На правах рукописи

Вовик Андрей Геннадьевич

Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Москва 2025

Работа выполнена в ордена Трудового Красного Знамени федеральном государственном бюджетном образовательном учреждении высшего образования «Московский технический университет связи и информатики» (МТУСИ) на кафедре «Интеллектуальные системы в управлении и автоматизации»

Научный руководитель: кандидат технических наук, **Ларин Александр Иванович**

Официальные оппоненты:

Лось Владимир Павлович
доктор военных наук, профессор
Федеральное государственное автономное образовательное учреждение высшего образования "Российский государственный гуманитарный университет", главный научный сотрудник кафедры Информационная безопасность

Цирлов Валентин Леонидович
кандидат технических наук, доцент
Акционерное общество «Научно-производственное объединение «Эшелон», генеральный директор

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий», г. Уфа

Защита состоится 25 июня 2025 г. в 11:00 на заседании 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», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», «Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 25 апреля 2025 г.

Учёный секретарь
диссертационного совета 99.2.038.03,
кандидат техн. наук, доцент А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. Информационная безопасность стала ключевой темой для национальной безопасности России, как указано в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ № 400 от 02.07.2021 г. и Доктрине информационной безопасности РФ 2016 г. Современные информационные технологии охватывают все сферы жизни, создавая новые угрозы, включая активизацию компьютерной преступности и информационно-психологических атак со стороны зарубежных спецслужб. Это угрожает суверенитету государства и требует определения стратегических целей для защиты информации.

В результате бурного развития IT-технологий на современном этапе выделяется отдельный класс информационных систем – системы «интернета вещей» (IoT), которые обрели высокую коммерческую привлекательность за счет практического отсутствия роли человека-пользователя в осуществлении основных этапов информационного цикла.

Однако, несмотря на это, безопасность систем интернета вещей остается серьезной проблемой. Эти технологии все чаще становятся объектом атак злоумышленников, что подтверждается большим количеством статистических исследований.

Растущие угрозы безопасности требуют комплексного подхода к защите информации в системах IoT. Внедрение системы защиты информации (СЗИ) является необходимым, но недостаточным условием для поддержания требуемого уровня защищенности информации в информационной системе. На защищаемый объект непрерывно воздействуют различные дестабилизирующие факторы, влияние которых направлено на снижение достигнутого уровня защищенности информации в системе.

Именно поэтому вопросы управления информационной безопасностью (ИБ) имеют первостепенное значение.

Степень разработанности темы. В работе проведен анализ требований по управлению ИБ в информационных системах (ИС), содержащихся в федеральных нормативных документах (ФЗ, постановлениях Правительства, ГОСТах), а также в нормативных документах ФСТЭК.

В работе использованы результаты исследований, посвященные:

- проблемам ИБ в информационных системах в том числе оценки эффективности СЗИ, обнаружения инцидентов ИБ, вопросам формального моделирования процессов управления ИБ: Гвоздика Я.М., Коломойцева В.С., Лившица И.И., Буйневича М.В., Зегжды Д.П., Лаврова Д.С., Цирлова В.Л., Котенко И.В., Саенко И.Б., Минаева В.А., Астахова Л.В., Цимбола В.И., Карпова М.А., Липатникова В.А., Синдеева М.А., Косолапова В.С., Миняева А.А. Scott Barman, Brian Carrie;
- вопросам ИБ систем интернета вещей: Перри Ли, Самюэля Грингарда, Гиба Соребо, Зегжды Д.П., Кучерявого А.Е., Киричек Р.В., Дмитриева А.В., Камаляна Н.А., Ершова А.С., Довгаля В.А., Федорченко Е.В., Новикова Е.С., Котенко И.В., Гайфулина Д.А., Татарникова Т.М., Коломейца М.В., Бутенко Е.Д., Черникова И.С.;
- разработке систем поддержки принятия решений, характеризующихся высоким уровнем неустранимой неопределенности, обработке неформализованной (слабо формализованной) и нечеткой информации, в том числе использования таких систем для решения задач управления ИБ: Л. Заде, И. Мамдани, М. Такаги, М. Сугено, А. Пегата, Кудинова Ю.И., Пащенко Ф., Леоненкова А.В., Полещука О.М., Дойниковой Е.В., Федорченко А.В., Котенко И.В., Паращука И. Б., Цимбола В.И, Саенко И.Б.

Научная задача вытекает из выявленного в результате анализа существующего противоречия:

современное состояние информационной безопасности в системах IoT требует повышения эффективности управления информационной безопасностью – обеспечение высокой оперативности управления, точности управления (оптимизации вводимых контрмер по критериям стоимости и времени внедрения), выполнение нормативных требований по непрерывности управления;

при этом существующие взгляды и подходы к управлению ИБ ориентированы в основном на качественные оценки основных параметров процесса управления информационной безопасностью на основе неформальных моделей существенно ограничивают возможности повышения эффективности управления информационной безопасностью, соответствующей современным вызовам.

Целью диссертационного исследования является повышение эффективности управления ИБ систем IoT по критериям оперативности и точности управления посредством внедрения методики управления информационной безопасностью, основанной на предложенной комплексной модели управления ИБ в системе IoT.

Достижение поставленной цели предусматривает решение **следующих задач:**

1. Выполнить исследования современного состояния решения проблемы управления информационной безопасностью в системах Интернета вещей. В результате исследования обосновать необходимость формализации процессов управления информационной безопасностью в системах IoT и моделирования таких процессов в целях поддержания заданного уровня защищенности информации в системе в изменяющихся условиях.
2. Выполнить сравнительный анализ существующих методов моделирования систем с высокой степенью неустранимой неопределенности, в результате анализа выбрать методы моделирования для разработки комплексной модели процесса управления информационной безопасностью в системах Интернета вещей.
3. Предложить способы формализации и разработать комплексную модель процесса управления информационной безопасностью в системах Интернета вещей. Обосновать корректность и адекватность полученной модели.
4. Разработать методику настройки предложенной модели с учетом особенностей конкретной защищаемой системы Интернета вещей.
5. Провести оценку полученных результатов моделирования путем компьютерного и натурного исследований.
6. На основе разработанной комплексной модели предложить методику автоматизированного управления информационной безопасностью в системах Интернета вещей.
7. Разработать рекомендации по применению разработанной методики автоматизированного управления информационной безопасностью в системах IoT.

Объект исследования – процесс управления информационной безопасностью в системах Интернета вещей.

Предмет исследования – модели и методы реализации процесса управления информационной безопасностью в системе Интернета вещей.

Для решения поставленных задач использованы следующие методы исследования:

теория нечетких множеств и нечеткая логика, алгоритмы нечеткого моделирования, методы структуризации, методы экспертных оценок и сложных экспертиз, методы аналитического моделирования.

Границы исследования. В работе не рассматриваются отдельные методы и способы защиты информации, их содержание и особенности применения в системах IoT, в том числе относящиеся к организационно-правовой, физической, технической и криптографической защите информации. Используемые в СЗИ методы и способы защиты информации, формирующие ее структуру, учитываются в виде интегральной характеристики «Возможности СЗИ».

Не рассматриваются вопросы, связанные с ненадлежащим применением имеющихся в СЗИ средств и способов защиты информации (например, вопросы несвоевременного или некорректного обновления ПО, неполного использования возможностей аутентификации оконечных устройств и т.д.), а также проблемы, связанные с технической готовностью программно-аппаратных средств, включаемых в состав используемых средств защиты информации.

