МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ»

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»

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
Кандидат технических наук,
Ларин Александр Иванович

Москва - 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4

Глава 1. Исследование современного состояния проблемы обеспечения информационной безопасности и управления информационной безопасностью в системах Интернета вещей 23

1.1 Характеристика системы интернета вещей как объекта защиты 23

1.2 Анализ проблематики обеспечения информационной безопасности Интернета вещей 30

1.3 Анализ проблемы управления информационной безопасностью в системах, использующих технологии Интернета вещей 36

Выводы 42

Глава 2. Способ управления информационной безопасностью в системах Интернета вещей посредством формирования и использования в системе управления обратной связи в режиме численной оценки основных параметров .. 44

2.1 Анализ современных представлений, моделей и методов в управлении информационной безопасностью 44

2.2 Способ управления информационной безопасностью в системах IoT на основе учета обратной связи 52

2.3. Оценка эффективности предложенного подхода к управлению информационной безопасностью в системах интернета вещей 58

Выводы 61

Глава 3. Комплексная модель процесса управления информационной безопасностью в системах Интернета вещей 63

3.1 Постановка задачи моделирования процесса управления ИБ в системах IoT 63

3.2 Показатель защищенности информации в системе 71

3.3 Общая структура комплексной модели процесса управления ИБ в системах IoT 75

3.3.1 Нечеткое ядро комплексной модели (НМ1-НМ4) 78

3.3.2 Экспертная модель М5 83

3.3.3 Модель М6 формализации тестовых сообщений об инцидентах ИБ 88

3.4 Оценка влияния разработанной модели на повышение эффективности управления ИБ 92

Выводы 94

Глава 4 Методика автоматизированного управления информационной безопасностью в системах IoT на основе разработанной комплексной модели 96

4.1 Анализ известных методик управления ИБ 96

4.2 Методика автоматизированного управления информационной безопасностью в системах IoT на основе разработанной комплексной модели 102

4.3 Рекомендации по практическому применению предложенной Методики управления информационной безопасностью в системах IoT 108

Выводы 109

Заключение и вывод по работе 111

Список сокращений и обозначений 113

Список использованной литературы 114

Приложения 128

Приложение А. Сведения о государственной регистрации «Программа для управления информационной безопасностью систем Интернета Вещей» 128

Приложение Б. Копия акта внедрения в ООО «Эмбеддед Системс Рус» 129

Приложение В. Копия акта внедрения в учебный процесс Московского технического университета связи и информатики 130

ВВЕДЕНИЕ

Актуальность темы исследования. Информационная безопасность в последние годы является значимой и важной сферой национальной безопасности Российской Федерации, что отражено в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 г. N 400 [1]. Основные положения Стратегии, касающиеся безопасности государства в информационной сфере, конкретизированы и закреплены в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 5 декабря 2016 г. № 646 [2]. В соответствии с Доктриной информационные технологии в настоящее время приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности общества и государства. Расширение областей и сфер применения информационных технологий значительно увеличивает опасность появления новых угроз информационной безопасности. Зарубежные специальные службы расширяют сферы и повышают возможности информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира, что в конечном итоге направлено на подрыв суверенитета и нарушение территориальной целостности других государств. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере. В сфере обороны страны, в области государственной и общественной безопасности, в экономической сфере, в области науки, технологий и образования, в области стратегической стабильности и равноправного стратегического партнерства государством определены стратегические цели для обеспечения эффективного состояния информационной безопасности [2].

Одновременно с ростом и развитием информационных технологий развиваются тактики, техники и способы реализации проведения атак, расширяется инструментарий для нарушения состояния информационной безопасности.

Обеспечение необходимого уровня защищенности информации в информационных системах на сегодняшний день является важнейшей задачей

информационной безопасности. Не менее важно поддерживать защищенность информации в системе на достигнутом уровне в условиях постоянных изменений среды безопасности: появления новых, ранее не идентифицированных угроз информационной безопасности, мутации известных угроз, вскрытие ранее не учтенных уязвимостей в защищаемой системе, а также изменений архитектуры и структуры защищаемой системы.

В результате бурного развития IT-технологий на современном этапе выделяется отдельный класс информационных систем – системы «интернета вещей». Отличительными признаками таких систем являются [33]:

- практическое отсутствие роли человека-пользователя в осуществлении основных этапов информационного цикла – создание информации, передачи данных, хранения данных, обработки данных и принятие решений в результате такой обработки, исполнение принятых решений;
- обязательное наличие среди различных типов используемых в системе каналов передачи данных глобальной сети Интернет;
- использование в системе в качестве источников информации «вещей», в качестве которых понимается широкий круг разнородных понятий – «предмет», «объект» и «сущность».

Как дополнительные отличия часто указываются [40]:

- существенно большее по сравнению с традиционными автоматизированными системами (АС) число подключенных к сетям объектов;
- существенно меньшие размеры подключенных объектов и относительно невысокие скорости передачи данных.

Таким образом, сама концепция интернета вещей поддерживается тремя базовыми принципами:

1) повсеместно распространенная коммуникационная инфраструктура;

2) глобальная идентификация каждого объекта или сущности («вещи»);

3) возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет при обеспечении бесперебойной и надежной работы.

Благодаря указанным отличиям от традиционных АС, а также безусловной коммерческой привлекательности, информационные системы, использующие технологии интернета вещей, получили мощный импульс развития, что подтверждается мировой статистикой. Так, по данным авторитетных источников ГидМаркет, Stratistics MRS, TAdviser тенденция бурного роста технологии Интернета вещей в мире и в России на сегодняшний день сохраняется. На рис.1 представлена динамика роста количества подключенных sim-карт M2M в системах IoT в мире, на рис.2 показана динамика выручки от коннективити M2M в системах IoT у операторов сотовой связи в России.

