

УТВЕРЖДАЮ



Проректор по научной работе
ФГБОУ ВО «Оренбургский
государственный университет»,
д-р Физ.-мат. наук, профессор

С.Н. Летута

12 2023 г.

ЗАКЛЮЧЕНИЕ

федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» по диссертации Абрамовой Таисии Вячеславовны на соискание ученой степени кандидата технических наук

Диссертация «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков» выполнена на кафедре вычислительной техники и защиты информации института математики и информационных технологий ФГБОУ ВО «Оренбургский государственный университет» Министерства науки и высшего образования Российской Федерации.

В период подготовки диссертации соискатель Абрамова Таисия Вячеславовна проходила обучение в очной аспирантуре ФГБОУ ВО «Оренбургский государственный университет», работала в должности преподавателя и старшего преподавателя кафедры вычислительной техники и защиты информации в ФГБОУ ВО «Оренбургский государственный университет», работала по совместительству в должности младшего научного сотрудника научно-образовательного центра перспективных технологий и автоматизированных систем в машино- и авиастроении ФГБОУ ВО «Оренбургский государственный университет», выполняя грант РФФИ и правительства Оренбургской области № 18-47-560012 «Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков».

В 2015 г. окончила с отличием бакалавриат ФГБОУ ВПО «Оренбургский государственный университет» по направлению подготовки 10.03.01 «Информационная безопасность».

В 2017 г. окончила с отличием 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».

Справки об обучении со сведениями о сданных кандидатских экзаменах выданы в 2023 г. в ФГБОУ ВО «Оренбургский государственный университет» и ФГБОУ ВО «Уфимский университет науки и технологий».

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

По итогам обсуждения диссертации принято следующее заключение:

1. Диссертация Абрамовой Таисии Вячеславовны является законченной научно-квалификационной работой, соответствующей п. 9 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), в которой на основании выполненных автором исследований изложены новые научно обоснованные организационно-технические решения и разработки, внедрение которых имеет существенное значение для теории и практики защиты информации в автоматизированных системах управления технологическими процессами.

2. Соискателем лично получены все основные результаты, выносимые на защиту:

1) Метод матричной кластеризации угроз и моделей угроз (далее - МУ) распределенной автоматизированной системы (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 автоматизированной системы управления технологическим процессом (АСУ ТП).

2) Метод построения математических и имитационных моделей для обнаружения аномалий, распознавания состояний компьютерных сетей (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.

В перечисленных в автореферате работах соискателем лично получены следующие результаты:

- в работах [18, 20, 23] представлены результаты разработки метода кластеризации угроз и моделей угроз БИ для подсистем распределенных объектов КИИ на основе статистической обработки значений рисков;

- в работах [1, 3, 7, 8, 17, 24] представлены результаты разработки метода построения математических и имитационных моделей для обнаружения аномалий и распознавания состояния КС АСУ на основе данных мониторинга сетевого трафика;

- в работах [2, 4, 7-9, 13, 15, 17, 19, 21, 27, 28] представлены результаты разработки алгоритмов, методик и программной реализации методов и средств обнаружения аномалий и нейтрализации угроз по данным сетевого трафика на основе принципов построения ассоциативных процессоров;

- в работах [1, 5, 6, 10-12, 14, 16, 22, 25, 26] представлены результаты вычислительных и натурных экспериментов по оценке эффективности разработанных моделей, методов и методик.

Опубликованные работы полностью отражают содержание диссертационной работы. Все основные положения и результаты, выносимые на защиту, отражены в публикациях автора: по главе 1 – [1, 3, 7, 23]; по главе 2 – [1, 2, 6, 7, 17, 18, 20, 24]; по главе 3 – [1, 3, 4, 7-9, 13, 15, 17, 19, 21, 27]; по главе 4 – [1, 5, 6, 10-12, 14, 16, 22, 25, 26, 28]. Три работы написаны автором единолично, другие – совместно с научным руководителем или другими членами научного коллектива.

3. Достоверность полученных результатов и выводов основана на том, что предложенные в диссертационной работе решения подтверждаются:

1) корректной постановкой задач и выбором методов исследования;

2) результатами практического применения разработанных методов, моделей и алгоритмов при решении ряда прикладных задач;

3) апробацией в процессе проведения экспериментов с использованием разработанных программных средств, программного комплекса SCADA TRACE MODE и эмуляторов промышленного сетевого протокола ModBus TCP;

4) апробацией на научных конференциях, публикацией результатов в ведущих рецензируемых научных изданиях, в том числе из перечня ВАК, и в изданиях, входящих в международные реферативные базы данных.