Не рассматриваются вопросы, связанные непосредственно с управлением системами IoT, проблематикой построения сетей IoT, сетевых протоколов и маршрутизации данных в сетях IoT.

Основные научные положения, выносимые на защиту:

1. Способ управления информационной безопасностью систем IoT посредством формирования и использования в системе управления отрицательной обратной связи в режиме численной оценки основных параметров процесса управления информационной безопасностью.

П. 18 - Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.

2. Комплексная модель процесса управления информационной безопасностью в системах IoT, реализующая принцип управления с обратной связью и обеспечивающая непрерывный замкнутый цикл оценки угроз.

П. 9 - Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

3. Методика управления информационной безопасностью в системах IoT с непрерывным замкнутым циклом нечеткой оценки угроз на основе разработанной комплексной модели.

П. 18 - Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.

Все результаты, выносимые на защиту, сопоставлены с пунктами 9 и 18 паспорта специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Научная новизна состоит в следующем:

1. Предложенный 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.

2. Разработанная новая комплексная модель процесса управления ИБ в системах IoT на основе способа управления ИБ с обратной связью учитывает полный цикл управления ИБ и обеспечивает возможность повышения эффективности управления по критериям оперативности и точности управления ИБ.

3. Предложенная методика автоматизированного управления ИБ в системах IoT с непрерывным замкнутым циклом нечеткой оценки угроз 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.

Теоретическая значимость результатов исследования заключается в формировании вклада в развитие теории и методов управления ИБ, а именно:

1. в разработке нового способа управления ИБ в информационных системах IoT, основанного на учете и 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 ИБ 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 работы:

1. Применение предложенной Методики управления ИБ в системах IoT на основе комплексной модели управления ИБ позволит повысить эффективность управления ИБ, обеспечит выполнение требования непрерывности управления ИБ, создает условия для автоматизированного управления ИБ.

2. Методика управления ИБ в системах IoT является адаптацией «Системы менеджмента информационной безопасности» (СМИБ) по ГОСТ Р ИСО/МЭК 270xx к особенностям информационных систем IoT, и может рассматриваться как способ формализации основных этапов внедрения СМИБ.

3. Результаты, полученные при выполнении диссертационного исследования, могут быть использованы владельцами информационных систем, использующих технологии IoT, администраторами ИБ для организации эффективного по введенным критериям управления ИБ с целью поддержания системы в требуемом состоянии защищенности информации в условиях постоянного воздействия различных дестабилизирующих факторов.

Внедрение результатов работы

1. Результаты диссертационного исследования используются в научно-производственной деятельности ООО «Эмбеддед Системс Рус» (г. Москва), специализирующейся на информационной безопасности систем Интернета вещей, а именно:

- программная реализация нечеткого ядра модели используется в повседневной деятельности для оценки уровня защищенности информации в системе IoT и определения необходимых контрмер;

- методика настройки параметров нечеткой модели под конкретную защищаемую систему.

2. Результаты диссертационного исследования используются в учебном процессе кафедры «Информационная безопасность» Московского технического университета связи и информатики (МТУСИ), а именно:

- способ управления информационной безопасностью Интернета вещей посредством формирования и использования в системе управления сигнала отрицательной обратной связи в режиме численной оценки основных параметров процесса управления используется в дисциплине «Основы информационной безопасности» для студентов бакалавриата по направлению 10.03.01 «Информационная безопасность»;

- 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», а также в дисциплине «Основы управления информационной безопасностью» для студентов бакалавриата по направлению 10.03.01 «Информационная безопасность».

Достоверность результатов диссертационной работы подтверждается соответствием результатов компьютерного моделирования с результатами экспериментальных данных, корректным использованием современного математического аппарата, а также рядом публикаций и обсуждением основных положений со специалистами на научных конференциях.

Апробация результатов

Основные результаты работы обсуждались и получили одобрение на 5 научных конференциях:

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

Публикации. Основные положения диссертации опубликованы в 10 научных работах, в том числе 4 в изданиях из перечня ВАК, сделано 5 докладов, опубликованных в сборниках

трудов международных научно-технических конференций.

Личное участие соискателя. Основные научные результаты, в том числе разработанный способ управления ИБ систем IoT, разработанная комплексная модель процесса управления ИБ в системах IoT, а также разработанная методика автоматизированного управления информационной безопасностью в системах IoT, получены автором лично. Вклад соавторов ограничивался постановкой задач на исследования и обсуждением полученных результатов.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

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

В первой главе выполнено исследование современного состояния решения проблемы обеспечения ИБ и управления ИБ в системах Интернета вещей. Выполнен анализ российской нормативно-правовой базы в области оценки риска информационной безопасности (требования ГОСТ Р ИСО/МЭК 27005-2010, конструкции ГОСТ Р ИСО/МЭК 15408-2012), анализ известных методов и методик оценки угроз и оценки рисков ИБ (FRAP, OCTAVE Allegro. Методики Microsoft, программного инструмента RiskWatch for Information Systems).

В представленном исследовании под управлением информационной безопасностью понимается процесс поддержания заданного значения показателя защищенности информации в системе IoT в условиях постоянного воздействия комбинации различных дестабилизирующих факторов.

В результате выполненного анализа установлено, что подход к управлению ИБ, лежащий в основе действующих нормативно-правовых документов и известных методик ориентирован на выполнение качественных оценок рисков ИБ на основе неформальных моделей этапов выполнения таких оценок: рекомендации по порядку проведения оценки угроз ИБ и идентификации актуальных угроз, выявление уязвимостей в защищаемой системе, определение модели нарушителя ИБ, идентификации информационных активов, оценке возможного ущерба пользователям и владельцам информационной системы и оценке рисков. Вместе с тем, качественные оценки рисков и других параметров модели управления, например уровня актуальных угроз в системе, не могут обеспечить оптимизацию выбора контрмер по критериям эффективности управления, таким как «оперативность управления ИБ» и «точность управления ИБ».

Выполнен анализ архитектуры информационных систем, использующих технологии Интернета вещей, выделены отличия от традиционных автоматизированных информационных систем, существенные для защиты информации в таких системах и управления ИБ:

- основные задачи обеспечения ИБ включают в себя обеспечение конфиденциальности, доступности и целостности информации в защищаемой системе на заданном уровне;
- особенности архитектуры и технологий IoT обусловливают невозможность применения или существенные трудности в применении целого ряда хорошо зарекомендовавших себя в АС методов и способов защиты информации;

- особенности архитектуры и технологий IoT размывают понятие информационного актива, что существенно затрудняет инвентаризацию активов и оценку предполагаемого ущерба от реализации угроз в системе;
- недостаточность правового регулирования со стороны государства вопросов ИБ в системах IoT затрудняет использование общих подходов к их решению, например таких как оценка эффективности систем СЗИ в IoT, а также вопросов, связанных с управлением ИБ.

В результате исследования обоснованы необходимость формализации процессов управления ИБ в информационных системах, использующих IoT-технологии, и формального моделирования таких процессов в целях поддержания заданного уровня защищенности информации в системе при постоянно изменяющемся контексте. Предложен обобщенный критерий эффективности управления ИБ в системах IoT и на его основе введены частные критерии эффективности управления, такие как «оперативность управления ИБ» и «точность управления ИБ».