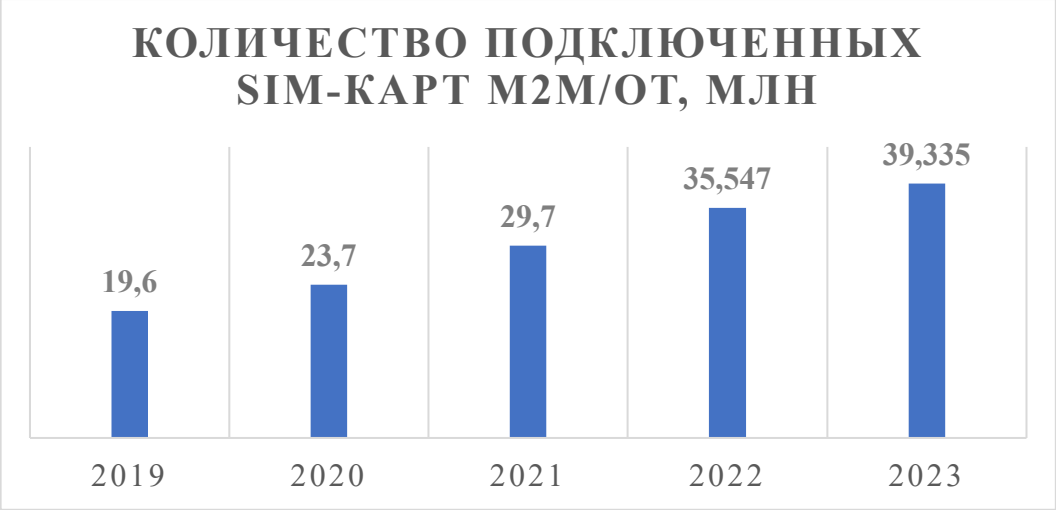

Рисунок 1 – Динамика ежегодного роста количества SIM-карт, подключенных к интернету вещей в мире (млн.шт.)

Рисунок 2 – Динамика экономического роста интернета вещей в России

Вместе с тем, объективно действуют факторы, тормозящие развитие технологий IoT, главным из которых является проблема обеспечения информационной безопасности [45]. Системы и устройства интернета вещей все чаще становятся целями для злоумышленников различного рода. Результаты исследования, проведенные специалистами Dr.Web показывают, что менее чем за три последних года количество попыток взлома и заражения устройств Интернета вещей возросло на 13 497% (рис. 3). Согласно исследованию Zscaler с 2022 по 2023 год на 400% увеличено количество атак вредоносного ПО для систем интернета вещей.

Рисунок 3 – Динамика роста количества атак на устройства интернета вещей

Таким образом, возможно констатировать наличие современного вызова – при сохранении объективной тенденции количественного и качественного роста технологии интернета вещей проблемы информационной безопасности также усугубляются, что приводит к увеличению рисков, связанных с значительными материальными и информационными потерями, созданию угрозы жизни и здоровью людей, экологическими и другими проблемами.

Основными задачами обеспечения ИБ в системах, использующих технологии интернета вещей, являются:

1) поиск и внедрение методов и способов защиты информации, учитывающих специфику такого класса информационных систем, главным образом методов идентификации и аутентификации оконечных устройств, защиту коммуникаций от удаленных сетевых атак, противодействие реализации атак типа

«отказ в обслуживании» (DoS), перехват данных, передаваемых по открытым каналам, способы физической защиты оконечных устройств и др.;

2) разработка и внедрение практически реализуемых и эффективных методик управления информационной безопасностью, как комплекса мероприятий, направленных на поддержание заданного уровня защищенности информации в системе.

Задача эффективного управления информационной безопасностью при этом представляется более значимой, так как даже при наличии возможности применения известных контрмер как реакции на изменение уровня информационных рисков в системе, неоптимальный выбор контрмер и несвоевременное их внедрение существенно снижает защищенность информации в системе.

Возможности синтеза систем защиты информации (СЗИ), обеспечивающих достаточно высокий уровень защищенности информации, в настоящее время, имеются: разработаны общие и частные методы защиты информации от угроз нарушения конфиденциальности, доступности и целостности в автоматизированных системах (АС), существует большой арсенал способов реализации этих методов. Для других классов информационных систем – систем, использующих технологии IoT, а также киберфизических систем, проводятся исследования по возможности адаптации известных методов защиты информации (например, идентификация и аутентификация по M2M), а также разрабатываются новые методы защиты.

Синтез и внедрение СЗИ является необходимым, но недостаточным условием для поддержания требуемого уровня защищенности информации в информационной системе. На защищаемый объект (информационную систему) постоянно действуют различные дестабилизирующие факторы, влияние которых направлено на снижение достигнутого уровня защищенности информации в системе.

Именно поэтому на первый план выходят вопросы управления информационной безопасностью, которые включают следующие основные этапы

[12]:

1) инвентаризация информационных активов;

2) оценка уровня актуальных угроз информационной безопасности по каждому информационному активу и по системе в целом;

3) анализ уязвимостей в защищаемой системе;

4) качественная и количественная оценка рисков и выбор актуальных способов обработки рисков информационной безопасности;

5) выбор и применение необходимых контрмер в рамках выбранных способов обработки рисков (например, снижения рисков) и, тем самым, поддержание заданного уровня защищенности информации в системе.

Степень разработанности темы. В работе проведен анализ требований по управлению информационной безопасностью в информационных системах (ИС), содержащихся в федеральных нормативных документах (ФЗ, постановлениях Правительства, ГОСТах) [1-15, 23-25, 27-30], а также в руководящих и методических документах ФСТЭК [17-22].

Проблемы информационной безопасности в информационных системах, в том числе оценки эффективности СЗИ, обнаружения инцидентов информационной безопасности, вопросам формального моделирования процессов управления информационной безопасностью отражены в работах Гвоздика Я. М., Коломойцева В. С., Чемина А. А., Лившица И. И., Буйневича М.В., Зегжды Д. П., Барабанова А. В., Лаврова Д. С., Цирлова В. Л., Котенко И. В., Саенко И. Б., Минаева В. А., Бондаря К. М., Вайц Е. В., Белякова И. 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, Jason T.Luttgens, Matthew Pepe, Kevin Mandia и др. [43, 44, 48-52, 54, 57, 58-71, 84, 85].

Вопросам информационной безопасности систем интернета вещей, в том числе проблемам мониторинга рисков и угроз в системах, использующих технологии интернета вещей, посвящены работы зарубежных и отечественных исследователей: Перри Ли, Самюэля Грингарда, Гиба Соребо, Кирич Р.В.,

Кучерявого А.Е., Зегжды Д.П., Дмитриева А.В., Камаляна Н.А., Ершова А.С., Громыко П.С., Осанова В.А., Довгаля В.А., Федорченко Е.В., Новикова Е.С., Котенко И.В., Гайфулина Д.А., Тушканова О.Н., Левшуна Д.С., Мелешко А.В., Муренина И.Н., Коломейца М.В., Бутенко Е.Д., Черникова И.С., аналитические материалы компании TAdviser «Интернет вещей» и блог компании Доктор Веб «Интернет вещей» [40, 41, 45, 47, 48, 52, 53, 72, 73, 78-80].

