ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА 99.2.038.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело № _____

решение диссертационного совета от 25 июня 2025 г. № 13

О присуждении Вовику Андрею Геннадьевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 23 апреля 2025 года, протокол № 8 объединенным диссертационным советом 99.2.038.03, созданным на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» Министерства науки и высшего образования Российской Федерации, Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства науки и высшего образования Российской Федерации, Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет

телекоммуникаций им. проф. М.А. Бонч-Бруевича» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, 191186, Санкт-Петербург, наб. реки Мойки, д. 61, приказ № 44/нк от 30 января 2017 года.

Соискатель Вовик Андрей Геннадьевич, 23 сентября 1993 года рождения, работает старшим преподавателем в Ордена Трудового Красного Знамени федеральном государственном бюджетном образовательном учреждении высшего образования «Московский технический университет связи и информатики», Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

В 2020 году соискатель окончил Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» с присвоением квалификации магистр. В 2024 году окончил освоение программы подготовки научных и научно-педагогических кадров в аспирантуре Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики».

Диссертация выполнена на кафедре интеллектуальных систем в управлении и автоматизации Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики».

Научный руководитель – кандидат технических наук, Ларин Александр Иванович, основное место работы: Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», кафедра интеллектуальных систем в управлении и автоматизации, доцент кафедры.

Оппоненты: 1. Лось Владимир Павлович, доктор военных наук, профессор, основное место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный

гуманитарный университет», кафедра информационной безопасности, главный научный сотрудник; 2. Цирлов Валентин Леонидович, кандидат технических наук, доцент, основное место работы: акционерное общество «Научно-производственное объединение «Эшелон», генеральный директор, дали положительные отзывы о диссертации.

Ведущая организация федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий», г. Уфа, в своем положительном заключении, подписанном Картаком Вадимом Михайловичем доктором физико-математических наук, профессором, зав. кафедрой вычислительной техники и защиты информации и Вульфиным Алексеем Михайловичем, доктором технических наук, профессором кафедры вычислительной техники и защиты информации, утвержденном Шарафуллиным Ильдусом Фанисовичем, доктором физико-математических наук, профессором, проректором по научной работе, указала, что диссертация Вовика Андрея Геннадьевича на тему: «Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз» рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 30 опубликованных работ, в том числе по теме диссертации 11, из них в рецензируемых научных изданиях, рекомендованных ВАК, – 4, в том числе 4 в изданиях, соответствующих искомой специальности, а также: 1 результат интеллектуальной деятельности; 6 статей в других научных журналах, сборниках научных статей, трудов и материалах конференций. Из них 6 работ опубликованы соискателем без соавторства. Общий объём авторского вклада в работы (без результатов интеллектуальной собственности) составляет 3,74 печ.л. из общего количества 4,58 печ.л. Диссертация не содержит недостоверных сведений об опубликованных соискателем ученой степени работах.

Наиболее значительные научные работы по теме диссертации.

Публикации в рецензируемых научных изданиях, рекомендованных ВАК:

1. Вовик А.Г., Ларин А.И. О возможности численных метрик в управлении информационной безопасностью // Наукоемкие технологии в космических исследованиях Земли. – 2022. – Т. 14. – № 6. – С. 12-19.

2. Вовик А.Г., Ларин А.И. Подход к формализации оценки угроз информационной безопасности методом нечеткого моделирования // Наукоемкие технологии в космических исследованиях Земли. – 2023. – Т. 15. – № 3. – С. 30-37.

3. Вовик А.Г. Проблемы моделирования процессов управления информационной безопасностью в автоматизированных системах // Приборы и системы. Управление, контроль, диагностика. – 2024. – № 9. – С. 28-39

4. Вовик А.Г. Методика автоматизированного управления информационной безопасностью в системах интернета вещей // Наукоемкие технологии в космических исследованиях Земли. – 2024. – Т.16. – №4. – С. 4-11.

Результаты интеллектуальной деятельности:

Вовик А.Г. Программа для управления информационной безопасностью систем Интернета Вещей: Свидетельство о государственной регистрации программы для ЭВМ № 2024615772, 13.03.2024.

Публикации в других изданиях:

6. Ларин А.И., Вовик А.Г., Тряпицын А.Д. Формализация неструктурированной текстовой информации на основе векторного представления слов // Инновационное развитие: потенциал науки и современного образования: монография. – Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2021. – С. 212-223.

7. Вовик А.Г. К вопросу формализации моделей управления информационной безопасностью в системах Интернета Вещей // Сборник научных трудов по материалам III Всероссийской научной школы-семинара Современные тенденции развития методов и технологий защиты информации. Москва, МТУСИ, 25-27 октября 2023 г. – М., 2023. – С. 253-257.