4. 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 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 бинаризованные 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.

5. 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%. Научные результаты получены при проведении работ в рамках гранта РФФИ и правительства Оренбургской области № 18-47-560012 «Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков». 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).

6. Ценность научных работ соискателя заключается в развитии теории и практики защиты информации в автоматизированных системах управления технологическими процессами за счет повышения производительности и достоверности методов и средств обнаружения аномалий и нейтрализации угроз.

7. Обоснование выбранной специальности и отрасли наук диссертации

Диссертация «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков» соответствует 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».

Отрасль науки – техническая, поскольку приведенные результаты исследований в области обнаружения аномалий и нейтрализация угроз в распределенных автоматизированных системах управления дают существенный технический эффект при их использовании и внедрении.

7. Полнота изложения материалов диссертации

По материалам исследования опубликовано 42 работы, в том числе 3 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.

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

1) 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.

2) Аралбаев, Т.З., Абрамова Т.В., Галимов Р.Р., Гайфулина Д.А., Хакимова Э.Р. Выбор базовой функции при автоматизированной идентификации временных рядов на основе ассоциативно-мажоритарного подхода // Вестник Ижевского государственного технического университета имени М.Т. Калашникова. – 2018. – Т. 21. – № 4. – с. 194 – 199.

3) Аралбаев, Т.З. Комбинаторная семантическая модель генерации гипотез/ Аралбаев Т.З., Абрамова Т.В., Галимов Р.Р. // Информация и безопасность, 2016. - Т. 19, № 3 (4). - С. 379-384.

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

4) 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.

Другие публикации по теме диссертации

5) 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. - Оренбург: ОГУ, 2019 – 160 с.

6) Аралбаев Т.З., Аралбаева Г.Г., Африн А.Г., Абрамова Т.В. Ассоциативно-мажоритарный подход к решению задач распознавания образов в системах защиты информации: учебно-методическое пособие / Т.З. Аралбаев, Г.Г. Аралбаева, А.Г. Африн, Т.В. Абрамова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2023. – 150 с. ISBN 978-5-7410-3150

7) Абрамова, Т.В., Аралбаев, Т.З. Анализ пространственно-временной модели угроз для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья. Вестник УГАТУ, [S.l.], v. 24, n. 1 (87), p. 76-84, май 2020. ISSN 1992-6502.

8) Аралбаев, Т.З. Концепция компьютерного мониторинга инновационной активности молодых специалистов и студентов на основе анализа информационных ресурсов в глобальной сети Интернет / Т.З. Аралбаев, Т.В. Абрамова, С.Ю. Романенко // Интеллект. Инновации. Инвестиции, 2017. - № 5. - С. 48-53. . - 6 с.

9) 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.

10) 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

11) 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

12) Зайчиков, И.Д. Метод мониторинга поведения пользователя на основе данных сетевого трафика/ И.Д. Зайчиков, Т.В. Абрамова // Шаг в науку, 2023. - № 1. - С. 35-40. . - 6 с.

13) Аралбаев, Т.З. Геоинформационное взаимодействие мобильных средств в задаче мониторинга распределенных промышленных объектов / 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. . - 9 с.

14) 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: материалов Всероссийской научно-методической конференции; Оренбург: ОГУ, 2022. – с. 1245 – 1250.

15) Т.В. Абрамова, В.В. Крылов, А.Т. Даминов Моделирование режима обнаружения атаки ring-flooding на базе учебно-исследовательского сетевого стенда// WORLD SCIENCE: PROBLEMS AND INNOVATIONS: сборник статей LIV Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение». – 2021. – с.50 – 53

16) В.Д. Родионов, Т.В. Абрамова Метод обнаружения атак на беспилотный летательный аппарат на основе анализа сетевого трафика//Современная наука: актуальные вопросы, достижения и инновации: сборник статей XIX Международной научно-практической конференции. Ч. 1. – Пенза: МЦНС «Наука и Просвещение». – 2021. – с. 55 – 59

17) 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

18) Абрамова, Т.В. Модель контроля транзакций пользователя АСУ ТП на основе сигнатурного принципа/Т.В. Абрамова, Т.З. Аралбаев, //«ИНФО-2020»: сборник трудов XVI международной научно-практической конференции; Сочи. - 2020. – с. 181 - 185.