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 информационной безопасностью, ряда российских и зарубежных ученых: Л. Заде, И. Мамдани, М. Такаги, М. Сугено, Т. Саати, Н. Вилема, М. Иржи, А. Пегата, Кудинова Ю. И., Пащенко Ф., Штовбы С. Д., Леоненкова А. В., Полещука О. М., Хованова Н. В., Дойниковой Е. В., Федорченко А. В., Котенко И. В., Новиковой Е. С., Паращука И. Б., Аникина И. В., Астаховой Л. В., Цимбола В. И. и др. [34-38, 49, 50, 55, 58, 86].

Работа Карпова А. М. [54] посвящена управлению системой информационной безопасности объекта критической инфраструктуры (КИИ). Представлена разработанная методика управления информационной безопасностью на основе аналитической математической модели, использующей вариационное представление систем, приводятся результаты разработки алгоритма эффективного управления, позволяющего уменьшать пространство состояний управляемого объекта. Представленная методика позволяет спрогнозировать количество итераций управления в зависимости от сегмента пространства состояний и выбранного количества переходов. Предполагается, что такой подход позволит воздействовать на сложные динамические системы в реальном времени, при сокращенных затратах на вычислительные мощности системы управления и её подсистем. В качестве алгоритма управления в методике применяется принцип сценарно-шагового управления, основой которого является концепция ситуационного управления разнородными системами, базирующаяся на

построении матрицы сценариев, учитывающих возможные пространства состояний системы и соответствующие характеристики. В качестве цели управления информационной безопасностью объекта критической информационной инфраструктуры автор указывает повышение эффективности функционирования объекта управления, при этом критерием эффективности определено такое решение на оптимальное управляющее воздействие, при котором убывает значение функции эффективности управления, зависящей от состояния управляемой системы и управляющих воздействий. Модель и методика, предложенные автором, предназначена для автоматизированных систем без привязки к классам, уровням защищенности и категориям значимости информационных систем КИИ. Вопросы учета актуальных угроз безопасности информации и постоянного изменения общего уровня угроз в информационной системе автором не рассматривались, также не учитывалась специфика систем, использующих технологии интернета вещей.

В работе исследователей Военной академии связи имени С.М. Буденного под руководством Липатникова В.А. [59] для выявления и проведения анализа возможных нарушений информационной безопасности предложено внедрение интеллектуальной системы с целью снижения степени субъективизма, повышение обоснованности и достоверности суждений при управлении кибернетической безопасностью. Представлена разработанная методика поддержки принятия решений администратором информационной системы в условиях кибератак на основе нечеткой когнитивной карты - направленного и ориентированного графа, в котором ключевые факторы объекта представлены как вершины графа и называются концептами, который описывает состояние информационной системы. Нечеткая когнитивная карта позволяет прогнозировать векторы атак, отображающие действия нарушителя, объекты информационной системы, на которые происходит атака и результаты возможной реализации таких воздействий. Авторы считают, что представленная методика, реализующая нечеткую когнитивную модель, обеспечит повышение эффективности обеспечения кибернетической безопасности и работы системы управления и администратора за

счет уменьшения времени необходимого на анализ и обработку рисков, а также за счет повышения точности прогнозов и обработки событий. Методика рассчитана на управление кибербезопасностью и не охватывает другие аспекты информационной безопасности. Не формализованы вводимые показатели эффективности управления безопасностью, такие как уменьшение времени, необходимого на анализ и обработку рисков, и повышение точности прогнозов и обработки событий. В методике не рассмотрены такие этапы процесса управления информационной безопасностью как выбор управляющего воздействия (контрмеры) на изменение уровня угроз в системе, также не учитывалась специфика систем, использующих технологии интернета вещей.

Работа Аникина И.В. [55] посвящена исследованию методов и алгоритмов количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики. Предложена формальная модель защищенности корпоративной информационной сети (КИС), описывающая различные виды активов и особенности их взаимодействия для решения задачи количественной оценки рисков ИБ, на основе которой разработаны алгоритмы нечеткой оценки ущерба от реализации угроз, при этом использованы подходы к количественной оценке частных показателей ущерба, нечеткой оценке уровней критичности активов и формальной модели КИС, а также нечетких оценок возможностей реализации угроз и использования уязвимостей при отсутствии защитных мер в условиях неопределенности исходной информации. Полученные алгоритмы позволили автору предложить метод повышения эффективности защиты информации в КИС на основе управления рисками ИБ с учетом модели защитных мер, нечеткой оценки рисков ИБ и разработать технологию количественной оценки и управления рисками ИБ в КИС. Такая технология может быть преобразована в методику управления информационной безопасностью в корпоративных информационных сетях, для чего автором представлен инструментальный комплекс программ для нечеткой оценки и управления рисками информационной безопасности в КИС, реализующего разработанные технологию, методы и алгоритмы. Для решения поставленных задач использовались теоретико-

множественный подход, методы экспертных оценок и методы нечеткого моделирования.

Понятие эффективности управления в работе сведено к экономическому показателю эффективности в виде

$$K(z_i) = \frac{Выгоды(z_i) - П\_Затраты(z_i)}{E\_затраты(z_i)},$$

где:

- $Выгоды(z_i) = \Delta R = Risk(T) - Risk(T)\{z_i\}$ – выгоды от реализации защитной меры z_i в единицу времени (например, год); $Risk(T) = \Sigma Risk(T_j)j$, $Risk(T)\{z_i\} = \Sigma\, Risk(T_j)\{zi\}j$ – нечеткие суммарные уровни риска в единицу времени по всем угрозам $T_j \in T$ без учета и с учетом реализации защитных мер соответственно;
- $E\_затраты(z_i)$ – единовременные затраты на реализацию защитной меры zi (оцениваются экспертом);
- $П\_Затраты\ (z_i)$ – дополнительные постоянные затраты на реализацию защитной меры zi в единицу времени.

Предложенная автором методика, при несомненной практической значимости, ограничена учетом только технических мер защиты и ориентирована в большей степени на класс удаленных сетевых угроз. Кроме того, применение представленной методики для систем интернета вещей требует дополнительных исследований. Использование же для оценки эффективности управления ИБ только экономического (ресурсного) показателя не вполне соответствует современным представлениям об эффективности информационных технологий, которые предполагают для оценки эффективности использование совокупности ресурсных и функциональных критериев [89, 90]. Несомненным достоинством предложенного решения является разработанный механизм выбора ответных мер (совокупности контрмер) из множества допустимых при учете условий финансовых ограничений.

В исследовании Чемина А. А. [62] сформулированы основные положения, лежащие в основе подхода к оценке эффективности выполнения политик

безопасности в зависимости от идентифицируемых инцидентов информационной безопасности и предложена методика расчета количественной оценки уровня защищенности информационной системы. При этом в работе не учитываются такие показатели оценки эффективности, как: требования по ИБ, степень противодействия угрозам безопасности информации, а также ресурсные показатели эффективности (учет материальных затрат на создание СЗИ). Степень детализации задач оптимизации состава комплекса средств защиты информации при разработке СЗИ и применении контрмер в процессе эксплуатации представляется недостаточной. Предложенная автором методика расчета количественной оценки уровня защищенности информации также не учитывает особенности систем интернета вещей и ее применимость к этому классу систем требует дополнительных исследований.