В качестве критерия эффективности выбрано «поддержание заданного уровня защищенности информации в системе при минимизации затрат» и формализован в общем виде:

$$K_{\text{эфф}} = \begin{cases} R_t \ \to R_0 \\ C_t \ \to C_{min}, \\ T_t \to T_{min} \end{cases} \quad (1)$$

где: $K_{\text{эфф}}$ - критерий эффективности управления ИБ в системе IoT;

R_t - текущее значение показателя защищенности информации в системе;

R_0 - заданное ЛПР значение показателя защищенности информации в системе;

C_t - текущие затраты на приведение показателя защищенности информации в системе к требуемому значению R_0;

T_t - время, необходимое для приведения показателя защищенности информации в системе к требуемому значению R_0 при текущей дестабилизации в СЗИ при введении выбранных контрмер.

Значения C_{min} и T_{min} определяет ЛПР исходя из существующей политики безопасности.

Таким образом, на основе введенного общего критерия эффективности возможно определить частные критерии эффективности для управления ИБ в системах IoT:

1. Критерий K_1 «оперативность управления ИБ». Определятся на основе показателя эффективности «продолжительность T* пребывания защищаемой системы в состоянии $R_t < R_0$ после начала действия дестабилизирующего фактора», например выявления новой, ранее не учитываемой актуальной угрозы:

$$K_1 = T^* \xrightarrow[R_t < R_0]{} min \quad (2)$$

2. Критерий K_2 «точность управления ИБ». Определяется на основе показателя эффективности «стоимость затрат на возврат защищаемой системы к требуемому состоянию $R_t \geq R_0$ после начала действия дестабилизирующего фактора»:

$$K_2 = C_t \xrightarrow[R_t \geq R_0]{} min \qquad (3)$$

Во второй главе выполнено исследование возможности применения способа управления с обратной связью (по аналогии с автоматическим управлением) для разработки модели управления ИБ в системах IoT. Обратная связь обеспечивает возможность измерения текущего состояния защищаемой системы и сравнение его с желаемым (заранее заданным) состоянием. Текущее состояние системы определяется по одной или нескольким характеристикам системы, которые в модели управления ИБ будут являться выходной (выходными) переменными модели. При этом весь цикл управления рассматривается как последовательность этапов, что соответствует процессному подходу в управлении ИБ:

1. Генерация ошибки. На основе сравнения текущего и заданного состояния, обратная связь определяет ошибку, которая представляет собой модуль разницы между ними. Ошибка является информацией о том, насколько система отклоняется от заданного состояния.

2. Принятие решений. Принимая во внимание величину установленной ошибки, принимается решение о величине необходимой корректировки (величине управляющего воздействия) для достижения заданного состояния.

3. Корректировка. После принятия решений, блок управления осуществляет корректировку системы или процесса и обеспечивает возврат системы в заданное состояние.

Таким образом, способ управления ИБ с учетом обратной связи позволяет обеспечить точность и оперативность реагирования на изменения дестабилизирующих факторов. При этом достигается конечная цель – поддержание защищаемой системы IoT в заданном состоянии защищенности информации.

Одним из важнейших достоинств применения в управлении различными системами способа с обратной связью является то, что реализованные механизмы обратной связи позволяют автоматизировать процессы управления.

Выполнена интерпретация способа управления с обратной связью для модели управления ИБ. Для реализации обратной связи использована следующая модель (рис.1).

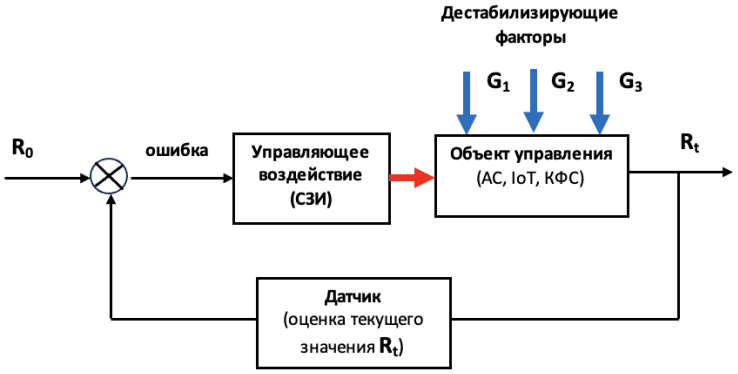

Рисунок 1. Структура модели процесса управления ИБ

R_t – текущее значение показателя уровня защищенности информации в системе;

R_0 – требуемое (минимально допустимое) значение показателя уровня защищенности информации в системе;

G_1 – дестабилизирующий фактор, характеризующий уровень актуальных угроз в

защищаемой системе;

G2 – дестабилизирующий фактор, учитывающий изменения в структуре защищаемой системы в соответствии с потребностями бизнеса;

G3 – дестабилизирующий фактор, учитывающий изменения в политике безопасности организации.

В качестве объекта управления выступает защищаемая система IoT, а управляемым параметром является показатель защищенности информации в системе.

Механизмом, генерирующим управляющие воздействия в системе управления ИБ является конкретная конфигурация СЗИ. Изменение конфигурации СЗИ, то есть изменение возможностей в сторону усиления защитных функций системы и определено в качестве управляющего воздействия.

В период, когда защищаемая информационная система не подвергается структурным изменениям для поддержки основных целей бизнеса, и политика безопасности организации остается неизменной, соответствующие дестабилизирующие факторы G_2 и G_3 могут не учитываться.

Выполнен сравнительный анализ современных представлений, моделей и методов в управлении ИБ, в результате которого установлено, что способ управления ИБ с выраженной обратной связью в известных методиках управления ИБ либо не учитывается, либо подразумевается в рамках неформализованных моделей для раскрытия характера процессов управления ИБ. Основной причиной такого положения являются трудности с численными оценками параметров процесса управления ИБ.

В результате проведенных исследований обоснован выбор методов моделирования, поддерживающих реализацию способа управления информационной безопасностью в системах IoT с использованием обратной связи в системе управления: методы нечеткого моделирования, экспертные методы, методы, основанные на структуризации моделируемой системы, методы формализации неструктурированной текстовой информации.

Введен критерий эффективности по точности управления ИБ на основе показателя эффективности K_2 (1) вида:

$$K_2 = \begin{cases} U_i \xrightarrow[C_{i+1} \le C_{max}]{} U_{i+1},\ R_t \ge R_o,\ C_{i+1} \to min \\ N_A \in F, F: \{R_t \ge R_o, C_{i+1} \le C_{max}, T_A \le T_{max}\} \end{cases}, \quad (4)$$

где:

U_i – конфигурация СЗИ до введения контрмер;

U_{i+1} – конфигурация СЗИ после введения в систему контрмер;

R_t – текущее значение показателя защищенности информации в системе;

R_0 – требуемое значение показателя защищенности информации в системе;

C_{i+1} – показатель, характеризующий затраты на введение необходимых контрмер для приведения системы в состояние требуемого значения показателя защищенности информации;

N_A – количество альтернативных контрмер, принадлежащих множеству F разрешенных контрмер, которые могут быть введены для обеспечения заданного показателя

защищенности информации в системе $R_t \geq R_0$ и отвечают ограничениям по затратам и времени на введение C_{max} и T_{max}.