8. Вовик А.Г. Комплексная математическая модель процесса управления информационной безопасностью в системах IoT // Актуальные проблемы

инфотелекоммуникаций в науке и образовании (АПИНО 2024): Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27-28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 195-201.

9. Вовик, А.Г., Ларин А.И., Вовик В.С. Количественные оценки в формальных моделях управления информационной безопасностью систем Интернета вещей // Наука, общество, технологии: актуальные вопросы, достижения и инновации: монография. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 64-74.

10. Вовик, А.Г. Подход к управлению информационной безопасностью систем Интернета Вещей посредством формирования и использования в системе управления сигнала отрицательной обратной связи // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 23-25 октября 2024 года. – С. 620-625.

11. Вовик А.Г. Управление ИБ систем IoT через отрицательную обратную связь // Региональная информатика (РИ-2024): Материалы XIX Санкт-Петербургской международной конференции, Санкт-Петербург, 23-25 октября 2024 года. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. – С. 424-425.

На диссертацию и автореферат поступили отзывы: официального оппонента Лося В.П., д.воен.н., проф., главного научного сотрудника кафедры информационной безопасности федерального государственного автономного образовательного учреждения высшего образования «Российский государственный гуманитарный университет»; официального оппонента Цирлова В.Л., к.т.н., доц., генерального директора акционерного общества «Научно-производственное объединение «Эшелон»; ведущей организации УУНиТ; Магомедова Ш.Г., д.т.н., доц., директора Института искусственного интеллекта федерального государственного бюджетного образовательного

учреждения высшего образования «МИРЭА – Российский технологический университет»; Елисеева В.Л., к.т.н., руководителя Центра научных исследований и перспективных разработок акционерного общества «Информационные технологии и коммуникационные системы»; Хайрова И.Е., к.т.н., доц., заместителя директора автономной некоммерческой организации дополнительного профессионального образования центр повышения квалификации «АИС»; Баранова В.В., к.воен.н., доц., зав. кафедрой информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Российский государственный политехнический университет (НПИ) имени М. И. Платова»; Петренко В.И., к.т.н., доц., зав. кафедрой организации и технологии защиты информации федерального государственного автономного образовательного учреждения высшего образования «Северо-Кавказский федеральный университет»; Осипова М.Н., к.ф.-м.н., доц., зав. кафедрой безопасности информационных систем федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева»; Частиковой В.А., к.т.н., доц., доцента кафедры кибербезопасности и защиты информации федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет»; Ветрова И.А., к.т.н., доц., методического руководителя по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Балтийский федеральный университет имени Иммануила Канта»; Шелупанова А.А., д.т.н., проф., президента федерального государственного автономного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники» и Новохрестова А.К., к.т.н., доцента кафедры комплексной информационной безопасности электронно-вычислительных систем федерального государственного автономного

образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Все отзывы положительные, но имеются следующие критические замечания. В диссертации недостаточно подробно описаны конкретные способы практической реализации предложенной методики. В работе не полностью раскрыты вопросы масштабируемости предложенной методики. Необходимо более подробно рассмотреть, как методика может быть применена к большим и сложным IoT-системам с тысячами или миллионами устройств. Необходимо более детально рассмотреть вопросы валидации и верификации предложенной модели и методики управления ИБ. Какие методы и подходы использовались для подтверждения корректности работы модели и соответствия результатов моделирования реальным процессам? В диссертации не полностью учтены вопросы, связанные с организационно-правовыми методами защиты информации. Необходимо пояснить, как предложенная методика может быть интегрирована с существующими нормативными требованиями и стандартами в области ИБ. Диссертация носит сугубо теоретический характер, результаты практического внедрения предложенного способа управления ИБ в IoT-системах изложены достаточно кратко. Следовало уделить отдельное внимание анализу возможности реализации компьютерных атак, характерных для систем, использующих методы управления с обратной связью. В диссертации недостаточно внимания уделено сравнению предложенной методики с другими известными подходами к управлению ИБ в IoT-системах. Недостаточно подробно описаны критерии выбора параметров для нечетких моделей и их влияние на результаты моделирования. В работе недостаточно полно раскрыты вопросы нормализации данных, собираемых из множественных источников, для их последующей формализации. Недостаточно детализированы вопросы совместимости предложенных решений с существующими силами и средствами управления информационной безопасностью. Не затронуты вопросы, касающиеся процедуры подбора экспертов для определения начального уровня угроз целостности, доступности конфиденциальности: сколько таких экспертов должно быть, какие