В работе группы исследователей СПб ФИЦ РАН Федорченко Е.В., Новикова Е.С., Котенко И.В., Гайфулина Д.А. и др. [91] предложена система измерения защищенности информации и персональных данных для пользователей устройств интернета вещей, которая позволяет автоматически вычислять показатели защищенности информации и персональных данных и формировать на их основе интегральную оценку защищенности информации и персональных данных. Предложена методика численной оценки рисков в условных единицах в диапазоне [0, 10] для отдельных компонентов систем интернета вещей на основе использования вектора отличий D между вектором прав доступа на основе описаний и вектором реальных прав доступа используя введенные показатели эффективности, для чего используются аналитические представления и имитационные модели. Предложенная система обладает несомненными достоинствами, важным из которых является возможность логически понятной и обоснованной численной оценки защищенности информации в системах интернета вещей, вместе с тем оценка защищенности является лишь этапом в процессе управления ИБ, то есть предложенная система не охватывает весь процесс управления. Кроме того, авторы в своем подходе разделяют общую информацию и персональные данные и используют терминологию «обеспечение защищенность

информации и конфиденциальности персональных данных», что соответствует различным зарубежным подходам и методикам, но в некотором смысле находится в противоречии с терминологией основных нормативных документов РФ [2, 4-6, 8-20].

В исследованиях Миняева А. А. [84, 85] представлена разработанная автором методика оценки эффективности системы защиты территориально-распределенных информационных систем.

В качестве показателей эффективности системы защиты информации предложены: перечень актуальных угроз безопасности информации, перечень требований по ИБ с учетом классификации конкретной ИС, а также перечень применяемых средств защиты информации и их стоимость. Эффективность СЗИ, по мнению автора, достигается при следующих необходимых условиях: нейтрализации угроз, выполнении требований по ИБ и наименьшей стоимости применяемых средств защиты из предлагаемых вариантов. Численные значения показателей предложенных показателей эффективности определяются с помощью квантилей.

Предложенная методика характеризуется «непрозрачными» решениями, например понятие «нейтрализация угрозы» носит качественный характер, для формирования перечня требований по ИБ применен «табличный» подход, что соответствует стандартам информационной безопасности 1-го поколения, которые в специализированной литературе считаются устаревшим и не соответствующим современному уровню развития информационных технологий. Для практической реализации методики автором предложено решение на основе нечеткой нейронной продукционной сети ANFIS с применением алгоритма TSK, реализованной на языке программирования Python 3, однако общая блок-схема алгоритма реализации методики автором не представлена, что затрудняет ее понимание.

При этом методика имеет внутреннюю логику и представляется инструментом, способным сравнивать альтернативные конкурирующие решения при проектировании СЗИ и планировать мероприятия, направленные на повышение эффективности СЗИ по введенным критериям.

Вместе с тем, разработанная методика ограничена оцениванием эффективности СЗИ и не охватывает всех аспектов процесса управления информационной безопасностью, кроме того, применение предложенной автором методики для систем, использующих технологии интернета вещей, не рассматривалась.

Таким образом, приведенные результаты анализа проработанности проблематики управления информационной безопасностью IoT-систем подтверждают вывод о необходимости совершенствования методов и методик эффективного управления информационной безопасностью в системах, использующих технологии интернета вещей, и тем самым подтверждает актуальность настоящего диссертационного исследования.

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, что существенно ограничивает 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 **частных 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 математического 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, оптимальные в смысле поставленной задачи – 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: методы аналитического и статистического представления систем, теория нечетких множеств и нечеткая логика, алгоритмы нечеткого моделирования, методы структуризации, методы экспертных оценок и сложных экспертиз, методы формализации неструктурированной информации.

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

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».

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.

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.

Практическая ценность 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 с непрерывным замкнутым циклом нечеткой оценки угроз пользуется 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.

Глава 1. Исследование современного состояния проблемы обеспечения информационной безопасности и управления информационной безопасностью в системах Интернета вещей

1.1 Характеристика системы интернета вещей как объекта защиты

Интернет вещей (Internet of Things. loT) традиционно рассматривается как инфраструктура взаимосвязанных сущностей, систем и информационных ресурсов, а также служб, позволяющих обрабатывать информацию о физическом и виртуальном мире и реагировать на нее [26].

Интернет вещей — концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой. Предполагается, что организация таких сетей способна перестроить экономические и общественные процессы, исключить из части действий и операций необходимость участия человека.

В словосочетании «Интернет вещей» «вещи» буквально означают любые вещи или предметы, которые подключаются к Интернету и друг к другу [39]. Примерами таких «вещей» могут быть компьютер, планшет, смартфон, лампочка, дверной замок, двигатель самолета, и все, на что хватит фантазии архитектора, разрабатывающего конкретную систему, использующую концепцию Интернета вещей. Каждое из этих устройств («вещей») имеет уникальный идентификационный номер и IP-адрес, то есть по сути является хостом. Эти объекты подключаются с помощью различных каналов передачи данных, проводных или беспроводных, таких как:

- средняя и дальняя зоны - спутниковая связь, сотовая связь (стандарты 3G, 4G-LTEA, 5G-NR);
- ближняя зона - Wi-Fi, Bluetooth, Zigbee, Z-Wave и др.

Независимо от того, какая архитектура используется в конкретном случае, технологии Интернета вещей подразумевают возможность перемещения данных для управления процессами на любые расстояния.

В действующем государственном стандарте ГОСТ Р ИСО/МЭК 29161-2019 [23] (идентичен международному стандарту ISO/IEC 29161:2016 «Information technology - Data structure - Unique identification for the Internet of Things», IDT) термин «вещь» трактуется достаточно широко и рассматривается как синоним понятий: «предмет», «объект» и «сущность».

Вещью может быть личность, объект или место нахождения, в зависимости от рода деятельности специалиста, рассматривающего тему интернета вещей». Если специалист связан с областью датчиков, то под интернетом вещей он подразумевает расширение сети датчиков. Если он связан с областью радиочастотной идентификации, то для него интернет вещей - расширение инфраструктуры радиочастотной идентификации. Если он связан с картографическими данными, то под интернетом вещей он подразумевает расширение сети, базирующейся на географических пунктах. Если он связан с телекоммуникационной областью, то под интернетом вещей он подразумевает расширение сети телекоммуникаций. Все эти определения являются верными [23].

