

УТВЕРЖДАЮ

Проректор по научной работе

п.ф. - М.Н., профессор

И.Ф. Шарафуллин



21 » 05 2025 г.

## ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационную работу Вовика Андрея Геннадьевича на тему: «Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз», представленную на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность

### Актуальность темы диссертации

Системы Интернета вещей стремительно проникают во все сферы жизнедеятельности – от промышленного производства до бытовых устройств. Однако их широкое распространение сопровождается серьезными вызовами в области информационной безопасности. Особенности IoT-устройств, такие как ограниченные вычислительные ресурсы, длительный жизненный цикл и автономность работы, делают их уязвимыми перед постоянно эволюционирующими угрозами безопасности информации.

Традиционные подходы к управлению информационной безопасностью, разработанные для классических информационных систем, демонстрируют свою неэффективность в условиях IoT-среды. Существующие методики не учитывают специфику распределенных гетерогенных сетей, состоящих из тысяч маломощных устройств. Более того, ручные методы оценки рисков и реагирования на инциденты не успевают за скоростью появления новых уязвимостей и векторов атак.

Особую остроту проблеме придает использование IoT-систем в

критически важных инфраструктурах – энергетике, транспорте, здравоохранении. Компрометация таких систем может привести не только к финансовым потерям, но и создать угрозу жизни и здоровью людей. При этом существующие нормативные документы и стандарты информационной безопасности не в полной мере охватывают особенности защиты IoT.

В этих условиях разработка специализированной методики управления информационной безопасностью, учитывающей уникальные характеристики IoT-систем, становится насущной необходимостью. Такой подход должен обеспечивать непрерывный мониторинг угроз, оперативное принятие решений и адаптацию защитных механизмов в условиях ограниченных ресурсов устройств. Особое значение приобретает автоматизация процессов управления безопасностью, позволяющая минимизировать человеческий фактор и сократить время реакции на инциденты.

Таким образом, актуальность исследования обусловлена критической важностью разработки новых методов защиты IoT-систем, соответствующих современным вызовам информационной безопасности и учитывающих технологические ограничения интернета вещей.

### **Структура и содержание диссертации**

Во введении обосновывается актуальность темы, формулируются научная задача, цель и частные задачи исследования, определяются объект и предмет исследования, приводится практическая значимость и научная новизна результатов, излагаются научные положения, выносимые на защиту.

В первой главе проведено исследование современного состояния проблемы обеспечения информационной безопасности (ИБ) в системах Интернета вещей. Рассмотрены характеристики IoT-систем как объектов защиты, проанализированы основные проблемы ИБ, включая недостаточность правового регулирования и специфику архитектуры IoT. Обоснована необходимость формализации процессов управления ИБ и введены критерии эффективности: оперативность и точность управления.

Вторая глава посвящена разработке способа управления ИБ в IoT-



системах с использованием обратной связи и численной оценки параметров. Проведен анализ существующих методов управления ИБ, выявлены их недостатки. Разработан способ, позволяющий повысить эффективность управления за счет оптимизации выбора контрмер и сокращения времени реакции на угрозы.

В третьей главе синтезирована комплексная модель управления ИБ в IoT-системах, включающая нечеткое ядро для оценки угроз, экспертную модель и модель формализации сообщений об инцидентах. Модель обеспечивает непрерывный замкнутый цикл оценки угроз и позволяет численно определять уровень защищенности информации. Проведена оценка эффективности модели, показавшая повышение оперативности и точности управления.

В четвертой главе приводится методика автоматизированного управления ИБ на основе разработанной комплексной модели. Методика включает два этапа: подготовку исходных данных и автоматизированное управление. Разработаны рекомендации по практическому применению, направленные на повышение эффективности управления.

В заключении подведены итоги исследования, подтверждена актуальность и научная новизна работы. Показано, что предложенные решения повышают эффективность управления ИБ в IoT-системах по критериям оперативности и точности. Полученные результаты исследования внедрены в практическую деятельность организации и учебный процесс кафедры «Информационная безопасность» МТУСИ.

### **Теоретическая значимость**

Теоретическая ценность диссертационного исследования заключается во вкладе в развитие теории и методов управления информационной безопасностью, а именно:

- 1) в разработке нового способа управления информационной безопасностью в системах IoT, основанного на использовании обратной связи в режиме численной оценки основных параметров процесса управления;

2) в разработке комплексной модели управления ИБ в системах IoT, охватывающей полный цикл управления и имеющей в основе нечеткое ядро для определения текущего уровня актуальных угроз в системе в виде последовательностей нечетких моделей с использованием алгоритма нечеткого вывода Мамдани;

3) расширении класса способов оценки эффективности управления информационной безопасностью введением показателя защищенности информации, как соответствия возможностей СЗИ уровню актуальных угроз в системе и разработке подхода к оцениванию эффективности управления ИБ на основе введенных формализованных критериев эффективности – оперативность управления ИБ и точность управления ИБ.

### **Практическая значимость**

1. Предложенная методика позволяет существенно улучшить управление информационной безопасностью IoT-систем за счет внедрения комплексной модели, обеспечивающей непрерывный контроль и автоматизированное принятие решений. Это снижает зависимость от ручных процессов и ускоряет реакцию на угрозы.

2. Методика представляет собой формализацию требований, предъявляемых к СМИБ (в соответствии с ГОСТ Р ИСО/МЭК 270xx), в части управления рисками информационной безопасности и управления защитными мерами. Она формализует ключевые этапы управления рисками, что обеспечивает конкретизацию требований к управлению информационной безопасностью применительно к системам IoT.

