по практическому применению результатов диссертационной работы в распределенных АС на примере АСУ ТП транспортировки нефтегазового сырья;

– **разработаны** алгоритмы, методики и осуществлена программно-аппаратная реализация методов и средств обнаружения аномалий и нейтрализации угроз БИ по данным сетевого трафика, позволяющие оперативно выявлять маршруты и источники распространения вредоносной информации в КС и принимать превентивные меры по нейтрализации угрозы дальнейшего распространения, 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, снизить риски от угроз нерегламентированных управляющих воздействий на систему;

– **представлены** результаты экспериментальной оценки и показатели эффективности применения разработанных методов, подтверждающие практическую значимость предложенных решений.

Оценка достоверности результатов исследования выявила:

– **для экспериментальных работ** использованы разработанные программные средства, программный комплекс SCADA TRACE MODE и эмуляторы промышленного сетевого протокола ModBus TCP, сетевой стенд лаборатории кафедры ВТиЗИ Оренбургского государственного университета;

– **теоретическая часть работы** базируется на известных, проверяемых и апробированных данных, фактах и согласуется с опубликованными ранее работами других авторов, а также экспериментальными данными по теме диссертации;

– **идея базируется** на результатах анализа современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой и смежных областях, обобщении опыта применения методов защиты информации на основе интеллектуальной обработки данных сетевого трафика;

– **использованы** экспериментальные данные сетевого трафика, данные трафика сервера Оренбургского государственного университета и датасеты с вирусными атаками в промышленных КС; анализ результатов экспериментальной оценки эффективности показал, что предложенные решения по достоверности не уступают аналогичными, при этом обладают большей оперативностью и меньшей вычислительной сложностью на этапе распознавания образа;

– **установлено** совпадение авторских результатов с результатами решения задач обнаружения аномалий и нейтрализации угроз в распределенных АСУ ТП, представленными в независимых источниках, при улучшении количественных показателей эффективности результатов диссертационной работы.

Личный вклад соискателя состоит: в постановке целей и задач, анализе современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой; разработке методов, моделей, алгоритмов, методик и участии в разработке

программно-аппаратных средств, представленных в диссертационной работе; в организации и проведении экспериментов по оценке эффективности результатов исследования; получении и интерпретации результатов на каждом этапе, их апробации и подготовке основных публикаций по выполненной работе.

Диссертационный совет пришел к выводу о том, что в диссертации:

- соблюдены установленные Положением о порядке присуждения ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени кандидата технических наук;

- отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации;

- соискатель ссылается на авторов и источники заимствования;

- оригинальность диссертационной работы составляет 86,1 %.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. На слайде № 11 вычисление оценки вероятности принадлежности значения амплитудной оценки спектра x информативной гармоники к одному из образов аномального или нормального состояния $P(x)$ производится с помощью функции Гаусса. На основании чего можно считать, что в этом случае имеет место нормальное распределение, а не распределение Пуассона или иное?

Соискатель Абрамова Т.В. согласилась с замечаниями и привела собственную аргументацию:

1. Поскольку сетевой трафик компьютерной сети АСУ ТП является совокупностью множества информационных потоков и содержит множество различных признаков о состоянии системы, было сделано предположение, что, согласно центральной предельной теореме, их суммарное воздействие на плотность вероятности подчиняется нормальному распределению. Статистические характеристики амплитудных оценок гармоник спектров временных рядов наборов данных сетевого трафика, использованные при разработки предлагаемых модели, метода и алгоритма, предварительно были проверены на соответствие критерию

Пирсона, что подтвердило соответствие оценок распределения плотности вероятности нормальному закону.

Диссертационная работа Абрамовой Таисии Вячеславовны на тему «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков» соответствует п. 9 Положения о присуждении ученых степеней (утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 (в редакции от 25.01.2024 г.), предъявляемых к кандидатским диссертациям.

Тема работы и содержание исследований соответствуют паспорту научной специальности ВАК 2.3.6. Методы и системы защиты информации, информационная безопасность по пунктам: 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».

Таким образом, диссертация Абрамовой Т.В. на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой содержатся научно обоснованные результаты решения научной задачи, заключающейся в разработке методов, моделей и алгоритмов, предназначенных для снижения рисков от реализации угроз безопасности информации в компьютерных сетях распределенных АСУ, имеющей существенное значение для развития отрасли знаний, связанной с обеспечением информационной безопасности объектов критической информационной инфраструктуры.

На заседании 17.09.2024 г. диссертационный совет принял решение:

- за решение научной задачи, заключающейся в разработке методов, моделей и алгоритмов, предназначенных для снижения рисков от реализации угроз безопасности информации в компьютерных сетях распределенных АСУ, имеющей существенное значение для развития отрасли знаний, связанной с обеспечением информационной безопасности объектов критической информационной инфраструктуры, присудить Абрамовой Т.В. ученую степень кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

При проведении тайного голосования диссертационный совет в количестве 15 человек, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 19 человек, входящих в состав совета, проголосовали: за – 15, против – 0.

Председатель
диссертационного совета
д-р техн. наук, профессор Султанов Альберт Ханович

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

17 сентября 2024 года