В представленном исследовании под интернетом вещей в большей степени рассмотрено расширение сети датчиков.

Таким образом система IoT – это с одной стороны информационная система, реализующая концепцию и технологии Интернета вещей, с другой стороны – это техническая система, представляющая собой совокупность элементов, ее составляющих, и связей между ними, а также имеющая цель (а чаще всего цели) ее существования. Такая система может быть представлена как совокупность подсистем (применяя известные методы структуризации). При таком подходе объединение элементов в подсистему может быть выполнено по признакам обеспечения выполнения локальных задач в системе или по признаку участия в том или ином этапе информационного цикла.

Для синтеза систем IoT необходимо наличие широко выпускаемых компонентов, способных реализовывать локальные задачи внутри системы и создавать необходимые связи для собственно объединения этих компонентов в систему. Для конкретизации понятия компонентов системы вводится понятие

экосистемы, то есть совокупности компонентов, формирующих сегменты применяемых информационных технологий [38] (Таблица 1.1).

Полный спектр различных вариантов на всех уровнях IoT-архитектуры от оконечного устройства (датчика) до центра обработки информации и принятия решений (облака) представлен на рис. 1.1.

Таким образом, Интернет вещей основан на трех базовых принципах:

- во-первых, повсеместно распространенную коммуникационную инфраструктуру;
- во-вторых, глобальную идентификацию каждого объекта или сущности («вещи»);
- в-третьих, возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет, к которой он подключен, при бесперебойной и надежной работе.

Таблица 1.1. Экосистема Интернета вещей

Наименование сегмента экосистемы	Основные используемые технологии
Оконечные устройства • датчики, • исполнительные устройства	Встроенные системы, операционные системы реального времени, источники бесперебойного питания, микроэлектромеханические системы (МЭМС)
Системы связи между оконечными устройствами	Каналы передачи данных – зона охвата персональных сетей от 0 до 100 м; для обмена данными между датчиками могут применяться низкоскоростные маломощные информационные каналы, которые часто построены не на протоколе IP
Локальные вычислительные сети	Системы обмена данными на основе протокола IP, например 802.11 Wi-Fi-сеть для быстрой радиосвязи
Агрегаторы, маршрутизаторы, шлюзы	Встроенные системы и модули (процессоры, динамическая оперативная память и системы хранения данных), инфраструктура туманных вычислений, инструментарий для граничной аналитики, безопасность граничных устройств, системы управления сертификатами
Глобальная вычислительная сеть	Сотовая связь, спутниковая связь, маломощные глобальные сети (Low-Power Wide-Area Network, LPWAN), транспортные протоколы интернета для IoT и сетевых устройств (MQTT, CoAP)
Облако	Инфраструктура и платформа в качестве поставщиков услуг, базы данных, поставщики услуг потоковой и пакетной обработки

	данных, ПО и озер данных, программно-определяемы сети, сервисы машинного обучения
Анализ данных	Работа с большими объемами данных – комплексная обработка событий, аналитики, приемов машинного обучения
Безопасность	На каждом уровне необходимо обеспечить конфиденциальность, доступность и целостность информации. Основной принцип – в цепи не должно быть «слабых» звеньев, поскольку предполагается, что интернет вещей станет главной целью для хакерских атак в мире в самое ближайшее время.

Рассматривая систему интернета вещей как совокупность элементов и связей между ними, объединенных для достижения целей существования такой системы, можно отметить основные характеристические признаки, позволяющие выделять системы интернета вещей в отдельный класс информационных систем:

1) практическое отсутствие роли человека-пользователя в осуществлении основных этапов информационного цикла – создание информации, передачи данных, хранения данных, обработки данных и принятие решений в результате такой обработки, исполнение принятых решений;

2) обязательное (в большинстве случаев) наличие среди различных типов используемых в системе каналов передачи данных глобальной сети Интернет;

3) использование в системе в качестве источников информации «вещей», в качестве которых понимается широкий круг разнородных понятий – «предмет», «объект» и «сущность».

Кроме указанных ключевых отличий от традиционных автоматизированных систем (АС) можно также указать и дополнительные отличия, встречающиеся в специализированной литературе, а также в ПНСТ 419—2020 [26]:

- фокус на вещах, а не на человеке;
- существенно большее число подключенных объектов;
- существенно меньшие размеры объектов и невысокие скорости передачи данных;
- фокус на считывании информации, а не на коммуникациях;
- необходимость создания новой инфраструктуры и альтернативных стандартов.

Эти отличия менее формализованы, так как сложно оценить такие понятия как «существенно меньшие размеры», «невысокие скорости», «фокус» и проч., тем более, что непрерывно развивающиеся технологии интернета вещей, включение в состав систем таких источников информации как IP-камеры, сложные комбинированные датчики физических величин ставят под сомнение такой признак как «невысокие скорости передачи данных», а значит и использовать такие отличительные признаки для четкого разграничения одного типа информационных систем (например, АС) от другого (IoT).