требования к ним предъявляются, какие вопросы задаются. В работе не рассматриваются особенности различных классов IoT-систем (промышленные, медицинские, бытовые и т.д.), каждый из которых имеет свою специфику с точки зрения обеспечения информационной безопасности. Автор не приводит сведения о том, как ведет себя система при увеличении количества защищаемых устройств на несколько порядков. В автореферате недостаточно представлены данные о работе методики в условиях реальных промышленных IoT-развёртываний с тысячами устройств. Обращает на себя внимание необходимость более детального рассмотрения вопросов возможности масштабирования предложенного решения для крупных распределенных IoT-систем, а также его взаимодействия с системами мониторинга безопасности корпоративного уровня. Объект и предмет исследования сформулированы корректно, однако изложены избыточно абстрактно. Было бы уместно конкретизировать, на каком классе IoT-систем производилась апробация. Формализация угроз на базе неструктурированных текстов (модель М6) представлена весьма схематично. Из автореферата неясно, в какой степени учитывается семантическое разнообразие источников и как обеспечивается сопоставимость с «деревом угроз». В работе недостаточно освещен вопрос масштабируемости предложенного решения. Современные IoT-системы могут включать миллионы устройств, и не совсем понятно, как предложенная методика будет работать в таких условиях. Вызывает вопросы выбор конкретных параметров нечетких моделей. Автор не приводит достаточного обоснования, почему были выбраны именно такие функции принадлежности и правила вывода. Было бы полезно увидеть сравнительный анализ с альтернативными вариантами. В разделе, посвященном практической реализации, не хватает информации о производительности разработанного решения. Для промышленного внедрения важно понимать, какие вычислительные ресурсы требуются для работы системы. Мало внимания уделено вопросам устойчивости предложенного алгоритма к целенаправленным атакам на систему управления безопасностью. В современных условиях это критически важный аспект. В некоторых разделах автореферата хотелось бы видеть более четкое

разделение между теоретическими положениями и практическими результатами. Было бы полезно привести более подробные сравнения с существующими аналогами, чтобы еще ярче подчеркнуть преимущества предложенного подхода. В представленной методике не рассматривается вариант действий, когда нельзя подобрать разрешенное состояние, чтобы выполнить условие. Представленная схема предполагает, что в любом случае система перейдет в защищенное состояние. Не в полной мере раскрыт принцип формирования базы правил нечеткой модели: используется ли ручная настройка экспертами, настройка с применением алгоритмов машинного обучения или гибридный подход? В автореферате не приведены сведения об экспериментах, подтверждающих эффект от применения методики на лабораторных стендах, а также отсутствуют сведения о результатах внедрения, приводятся только сведения о самом факте внедрения в деятельность ООО «Эмбеддед Системс Рус».

Выбор оппонентов и ведущей организации обосновывается широкой известностью их достижений в отрасли науки, связанной с тематикой диссертации, наличием у них актуальных публикаций в соответствующей и смежных сферах научных исследований, способностью квалифицированно оценить актуальность, теоретическую значимость и практическую ценность диссертации. Лось В.П., д.воен.н., проф., является известным специалистом в области ИБ, Президентом Ассоциации защиты информации. Занимается решением проблем связанных с подготовкой специалистов в области ИБ, с разработкой архитектур управления ИБ и процессов управления инцидентами ИБ; Цирлов В.Л., к.т.н., доц., ведет активную деятельность в области обеспечения ИБ, является генеральным директором компании НПО «Эшелон», занимающейся обеспечением комплексной кибербезопасности. Продукты компании соответствуют современным требованиям и актуальным цифровым угрозам. Качество работы подтверждено более 30 лицензиями и аттестатами аккредитации. Выбор ведущей организации обосновывается тем, что Уфимский университет науки и технологий (УУНиТ) является крупным научным центром и активно занимается проблематикой по направлению диссертационной работы

А.Г. Вовика. Специалисты кафедры вычислительной техники и защиты информации УУНиТ известны своими публикациями по направлению защиты промышленного Интернета вещей, по направлению оценки рисков ИБ и др.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработана новая комплексная модель процесса управления ИБ в системах IoT, которая учитывает полный цикл управления ИБ и обеспечивает возможность повышения эффективности управления по критериям оперативности и точности управления ИБ; **разработана** методика автоматизированного управления ИБ в системах IoT с непрерывным замкнутым циклом нечеткой оценки угроз, которая уточняет порядок выполнения численных оценок основных параметров процесса управления ИБ в системах IoT и обеспечивает возможность автоматизированного управления с высокой эффективностью по критериям оперативности и точности, в то время как нормативный подход к управлению ИБ предполагает исключительно «ручное» управление ИБ на основе неформальных моделей;

предложен способ управления ИБ в системах IoT отличается от известных способов управления учетом и использованием в системе управления ИБ обратной связи в режиме численной оценки основных параметров процесса управления, что обеспечивает повышение эффективности управления по критерию точности управления ИБ;

доказана возможность повышения эффективности управления ИБ по критерию «точность управления» более чем на 40% по сравнению с нормативными способами управления ИБ в случае наличия 3-4 альтернативных решений по изменению конфигурации СЗИ в ответ на изменение уровня угроз в системе; **доказана** возможность повышения эффективности управления ИБ в системе IoT по критерию «оперативность управления» более чем на 30% по сравнению с нормативными способами управления ИБ;

введены критерии эффективности управления ИБ: «оперативность управления ИБ» и «точность управления ИБ».