Показатель эффективности управления ИБ «точность управления ИБ» для систем IoT определяется согласно выражению:

$$K_2 = \left(1 - \frac{1}{N_A}\right)^2, \quad (5)$$

где:

N_A – количество альтернативных контрмер, которые могут быть введены для обеспечения заданного показателя защищенности информации в системе $R_t \geq R_0$;

Достоинством предложенного способа управления ИБ для систем IoT является возможность при определении необходимых контрмер (т.е. изменения конфигурации СЗИ) численно оценивать уровень повышения защищенности информации в системе и делать обоснованный вывод о достаточности или недостаточности предполагаемого управляющего воздействия.

Выполнена предварительная оценка эффективности способа управления информационной безопасностью в системах IoT (рис. 2) и обоснована возможность повышения эффективности управления ИБ более чем на 40% в случае наличия 3-4 альтернативных решений по изменению конфигурации СЗИ в ответ на фиксируемое дестабилизирующее воздействие – изменение уровня угроз в системе. Оценка эффективности предложенного способа по введенному критерию выполнена для случая, когда имеется N_A альтернативных реакций системы на изменение текущего уровня угроз, причем выбор любого из них ЛПР равновероятен.

Таким образом обосновано, что способ управления информационной безопасностью Интернета вещей посредством формирования и использования в системе управления отрицательной обратной связи в режиме численной оценки основных параметров процесса управления реализуем практически и его применение способно повысить эффективность управления ИБ по сравнению с применяемыми способами по введенному критерию «точности управления».

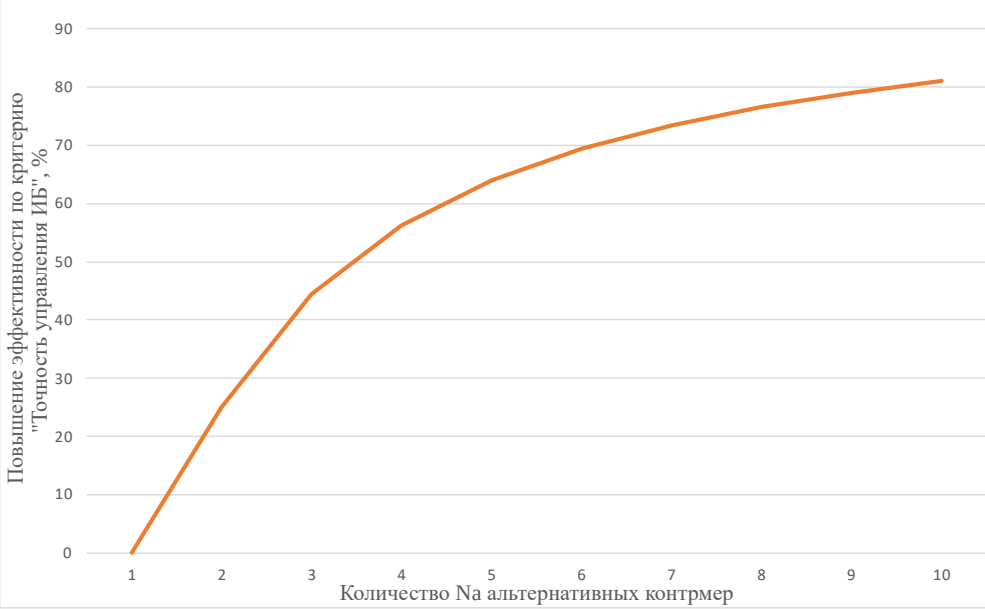

Рисунок 2. Оценка повышения эффективности управления ИБ в системах IoT с учетом обратной связи по критерию «точность управления ИБ»

Третья глава посвящена разработке комплексной модели процесса управления ИБ в системах Интернета вещей на основе структурного моделирования.

В качестве показателя защищенности информации в системе IoT введен показатель, характеризующий уровень защищенности информации в системе R_t в зависимости от текущего уровня актуальных угроз в системе G_t и уровня U возможностей СЗИ:

$$R_t = F(G_t, U) \quad (6)$$

В (6) оператор F не является числовой функцией или функционалом. Связь между параметрами модели определяется с помощью нечеткого вывода на правилах типа Мамдани.

Очевидно, что введенный показатель защищенности информации R_t в системе IoT не является выражением общего риска ИБ в защищаемой системе, однако в некоторых случаях он может быть приведен к понятию риск ИБ (7). Это может быть полезно при назначении ЛПР требуемого значения показателя защищенности информации в системе R_0 для обеспечения возможности сравнения R_0 и R_t.

$$R_{\text{общ}} = R_t * C_{max}\,, \quad (7)$$

где C_{max} – максимально возможный ущерб, который может быть причинен в результате реализации угрозы.

Приведены доказательства корректности и обоснование качественной адекватности разработанной модели. Разработана методика (алгоритм) настройки разработанной комплексной модели под особенности конкретной защищаемой системы Интернета вещей с целью повышения ее точности в соответствии с заданными требованиями.

Структура модели, показанная на рисунке 3, представляет собой совокупность нескольких связанных подмоделей.