19) Абрамова, Т.В. Исследование безопасности Wi-Fi сетей средствами моделирования атак злоумышленника на базе Kali Linux/ Т.В. Абрамова, И.Д. Зайчиков// Наука и инновации в XXI веке: актуальные вопросы, достижения и тенденции развития: Материалы XIX Международной научно-

практической конференции. – Пенза: Изд-во МЦНС «Наука и просвещение». 2020. – с. 83 - 86.

20) 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.

21) 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: сборник материалов Всероссийской научно-методической конференции. - Оренбург: ОГУ, 2020. – с. 1389 – 1395.

22) 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.

23) 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.

24) Аралбаев, Т.З. Концепция оптимизации системы контроля технического состояния распределенных автоматизированных систем на основе мониторинга сетевых информационных потоков / 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. 40-46.

25) 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. - Оренбург: ОГУ, 2018. - с. 37-40.

26) 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.

27) 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.

28) Абрамова, Т.В., Аралбаев Т.З., Галимов Р.Р., Манжосов А.В., Хатеев М.Д. Моделирование аномалий в информационной системе мониторинга состояния нефтепровода по данным сетевого трафика//Безопасность: Информация, Техника, Управление: Материалы международной научной конференции. – Санкт-Петербург: Изд-во ГНИИ «НАЦРАЗВИТИЕ». 2018. – С. 127-130.

29) 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. Сеницын // Университетский комплекс как региональный центр образования, науки и культуры: материалов Всероссийской научно-методической конференции; Оренбург: ОГУ, 2018. – С. 1719 – 1725

30) Аралбаев, Т.З. Особенности оперативного поиска информации о сетевом трафике по первичным данным аномальной активности компьютерной сети/ Аралбаев Т.З., Абрамова Т.В. // Информационное противодействие угрозам терроризма, 2015. - № 24. - С. 76-81. - 5 с.

31) Аралбаев, Т.З. Исследование эффективности метода оперативного поиска информации о сетевом трафике на основе ассоциативного принципа / Аралбаев Т.З., Абрамова Т.В. // Современные информационные технологии в науке, образовании и практике : материалы VII Всерос. науч.-практ. конф., 2015 г., Оренбург / М-во образования и науки РФ; Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Электрон. дан. - Оренбург: ОГУ, 2015. - с. 235-238.

32) Абрамова, Т.В. Моделирование сетевых атак на ресурсы вычислительных систем с использованием принципов самоорганизации/ Абрамова Т.В., Аралбаев Т.З. // Современные информационные технологии в науке, образовании и практике : материалы X Всерос. науч.-практ. конф., посвящ. 80-лет. Оренбург. обл., Оренбург / М-во образования и науки РФ; Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург: Университет, 2014. - . - С. 109-114. - 6 с.

33) 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.

34) 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.

35) 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.

36) Абрамова Т.В., Аралбаев Т.З., Галимов Р.Р., Программный комплекс «Моделирование сетевого трафика на базе протокола ТСР/ModBUS». Свидетельство о регистрации электронного ресурса. Рег. № 1657. Дата регистрации: 10.11.2018. Оренбургский государственный университет.

37) 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.

38) 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.

39) 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.

40) Абрамова Т.В., Аралбаев Т.З., Гаврилов М.С. 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.

Патенты и свидетельства о регистрации программ для ЭВМ

41) 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.

42) Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus ТСР: 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 .

Диссертация Абрамовой Таисии Вячеславовны соответствует п. 14 Положения о порядке присуждения ученых степеней:

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

Диссертация на тему «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков» Абрамовой Таисии Вячеславовны рекомендуется к защите на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Заключение принято на расширенном заседании кафедры вычислительной техники и защиты информации ФГБОУ ВО «Оренбургский государственный университет» Министерства науки и высшего образования Российской Федерации.

Присутствовало на заседании 14 человек, в том числе 4 доктора наук.

Результаты голосования: «за» – 14 человек, «против» – нет, «воздержалось» – нет.

Протокол № 6 от «7» декабря 2023 года.

Заведующий кафедрой
вычислительной техники
и защиты информации,
д-р техн. наук, доцент

В.В. Тугов

Подпись _____
заверю _____
Входящий след. пакет по документационному
обеспечению персонала _____