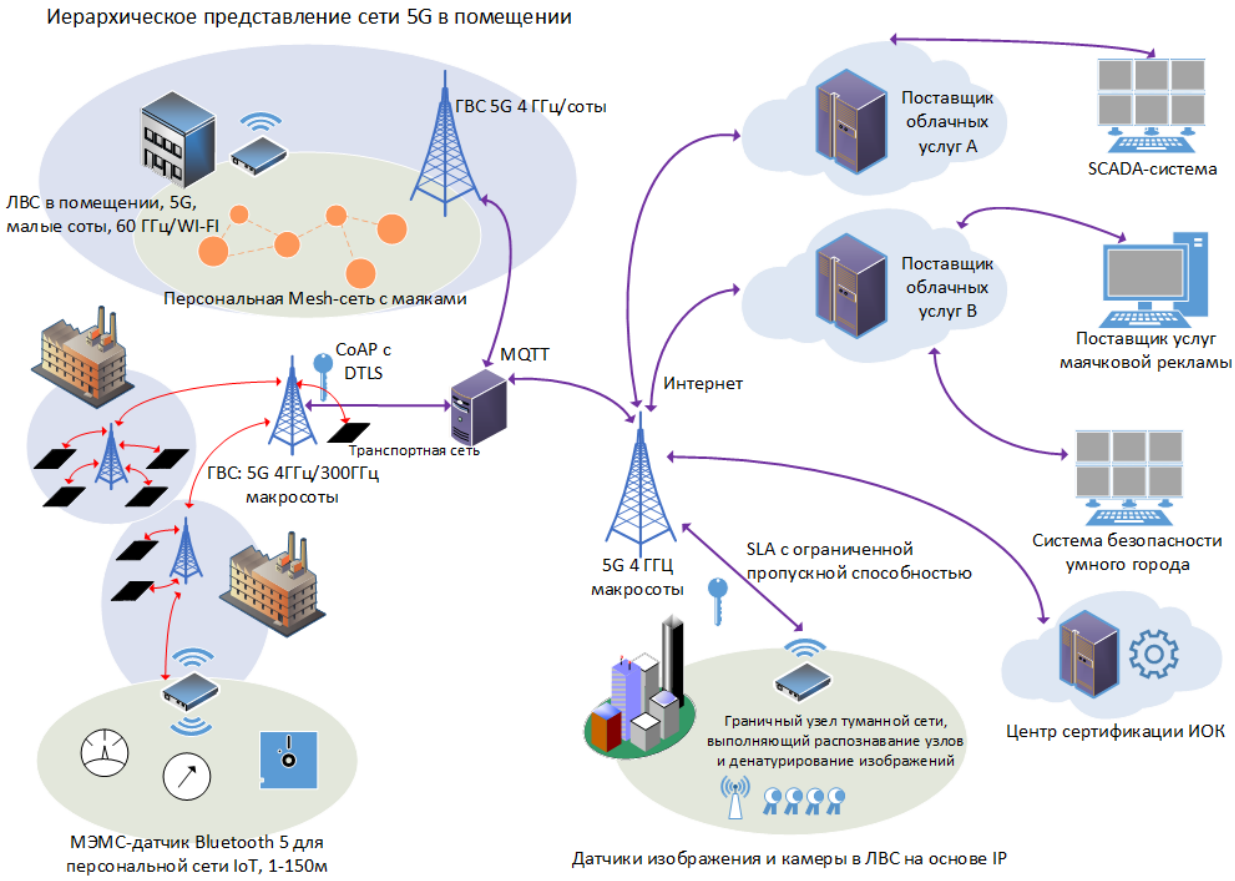

Рисунок 1.1 Полный спектр различных вариантов на всех уровнях IoT-архитектуры от оконечного устройства (датчика) до центра обработки информации и принятия решений (облака)

В настоящее время технологии Интернета вещей находятся на этапе роста как в России, так и во всем мире.

По оценкам аналитического агентства Oneside, всего в 2022 году количество подключенных IoT-устройств в России превысило 70 млн. Несмотря на то, что традиционным примером реализации технологии Интернета вещей является

концепция «умного дома», самыми распространенными сценариями использования M2M и IoT-технологий в 2022 году стали системы безопасности, подключенные камеры видеонаблюдения, интеллектуальные системы для транспорта и умные системы учета расхода воды и энергоресурсов.

К концу 2023 года общее количество подключенных IoT-устройств в России в сегментах B2B/B2G выросло до 55,8 млн. шт, из которых 34,2 млн работало в сетях телеком-операторов. Затраты государства и бизнеса в РФ на внедрение M2M и IoT составили почти 114 млрд рублей [102]. Темпы роста количестве устройств, подключенных к Интернету вещей в России представлены на рис. 1.2.

Рисунок 1.2 Динамика роста технологии интернета вещей в России по оценкам TAdviser [58]

Достоверные статистические данные, свидетельствующие о ежегодном росте количества инцидентов ИБ в системах интернета вещей в открытом доступе отсутствуют, чему есть объективные причины: по большей части такие системы носят коммерческий характер, поэтому владельцы систем не стремятся обнародовать факты нарушения информационной безопасности, опасаясь репутационных потерь, и кроме того, на сегодняшней день не существует информационных технологий, подобных ГосСОПКА, собирающих такую информацию в законодательно-обязательном порядке. Однако отдельные факты инцидентов известны в свободном доступе, что позволяет обоснованно

предполагать, что обеспечение надлежащей защиты миллиардов устройств из категории «Интернет вещей» исключительно важно.

Что касается определения свойств информации, содержащейся в системах IoT, рассматриваемых с точки зрения объекта защиты, то здесь также присутствует достаточно высокая степень лингвистической неопределенности. Кроме так называемых «базовых» свойств информации – конфиденциальности, доступности и целостности [49] в государственном стандарте ГОСТ Р 70924-2023 «Информационные технологии. Интернет вещей. Типовая архитектура» [103] в разделе 7.2 «Характеристики доверенности системы ИВ», посвященном отдельно выделяются «защита персональных данных», «достоверность», «способность к восстановлению» и «безопасность». Конфиденциальность, доступность и целостность объединены в свойство «защищенности». Кроме того, в документе упоминается «приватность», однако четкого определения этому понятию в документе не дается. Анализ приведенных в стандарте определений и примеров показывает, что «способность к восстановлению» является одним из известных методов обеспечения доступности информации, раскрытие понятия «достоверности» («отсутствие или искажение данных», важных для принятия решений в системе IoT) сводится к обеспечению доступности и целостности в системе. «Защита персональных данных» как характеристика доверенности системы ИВ может быть сведена к обеспечению конфиденциальности информации в системе.

Беря во внимание то, что в преамбуле ГОСТ Р 70924-2023 есть указание о том, что «вопросы безопасности выходят за рамки положений настоящего стандарта и являются объектом стандартизации профильных национальных технических комитетов» [103], возможно считать, что перечисленные характеристики доверенности системы ИВ (приватность, достоверность, способность к восстановлению, защита персональных данных) являются уточнением и конкретизацией «базовых» характеристик информации – конфиденциальности, доступности и целостности, как объекта защиты для систем

IoT и не являются самостоятельными свойствами информации, ортогональными базовым.

Таим образом, характеризуя системы IoT как объект защиты, можно отметить следующее:

1) основные задачи обеспечения информационной безопасности включают в себя обеспечение конфиденциальности, доступности и целостности информации, содержащейся в защищаемой системе, на заданном уровне;

2) особенности архитектуры и технологий интернета вещей обусловливают невозможность применения или существенные трудности в применении целого ряда хорошо зарекомендовавших себя в АС методов и способов защиты информации;

3) кроме того, особенности архитектуры и технологий интернета вещей в некотором смысле размывают понятие информационного актива и могут существенно затруднить инвентаризацию информационных активов в системе;

4) недостаточность правового регулирования со стороны государства вопросов информационной безопасности 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 информационной безопасностью.

1.2 Анализ проблематики обеспечения информационной безопасности Интернета вещей

Еще в 2007 г. исследователи показали, что электрогенератор может быть дистанционно выведен из строя путем его быстрого включения-выключения с помощью автоматического выключателя. В 2014 г. злоумышленники взломали промышленную сеть немецкого сталелитейного завода и заблокировали остановку доменной печи. И, наконец, совсем недавно в общественно-политическом телешоу «60 минут» специалисты Агентства по перспективным оборонным научно-исследовательским разработкам США (Defense Advanced Research Projects Agency, DARPA) продемонстрировали дистанционное управление автомобильными

тормозами в беспилотном транспортном средстве, получив несанкционированный доступ к информации [59].