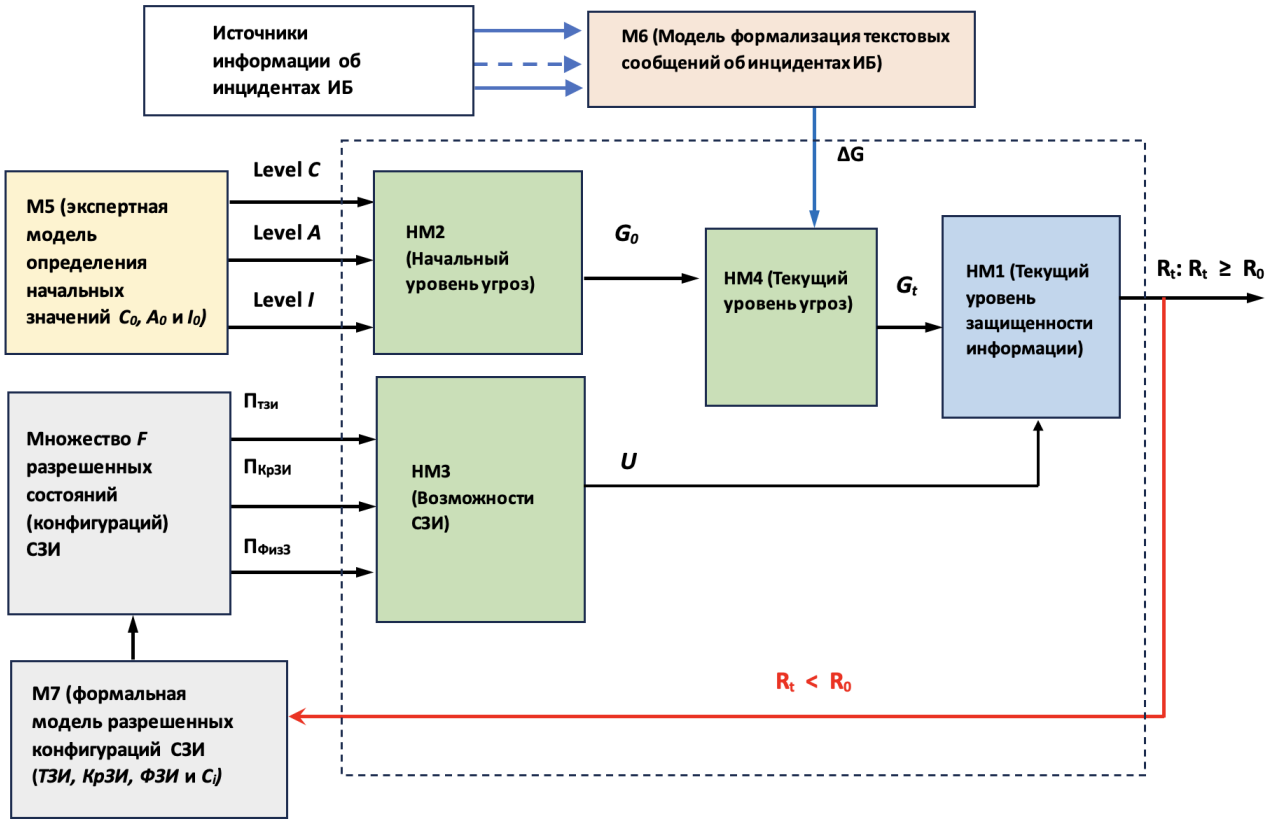

Рисунок 3. Структура комплексной модели управления ИБ в IoT системах

Центральное место занимает нечеткое ядро модели (на рис. 3 обозначена пунктиром), которое состоит из последовательности нечетких моделей типа Мамдани:

НМ1 (Общая) – предназначена для определения численного значения показателя уровня защищенности информации в системе (значения информационного риска) в зависимости от значения показателя текущего уровня угроз и показателя, характеризующего возможности СЗИ;

НМ2 (Угрозы) – предназначена для численного определения общего уровня угроз в системе в зависимости от уровней угроз нарушения конфиденциальности (Level C), доступности (Level A) и целостности (Level I);

НМ3 (СЗИ) – предназначена для численного определения показателя, характеризующего уровень возможностей текущей конфигурации СЗИ, учитывающий показатели уровней технической защиты, криптографической защиты и физической защиты;

НМ4 (Текущий уровень угроз) – предназначена для численного определения текущего уровня угроз в системе в зависимости от начального уровня угроз и текущих изменений угроз.

Основным назначением нечеткого ядра модели является оценка текущего уровня показателя защищенности информации в системе R_t. Для этого создается непрерывный замкнутый цикл нечеткой оценки угроз и численно определяются изменения относительно первоначального уровня угроз. Полученная численная оценка текущего уровня угроз в системе соотносится с показателем возможностей СЗИ, носящем интегральный характер.

Прагматическим назначением нечеткого ядра модели является согласование

разнородных подмоделей по масштабу и размерности через инструментарий лингвистических переменных.

Основные допущения (границы модели):

1. защищаемая система находится в относительно стабильном состоянии: не изменяется конфигурация системы, не пересматриваются положения политики безопасности в течение длительного времени;

2. R_0 – минимально допустимый уровень информационного риска в системе, определяется ЛПР;

3. C_{max} – максимально допустимые расходы на i-ю конфигурацию СЗИ, определяется ЛПР;

4. предложенная модель соответствует способу обработки риска - «снижение риска» по ГОСТ Р ИСО/МЭК 27005-2010.

М5 (Экспертная модель) – предназначена для определения начальных значений уровней актуальных угроз конфиденциальности C_0, доступности A_0 и целостности I_0 и поддерживает нечеткое ядро модели.

Модель М5 в целом соответствует вербальной экспертной модели, содержащейся в методическом документе ФСТЭК «Методика оценки угроз безопасности информации» (от 5 февраля 2021 г.) Приложение 2 «Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке угроз безопасности информации», с добавлением оценки согласованности мнения экспертов с помощью коэффициента вариации:

$$K = \frac{1}{X_{\text{ср}}}\sqrt{\frac{\sum_{i=1}^{n}\left(X_i - X_{\text{ср}}\right)^2}{n-1}} \leq 0{,}25\,, \qquad (8)$$

где $\boldsymbol{X_i}$ – оценка *i*-го эксперта;

$\boldsymbol{X_{ср}}$ – среднее значение оценки экспертов, $\boldsymbol{X_{ср}} = (\sum_{i=1}^{n} X_i)/n$;

$\boldsymbol{n}$ – количество экспертов.

Обобщенный алгоритм проведения экспертной оценки в модели М5 представлен на рис. 4.

Экспертная модель М5 активируется в следующих случаях:

1) на начальном этапе применения методики управления ИБ в системе IoT;

2) в случае существенного изменения структуры или конфигурации защищаемой системы;

3) в случае изменения политики безопасности.

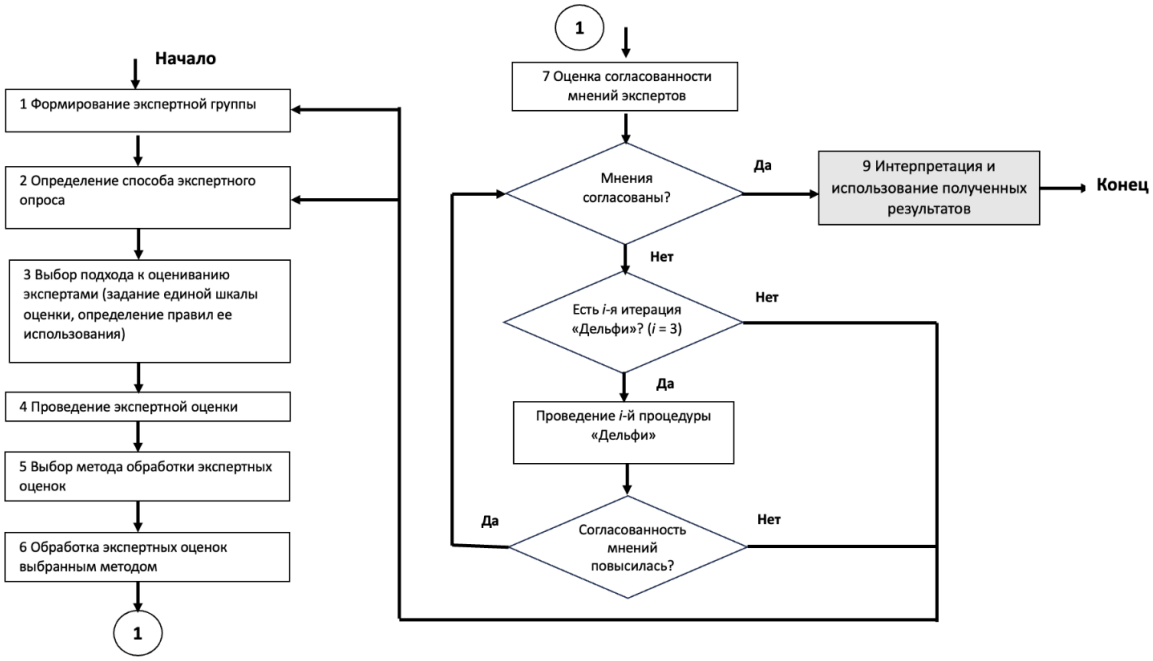

Рисунок 4. Обобщенный алгоритм проведения экспертной оценки в модели М5

В остальных случаях изменение уровня угроз в системе определяется с помощью формальной модели **М6** использующей информацию из текстовых сообщений об инцидентах ИБ из различных источников.