3. Результаты исследования могут быть применены компаниями-владельцами IoT-инфраструктуры и администраторами безопасности для поддержания требуемого уровня защиты данных. Методика помогает эффективно противодействовать постоянно меняющимся угрозам, минимизируя риски и операционные издержки.

## Апробация работы

Основные результаты работы доложены на 5 международных и российских научных конференциях:

1. XII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании», Санкт-Петербург, 28 февраля – 1 марта 2023г.
2. III Всероссийская научная школа-семинар «Современные тенденции развития методов и технологии защиты информации», Москва, 24-27 октября 2023 г.
3. XIII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании», Санкт-Петербург, 27-28 февраля 2024г.
4. XV Молодежный Научный Форум МТУСИ «Телекоммуникации и инфокоммуникационные технологии - реалии, возможности, перспективы» «1» - «22» апреля 2024 г.
5. XIX Санкт-Петербургская международная конференция «Региональная информатика (РИ-2024)», 23-25 октября 2024г.

Автором опубликованы работы в рецензируемых научных изданиях, рекомендованных ВАК:

1. Вовик А. Г., Ларин А.И. О возможности численных метрик в управлении информационной безопасностью // Научные технологии в космических исследованиях Земли. – 2022. – Т. 14, № 6. – С. 12-19. – DOI 10.36724/2409-5419-2022-14-6-12-19. – EDN BRHJMS.
2. Вовик А.Г., Ларин А.И. Подход к формализации оценки угроз информационной безопасности методом нечеткого моделирования // Научные технологии в космических исследованиях Земли. 2023. Т. 15, № 3. С. 30-37. doi: 10.36724/2409-5419-2023-15-3-30-37.
3. Вовик А. Г. Проблемы моделирования процессов управления информационной безопасностью в автоматизированных системах // Приборы и системы. Управление, контроль, диагностика. – 2024. – № 9. – С. 28-39. – DOI 10.25791/pribor.9.2024.1524. – EDN DRPKJA.



4. Вовик А. Г. Методика автоматизированного управления информационной безопасностью в системах интернета вещей // Научные технологии в космических исследованиях Земли. Т.16. №4. С. 4-11. doi: 10.36724/2409-5419-2024-16-4-4-11

**Работы, опубликованные в других изданиях:**

5. 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. – EDN KSZKSL

6. Ларин А. И., А.Г. Вовик, А.Д. Тряпицын 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. – EDN HGYJAJ

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

8. 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.

9. Вовик А. Г. Управление ИБ систем IOT через отрицательную обратную связь / А. Г. Вовик // Региональная информатика (РИ-2024) : Материалы XIX Санкт-Петербургской международной конференции, Санкт-

Петербург, Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. – С. 424-425. – EDN HLQIXV.

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-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. – С. 620-625. – EDN PSZNHY.

**Полученные автором свидетельства о государственной регистрации программы для ЭВМ:**

11. Вовик А.Г. «Программа для управления информационной безопасностью систем Интернета Вещей» Свидетельство о государственной регистрации программы для ЭВМ № 2024615772 Российская Федерация.: № 2024614411: заявл. 06.03.2024: опубл. 13.03.2024

Публикации соответствуют направлению диссертационного исследования и раскрывают основные положения, полученные в диссертации.

**По диссертации имеются следующие замечания**

1. Сформулированные в Главе 1 критерии эффективности управления («оперативность управления» и «точность управления») приведены без детального обоснования возможности их применения в контуре управления.

2. При применении нечетких методов моделирования в качестве нелинейного подхода к решению проблемы управления информационной безопасностью в исследовании не уделено достаточного внимания обоснованию устойчивости предложенного решения при различных условиях работы и внешних воздействиях.

3. Описание процесса внедрения методики, включая конкретные этапы, требования к инфраструктуре и алгоритмы адаптации для реальных

условий эксплуатации недостаточно детализировано и конкретизировано.

4. В работе не приведен развернутый пример применения разработанной методики для конкретного объекта защиты.

5. В работе уделено недостаточно внимания явному определению категорий IoT-систем (промышленные, бытовые или смешанные), для которых предназначена разработанная методика, что может оказать влияние на требования к безопасности, и условия применения.

6. В Заключение недостаточно подробно приведено описание количественных оценок повышения эффективности, основное внимание уделено качественным характеристикам.

#### **Соответствие диссертации научной специальности**

Диссертация соответствует Паспорту научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность в пунктах «9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности, «18. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании».

#### **Общее заключение**

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.

Диссертационная работа и отзыв обсуждены на расширенном заседании кафедры вычислительной техники и защиты информации федерального



государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий».

Протокол № 9 от «12» мая 2025 г.

Голосовали «за» – 14 чел.;

«против» – 0 чел.;

«воздержались» – 0 чел.

Зав. кафедрой

вычислительной техники и защиты информации,

д.ф.-м.н., профессор

В.М. Картак

Профессор кафедры

вычислительной техники и защиты информации,

д.т.н.

А.М. Вульфин

Сведения об организации:

Федеральное государственное бюджетное образовательное учреждение образования «Уфимский университет науки и технологий»

Почтовый адрес:

450076, Республика Башкортостан, г.о. город Уфа, г. Уфа, ул. Заки Валиди,

д. 32 тел.: 8(347) 272-63-70, факс: 8(347) 273-67-78,

e-mail: rector@uust.ru



Картак В.М., Вульфин А.М.  
Подтверяю «12» 05 2025 г.  
Зам. начальника общего отдела УУНИТ Т.Шам  
Шамиева Т.Р.