Наблюдения аналитиков компании «Dr.Web» начиная с 2016 года фиксировали относительно низкую активность вредоносных программ, нацеленных на устройства Интернета вещей.

В качестве способа исследования была развернута сеть специализированных приманок — ханипотов (honeypot — горшочек с медом). Такие ловушки имитируют различные типы «умных» электронных устройств и регистрируют попытки их заражения. Ханипоты охватывают сразу несколько аппаратных платформ, в числе которых ARM, MIPS, MIPSEL, PowerPC и Intel x86_64. Они позволяют отслеживать векторы атак, обнаруживать и исследовать новые образцы вредоносных программ, улучшать механизмы их обнаружения и более эффективно бороться с ними.

За четыре месяца 2016 года специалисты «Dr.Web» выявили 729 590 атак, однако всего через год — в 32 раза больше, 23 741 581. Еще через 12 месяцев их было уже 99 199 434. Что же касается 2024 года, то лишь за первые шесть месяцев было совершено 73 513 303 атаки — почти столько же, сколько за весь 2018 год.

Менее чем за три года количество попыток взлома и заражения устройств Интернета вещей возросло на 13 497%. Атаки на «умные» устройства выполнялись с IP-адресов, расположенных в более чем 50 странах. Чаще всего это были США, Нидерланды, Россия, Германия, Италия, Великобритания, Франция, Канада, Сингапур, Индия, Испания, Румыния, Китай, Польша и Бразилия [60].

Рисунок 1.3. Зафиксированные ханипотами атаки на устройства Интернета вещей

После успешной компрометации устройств злоумышленники могут загружать на них одного или нескольких троянцев. В общей сложности число уникальных вредоносных файлов, обнаруженных за время наблюдения, составило 131 412. Динамика их выявления показана на рис.1.4.

Рисунок 1.4. Количество уникальных вредоносных файлов, атакующих системы IoT

Используя полученные статистические результаты, можно сделать вывод о тенденции в сфере угроз для «умных» устройств в области кибербезопасности:

- из-за доступности исходных кодов троянцев, таких как Linux.Mirai, Linux.BackDoor.Fgt, Linux.BackDoor.Tsunami и др., растет количество новых вредоносных программ;
- появление все большего числа вредоносных приложений, написанных на «нестандартных» языках программирования, например Go и Rust;
- злоумышленникам доступна информация о множестве уязвимостей, эксплуатация которых помогает заражать «умные» устройства;
- сохраняется популярность майнеров, добывающих криптовалюты (преимущественно Monero) на устройствах Интернета вещей.

Проблемы обеспечения информационной безопасности в системах интернета вещей условно можно разделить на две группы:

- противодействие хищению персональных данных и данных, раскрывающих информацию о поведении владельца и проч. – подпадает под действие государственных нормативных актов (Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006г.)

- противодействие нарушению работы систем интернета вещей (функциональная безопасность), то есть обеспечение конфиденциальности, доступности и целостности, нормативными актами не регламентируется.

Регулирование вопросов обеспечения информационной безопасности интернета вещей со стороны государства носит противоречивый и непоследовательный характер. На сегодняшний день можно констатировать отсутствие специального государственного стандарта, посвященного регламентированию вопросов обеспечения информационной безопасности в системах Интернета вещей, более того в открытых источниках отсутствует информация о том, что такой стандарт вообще разрабатывается.

Кроме того, можно признать, что деятельность регулирующих органов государственной власти в отношении проблем информационной безопасности интернета вещей не соответствует современным вызовам, при этом интересы непрерывности бизнес-процессов рассматриваются как безусловно приоритетные по отношению к обеспечению информационной безопасности.

Например, 8 июля 2021 года, Министерство цифрового развития, связи и массовых коммуникаций РФ решило отказаться от идеи по регистрации SIM-карт, устанавливаемых в банкоматах, счетчиков электроэнергии и другом оборудовании Интернета вещей.

Как сообщает РБК со ссылкой на проект постановления Правительства РФ, разработанный ведомством, юридические лица и индивидуальные предприниматели не должны вносить сведения о своих IoT-устройствах в Единую систему идентификации и аутентификации (ЕСИА), если договор об оказании услуг связи был заключен до 1 июня 2021 года.

Обоснованием для такого решения послужило мнение, что регистрация SIM-карт устройств Интернета вещей влечет за собой «большой и сложно реализуемый объем работы» и риски того, что большое количество техники, например банкоматы, перестанут работать, так как их функциональность напрямую зависит от оказываемых услуг связи [78].

Однако, недостаточная защищенность тех же банкоматов от сетевых атак различного типа может также быть причиной того, что банкоматы «перестанут работать», только при этом такая ситуация может усугубиться значительным материальным ущербом.

В месте с тем, в настоящее время, у технологии Интернет-вещей с точки зрения безопасности информации есть множество существенных недостатков. По мнению ряда специалистов одним из важнейших недостатков считается низкий уровень безопасности личных данных пользователей [101].

По оценке компании Hewlett-Packard, больше 70% вещей с доступом к сети Интернет, имеют уязвимость, связанную с небезопасным web-interface, а также проблемы вызывает слабая защищенность IP-адресов и их портов [102].

В результате взлома злоумышленники получают данные своих жертв, а также информацию о структуре и характеристиках системы, которые в дальнейшем используются по усмотрению злоумышленников. В случае, если атакованная система имеет определенную суммарную производительную мощь, злоумышленник может использовать это для нападения на определенные ресурсы (посредством организации DOS-атак). А учитывая огромное количество подключенных к сети устройств, даже при небольшой вычислительной мощности отдельного устройства, это может представлять системную угрозу. Если же целью злоумышленника является эта конкретная система Интернета вещей, то полученная им информация позволит осуществить свои преступные замыслы.

Начиная с 2016 года в качестве инструмента для взлома Интернета-вещей начинают использовать Botnet (англ. Robot network – рус. сеть роботов). Это группа из зараженных программ, объединенных в одну сеть. Взломы с помощью Botnet, показали, что, несмотря на свое удобство, технология Интернета вещей является небезопасной и нуждается в доработке.

Таким образом можно утверждать, что обеспечение безопасности технологии Интернета-вещей – это актуальная на сегодняшний день задача, решение которой еще не найдено [47]. Вместе с тем, необходимо и возможно по крайней мере

осознавать структуру проблематики обеспечения информационной безопасности Интернета вещей.