Модель формализации текстовых неструктурированных сообщений об инцидентах ИБ **М6** предназначена для идентификации вновь выявляемых угроз и соотнесении их с базовым «деревом угроз», которое также используется для работы модели **М4**. Таким образом модель **М6** позволяет фиксировать изменения выходной переменной нечеткой модели **НМ2** и тем самым отслеживать изменение уровня защищенности информации в системе (выходной переменной нечеткой модели **НМ1**).

Нечеткая модель НМ1.

Выходные переменные модели представлены в виде лингвистических переменных с 4 нечеткими множествами на непрерывной условной области определения [0…1]. (Рис.5 и 6). При отсутствии информации об особенностях конкретной информационной системы область определения разбита на термы равномерно.

Лингвистическое терм-множество переменной «Общий уровень угроз в защищаемой IoT систем» AL = {низкий, средний, высокий, критический} Лингвистическое терм-множество переменной «Возможности СЗИ» BL = {слабый, средний, сильный, высший}.

В качестве функции принадлежности использованы функции gauss2mf, и trimf посокольку они позволяют получить более сглаженный отклик на выходе модели: вычисляются нечеткие значения членства с помощью, основанной на сплайне, функции принадлежности, имеющей форму y = gauss2mf (x, params) или y = trimf (x, params) и возвращается вычисленное использование значений нечеткого членства основанной на сплайне функции принадлежности.

Задание лингвистической переменной возможно с помощью программной библиотеки scikit-fuzzy, написанной на языке программирования Python.

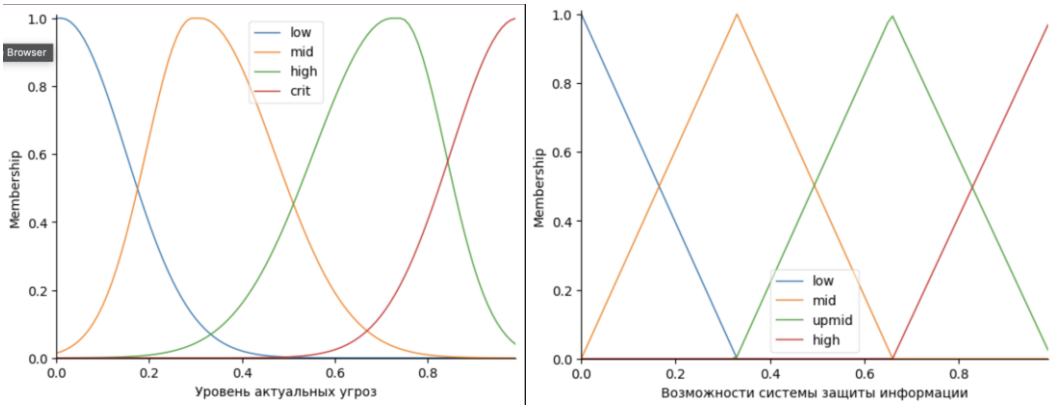

Рисунок 5. Представление входных переменных «Общий уровень актуальных угроз в защищаемой системы» и «Возможности системы защиты информации» в виде лингвистических переменных

Выходная переменная «Уровень защищенности информации в системе» также представлена с помощью четырех нечетких множеств на непрерывной области определения [0…1] с помощью функции принадлежности (gauss2mf). Эта функция вычисляет нечеткие значения членства с помощью гауссовой функции принадлежности (*y = gauss2mf(x,params*) возвращает вычисленное использование значений нечеткого членства следующей функции принадлежности в виде функции Гаусса с «закрепленными концами»:

$$f(x;a,b,c) = max\left(min\left(\frac{x-a}{b-a},\frac{c-x}{c-b},0\right)\right) \qquad \text{…….(9)}$$

Лингвистическое терм-множество выходной переменной «Состояние защищенности информации в системе» CL = {критический, низкий, средний, высокий}.

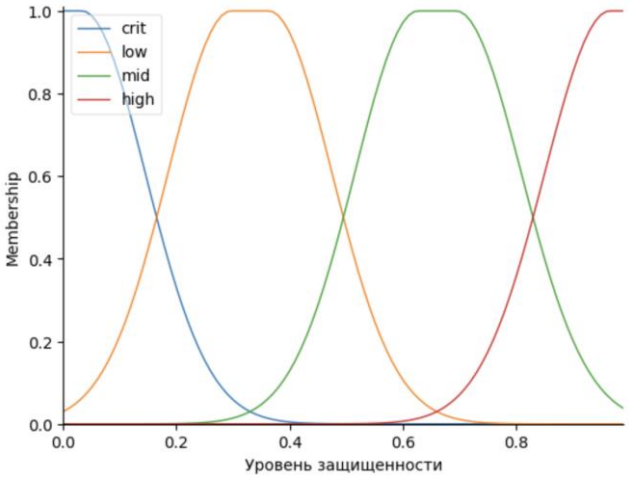

Рисунок 6. Представление выходной переменной «Уровень защищенности информации в системе» в виде лингвистической переменной

База правил нечеткой модели Мамдани представлена в таблице 1 и содержит 16 правил. Каждое правило в базе содержит условие и заключение и имеет вид:

R_1: ЕСЛИ (A = A_1) И (B = B_1) ТО (C = C_2)

R_{16}: ЕСЛИ (A = A_4) И (B = B_4) ТО (C = C_3)

Таблица 1. База правил нечеткой модели (вариант)

Уровень угроз / озможности СЗИ	A1 низкий)	A2 средний)	A3 ысокий)	A4 критич)
1 (низкий)	C2	C2	C1	C1
2 (средний)	C3	C2	C2	C1
3 (в-средний)	C4	C3	C3	C2
4 (высокий)	C4	C4	C3	C3

Параметры нечеткой модели НМ1 приведены в таблице 2.

Таблица 2. Параметры нечеткой модели НМ1

Параметры нечеткого вывода	Значения
And method	min
Or method	max
Implication	prod
Agregation	max
Deffazification	centroid

Для полного использования диапазона изменения выходной переменной использован метод дефаззификации Extended CS (расширенный центр сумм).

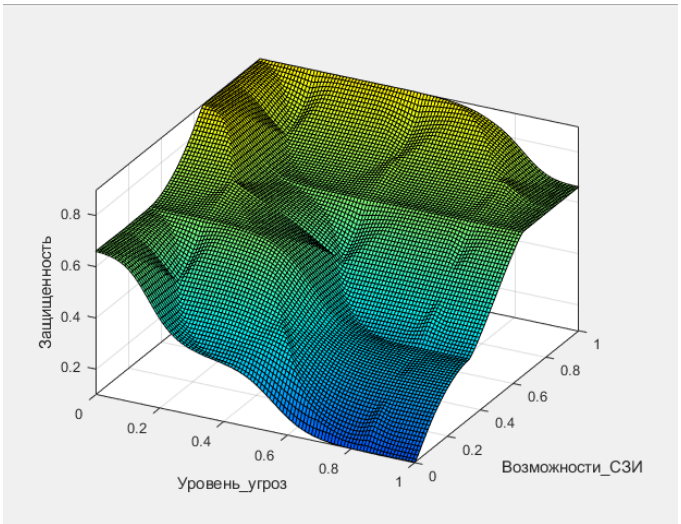

Рисунок 7. Графическая интерпретация поверхности нечеткой модели НМ1

Нечеткие модели НМ2 и НМ3 строятся по аналогичным принципам. Пример графической интерпретации решения нечеткой модели НМ2 показан на рис. 8.