Теоретическая значимость исследования обоснована тем, что: доказана возможность повышения эффективности управления ИБ по критериям «точность управления ИБ» и «оперативность управления ИБ»;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использованы аналитические методы представления систем, методы экспертных оценок, методы нечеткого моделирования, методы структуризации и методы формализации текстовых сообщений на основе векторного представления слов;

изучены факторы, препятствующие получению возможности проведения численных оценок основных показателей процесса управления ИБ;

раскрыто существующее противоречие между необходимостью повышения эффективности управления ИБ для систем Интернета Вещей и невозможностью такого повышения по критериям оперативности и точности управления ИБ традиционными методами;

проведена модернизация существующих моделей и методик управления информационной безопасностью, обеспечивающая повышение эффективности управления ИБ для систем Интернета Вещей.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработанный способ управления информационной безопасностью Интернета Вещей **используется** в дисциплине «Основы информационной безопасности» для студентов бакалавриата по направлению 10.03.01 «Информационная безопасность», **разработанная** методика автоматизированного управления информационной безопасностью в системах IoT **используется** в дисциплине «Методы управления информационной безопасностью в технических системах» для магистрантов по направлению 27.04.04 «Управление в технических системах», программа «Информационная безопасность автоматизированных систем управления»;

определены границы диссертационного исследования и ограничение разработанных моделей;

представлены рекомендации по практическому применению предложенной Методики управления информационной безопасностью в системах IoT.

Оценка достоверности результатов исследования выявила: для экспериментальных работ результаты проверены на системе испытательных стендов, представляющих собой набор компонентов Интернета Вещей, соединенных по различным каналам передачи данных и управляемых программируемым логическим контроллером, показана возможность получения численных оценок параметров процесса управления ИБ;

теория построена на известных методах моделирования систем управления;

идея базируется согласовании разнородных подмоделей по масштабу и размерности через инструментарий лингвистических переменных;

использованы положения нормативных документов и государственных стандартов РФ и МД ФСТЭК.

Личный вклад соискателя состоит в непосредственном участии в разработке способа управления информационной безопасностью системы Интернета Вещей, комплексной модели процесса управления информационной безопасностью системы Интернета Вещей и Методики управления информационной безопасностью системы Интернета Вещей, разработанной программе для ЭВМ, реализующей нечеткое ядро комплексной модели; в том, что опубликовано 2 печатные работы в изданиях из перечня рецензируемых научных журналов ВАК при Минобрнауки России без соавторства; с 2021 по 2024 годы соискатель выступал с докладами на научных российских и международных конференциях. Все основные результаты диссертационной работы, в том числе результаты теоретических и экспериментальных исследований получены автором самостоятельно.

В ходе защиты диссертации были высказаны следующие критические замечания о том, что: не до конца понятно назначение графиков на слайдах 13 и 21, для чего они вынесены на защиту; в работе не приведены сведения о валидации и верификации предложенных результатов.

Соискатель Вовик А.Г. в ходе заседания **ответил** на задаваемые ему вопросы, **согласился с замечаниями** и привел собственную аргументацию.

Диссертационный совет установил, что диссертация «Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз» является законченной научно-квалификационной работой и соответствует требованиям п. 9 Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а также пунктам 9 и 18 паспорта научной специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

На заседании 25 июня 2025 года объединенный диссертационный совет принял решение присудить Вовику А.Г. ученую степень кандидата технических наук за решение научной задачи по повышению эффективности управления ИБ IoT-систем.

При проведении тайного голосования объединенный диссертационный совет в количестве 16 человек, из них 5 докторов наук по научной специальности рассматриваемой диссертации, участвовавших в заседании, из 23 человек, входящих в состав совета, проголосовали: за – 16, против – нет, недействительных бюллетеней – нет.

Председательствующий диссертационного совета,
доктор технических наук, профессор

Татарникова Татьяна Михайловна

Ученый секретарь диссертационного совета,
кандидат технических наук, доцент

Владыко Андрей Геннадьевич

25 июня 2025 года