Таким образом разработана комплексная модель процесса управления ИБ в системах IoT на основе предложенного способа управления ИБ с обратной связью, обоснована качественная адекватность модели и подтверждена ее корректность.

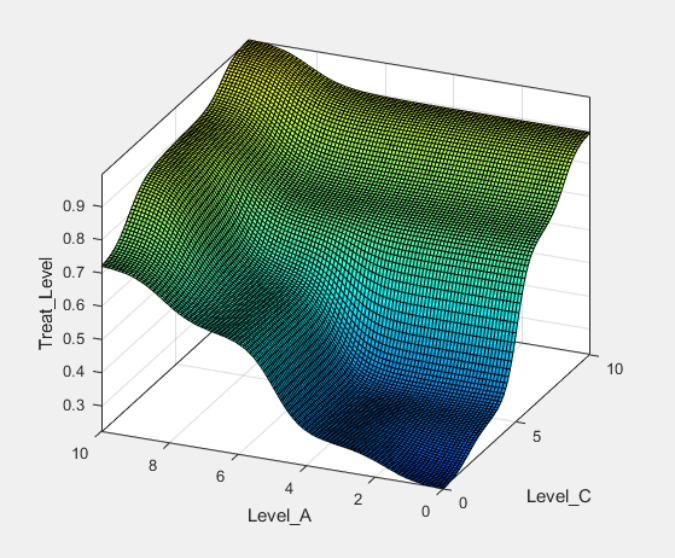

Рисунок 8. Зависимость общего уровня угроз в защищаемой системе (Treat Level) от уровня угроз конфиденциальности (Level C) и доступности (Level A) информации

Проведена оценка эффективности разработанной комплексной модели по введенному критерию оперативности управления ИБ.

Показатель эффективности «оперативность управления» определен на основе введенного критерия К1 «оперативность управления ИБ» (10):

$$П_2 = 1 - \frac{T_1}{T_{max}}, \quad (10)$$

где T_1 – временной интервал между проявлением новой угрозы (не учтенной в базовом «дереве угроз») и определением контрмер, необходимых для возвращения уровня защищенности информации в системе к заданному, ч;

T_{max} – временной интервал, аналогичный T_1, но в случае применения для оценки угроз только метода экспертных оценок, ч.

На рис. 9 и 10 представлены результаты оценки эффективности предложенной Методики по критерию «оперативность управления ИБ».

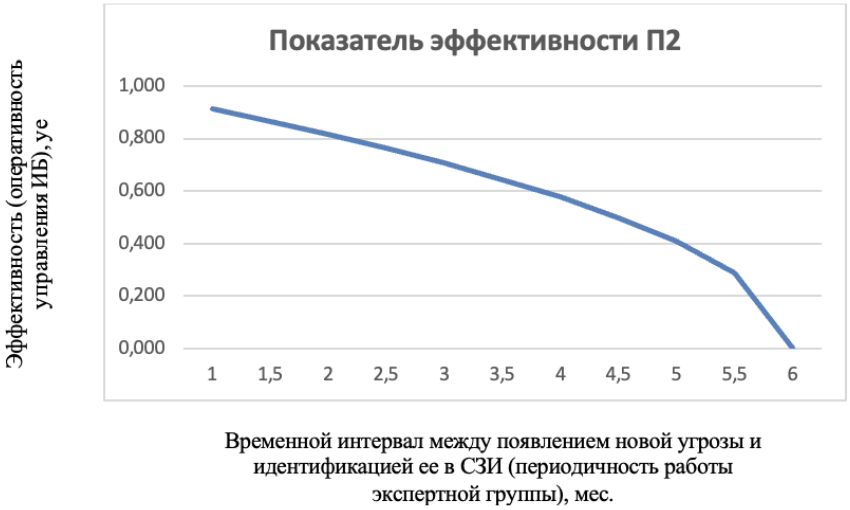

Рисунок 9. Зависимость эффективности управления ИБ от продолжительности T_1, (традиционный способ управления)

Для оценки значений $П_2$ принято T_{max} 2200 часов (примерно 3 месяца).

Оценка оперативности управления ИБ в предложенной комплексной модели позволяет принять значение T_1 – 72 часа.

Эффективность управления ИБ при практическом использовании разработанной комплексной модели при заданных параметрах составит 0,97. При этом эффективность «ручного» управления ИБ с использованием для оценки угроз только метода экспертных оценок, с частотой сбора экспертной группы 1 месяц – 0,67. При таких параметрах эффективность организации управления ИБ в системе IoT в соответствии с разработанной комплексной моделью будет выше традиционных методов управления ИБ более чем на 30%.

Рисунок 10. Зависимость эффективности управления от продолжительности T_1, (в рамках разработанной комплексной модели управления ИБ)

В четвертой главе представлена разработанная Методика автоматизированного управления информационной безопасностью в системах Интернета вещей на основе предложенной комплексной модели в виде сетевой структуры (алгоритма) рис.11.

Методика, реализующая предложенный способ управления ИБ, представляет собой совокупность взаимосвязанных этапов, реализующих разработанную комплексную модель.

Методика содержит два этапа – предварительный (установление контекста управления) и раздел, реализующий автоматизированное управление ИБ.

Предварительный этап.

1. Проведение экспертной оценки начальных уровней базовых угроз информации в системе IoT и реализует предложенную экспертную модель **M5**. Основное назначение модели – определение численных значений начального уровня угроз конфиденциальности (**level C_0**), целостности (**level A_o**) и доступности (**level I_o**) информации в защищаемой системе на основании активации интуиции и опыта экспертов и предоставленных им знаний о структуре защищаемой системе, характере информационного массива и характеристик среды безопасности.

2. Формирование пула используемых источников информации. Необходимо определить источники информации об инцидентах ИБ в системах IoT или других типах информационных систем. Это могут быть новостные ленты информационных агентств, релизы

вендоров и разработчиков ПО, релизы компаний, осуществляющих мониторинг вредоносного ПО и т.д. Кроме того, необходимо определить параметры формализации полученной неструктурированной информации и способ формализации – «вручную» специалистом или с помощью специального ПО.

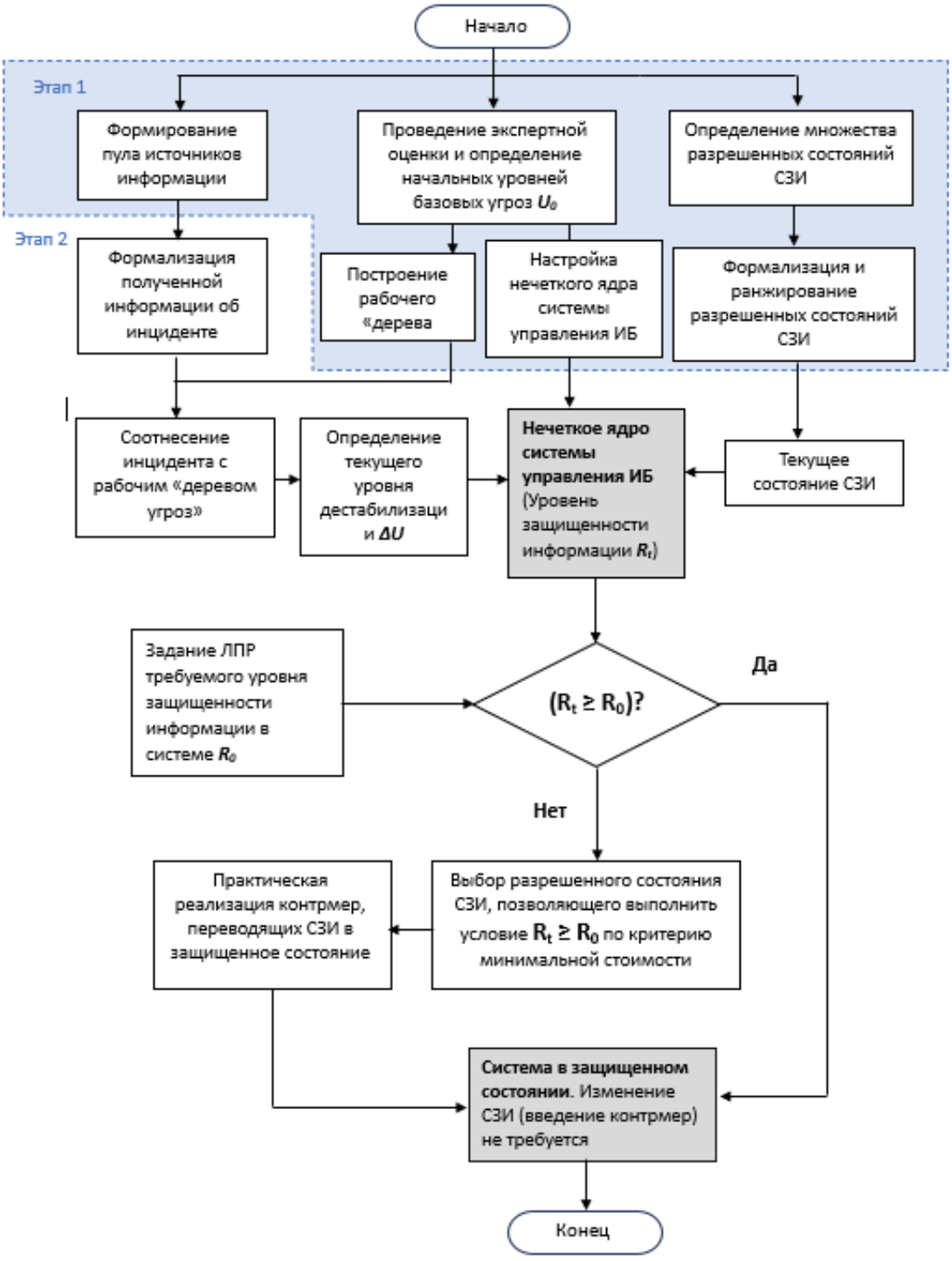

Рисунок 11. Структурная схема Методики автоматизированного управления информационной безопасностью в системах Интернета вещей

3. **Определение множества *F* разрешенных состояний (конфигураций) СЗИ** как совокупности контрмер, относящихся к техническим, физическим и криптографическим мерам. Отнесение ***i***-ой конфигурации СЗИ к множеству разрешенных состояний производится при одновременном выполнении следующих условий:

- реализация i-й конфигурации технически реализуема;
- стоимость i-й конфигурации C_i не превышает стоимости C_{lim}, установленной ЛПР;
- время перехода от (*i-1*)-ой конфигурации T_0 к i-ой не превышает времени T_{lim}, установленного ЛПР.

После определения множества F выполняется формализация и ранжирование разрешенных состояний СЗИ.

Этап, реализующий автоматизированное управление информационной безопасностью.

Необходимо установить на специализированный сервер ПО «Программа для управления информационной безопасностью систем Интернета вещей» свидетельство 2024615772 от 13.03.2024г.

При вводе исходных данных (предварительный этап) в автоматизированном режиме определяется текущий уровень угроз в системе (U), наличие дестабилизирующего фактора (ΔU). При учете текущего состояния СЗИ определяется текущий уровень защищенности информации в системе (R_t), который сравнивается с заданным уровнем R_0. При обнаружении снижения текущего уровня защищенности ниже заданного уровня выбор необходимых дополнительных контрмер, т.е. изменение конфигурации СЗИ осуществляется из имеющихся альтернатив по критерию минимальной стоимости $C_i \le C_{lim}$, $C_i \rightarrow \min$. Такой выбор может быть осуществлен администратором безопасности или в автоматизированном режиме как рекомендация системы управления.

Разработаны рекомендации по практическому применению предложенной Методики управления ИБ в системах IoT. Основными рекомендациями, в целях повышения эффективности по критерию оперативности управления ИБ можно считать:

- использование максимально возможного количества источников информации;
- настройка нечеткого ядра в соответствии с особенностями конкретной защищаемой системы IoT;
- предпочтение формализации информации об инцидентах ИБ программными методами.

В результате выполненной работы разработана Методика автоматизированного управления информационной безопасностью в системах IoT на основе разработанной комплексной модели процесса управления ИБ.

ЗАКЛЮЧЕНИЕ

В результате диссертационного исследования решена актуальная научная задача и достигнута поставленная цель, состоящая в повышение эффективности управления ИБ в системах, использующих технологии IoT, по критериям оперативности и точности управления ИБ.

Это подтверждается следующими полученными научными и практическими результатами:

1. В результате проведенного исследования современного состояния решения проблемы управления ИБ в системах IoT обоснована необходимость формализации процессов управления информационной безопасностью в системах IoT и моделирования таких процессов в целях поддержания заданного уровня защищенности информации в системе в изменяющихся условиях и обеспечения непрерывности, оперативности и точности управления.

2. В результате выполненного сравнительного анализа существующих методов моделирования систем с высокой степенью неустранимой неопределенности выбраны методы моделирования, оптимальные в смысле поставленной задачи – разработки модели процесса управления информационной безопасностью в системах Интернета вещей.

3. Используя результаты проведенных исследований предложен способ формализации на основе отрицательной обратной связи

4. Разработана комплексная модель процесса управления информационной безопасностью в системах Интернета вещей. Обоснована корректность и адекватность модели.

5. В результате выполненной оценки полученных результатов моделирования путем компьютерного и натурного исследований обоснована реализуемость разработанного подхода к управлению информационной безопасностью в системах, использующих технологии IoT.

6. На основе разработанной комплексной модели предложена методика автоматизированного управления информационной безопасностью в системах Интернета вещей. Обоснована эффективность предложенной методики по введенным критериям эффективности – «точность управления» и «оперативность управления» информационной безопасностью.

7. Разработаны рекомендации по практическому применению предложенной комплексной модели управления информационной безопасностью в системах IoT, направленные на повышение эффективности предложенной методики по введенным критериям.

Все поставленные задачи исследования выполнены, цель работы достигнута.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ 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. DOI 10.36724/2409-5419-2022-14-6-12-19

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. 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

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. DOI: 10.36724/2409-5419-2024-16-4-4-11

Программы для ЭВМ

5. 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. – EDN KSZKSL.

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. – EDN AAQFSV.

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. – EDN PSZNHY.

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. – EDN HLQIXV.

Подписано в печать 24.04.2025. Формат 60×84 1/16.
1,0 а.л. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1