1. Прежде всего, существует неопределенность в конкретизации собственно объекта защиты. Говоря об информационных системах, использующих технологии интернета вещей, очевидно, что сам термин «интернет вещей» подразумевает очень разные системы и по составу, и по целям, и по размеру предполагаемого ущерба, и по количеству потенциальных «жертв» – от «умных домов» до систем управления транспортом в городах, систем управления технологическими процессами, в том числе повышенной экологической опасности (IIoT) и т.д. При этом общепринятой классификации по каким-то важным классификационным признакам в настоящее время не существует. Между тем, конкретизируя тип объекта защиты, появляется возможность построения более точной модели «угрозы-уязвимости-риски информационной безопасности».

2. В отличие от традиционных АС существует проблема арсенала эффективных методов и способов защиты информации именно для систем интернета вещей. Так, например, многие, хорошо зарекомендовавшие себя в АС способы аутентификации неприменимы в ситуации M2M (биометрия, использование заранее известной пользователю-человеку нетривиальной информации и т.п.). Применение систем обнаружения вторжений (СОВ/IDS) уровня хоста, защищающие информационные активы в АС от сетевых атак изнутри системы, также весьма затруднено в системах интернета вещей по причине огромного количества устройств, имеющих собственный IP (хостов) и их ограниченных габаритных размеров в сочетании с небольшой вычислительной мощностью.

3. Проблема управления информационной безопасностью в системах интернета вещей, которая в существующей парадигме угрозы – уязвимости - риски может быть сведена к задаче управления рисками информационной безопасности или альтернативными показателями, так или иначе ассоциированными с рисками информационной безопасности.

1.3 Анализ проблемы управления информационной безопасностью в системах, использующих технологии Интернета вещей

Последняя проблема представляет наибольший интерес, так как ее решение и создает условия поддержания заданного уровня защищенности информации в системе в условиях постоянного воздействия на защищаемую систему комбинаций различных дестабилизирующих факторов:

- изменения во времени уровня информационных рисков в следствие появления новых угроз и выявления новых уязвимостей в системе, в том числе уязвимостей как к вновь появившимся, так и ранее уже известным угрозам;
- изменению самой структуры защищаемой системы – появлению новых элементов, изменению масштаба, появлению новых связей между элементами;
- изменениям стоимости информации в защищаемой системе, при чем характер таких изменений не будет стационарным;
- «старению» (снижению эффективности) с течением времени жизни системы применяемых методов и способов защиты информации в этой системе. Под эффективностью в данном случае понимаем способность способа защиты решать поставленную задачу: обеспечивать надежную аутентификацию «вещей» при информационном обмене, обеспечивать противодействие сетевым атакам и т.д.

В государственных стандартах, научных трудах, посвященных проблематике управления информационной безопасностью, существуют термины «менеджмент информационной безопасности» и «управление информационной безопасностью». С точки зрения терминов это различные варианты перевода на русский язык английского слова management.

Отправной точкой стандартизации и унификации процессов управления информационной безопасностью можно считать серию стандартов, разработанных Британским институтом стандартизации (BSI – British Standards Instiution) в 1999 году, в которых впервые сформулированы принципы риско-ориентированного подхода к управлению ИБ:

BS 7799-1 «Information technology – Security techniques – Code of practice for information security management». (Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью)

BS 7799-2 «Information technology – Security techniques – Information security management systems - Requirements». (Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.)

BS 7799-3:2006 «Information security management systems – Part 3: Guidelines for information security risk management». (Системы управления информационной безопасностью — Часть 3: руководство по управлению рисками в информационной безопасности).

В последствии эта серия стандартов получила международный статус, например BS 7799-1 был трансформирован в стандарт ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management» и в последствии его аутентичный перевод был принят в качестве государственного стандарта РФ – ГОСТ Р ИСО/МЭК 17799-2005 «Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью».

Нетрудно заметить, что во всех случаях английский термин «management» (Information security management systems) на русский язык переводился термином «управление» (управление информационной безопасностью). Однако, начиная с 2010 года, с принятием в РФ стандарта ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», который является прямым переводом на русский язык международного стандарта «ISO/IEC 27005:2008 Information technology – Security techniques - Information security risk management (IDT)», термин «управление» при переводе был заменен термином «менеджмент». В последующим, при принятии других стандартов т.н. 2700-й серии, описывающих различные аспекты Системы менеджмента информационной безопасности (СМИБ)

такая терминология сохранилась. В качестве примера, приведены названия некоторых актуальных стандартов, образующих СМИБ:

ГОСТ Р ИСО/МЭК 27000-2021 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» [10];

ГОСТ Р ИСО/МЭК 27001-2021 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [11].

При этом термин «управление» продолжает встречаться в стандартах СМИБ, но в более узком смысле, например «управление сменными носителями информации», «управление доступом» [11], «управление инцидентами ИБ» [10], «управление техническими уязвимостями» [12], в том числе и «управление ИБ» [10].

Вопрос о том, являются ли «менеджмент информационной безопасности» и «управление информационной безопасностью» эквивалентными понятиями принимая во внимание то, что в аналогичных англоязычных документах термин «management» не менялся с момента появления, остается открытым. Существует мнение ряда авторитетных специалистов [92], что эти термины не эквиваленты и понятие «management» гораздо шире и богаче, чем «управление», то есть управление информационной безопасностью описывает только часть процесса менеджмента. Учитывая, что современные представления о СМИБ [10] для успешного внедрения СМИБ организации определяют такие основные принципы, как:

a) понимание необходимости использования СМИБ;

b) назначение ответственности за обеспечение ИБ;

c) обеспечение баланса между обязательствами руководства и потребностями заинтересованных сторон;

d) повышение социальной значимости,

то с таким утверждением следует согласиться.

В любом случае можно лишь констатировать, что к существующим объективным и субъективным неопределенностям, характеризующим процесс управления информационной безопасностью, добавляются еще и лингвистические неопределенности, вносимые регуляторами.

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 настоящее время процессы управления информационной безопасностью регламентируются серией стандартов ГОСТ Р ИСО/МЭК 2700х под общим названием «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности», а также рядом документов ФСТЭК, разработанных в качестве развития и конкретизации отдельных подпроцессов, например Методический документ «Методика оценки угроз безопасности информации» (Утвержден ФСТЭК России 05.05.2021 г.). Для оценки защищенности информации в системе применяются положения стандартов ГОСТ Р ИСО/МЭК 15408-х-2012 «Методы и средства обеспечения безопасности информационных технологий. Критерии оценки безопасности» [8, 9]. Однако следует учитывать, что указанные стандарты и регламентирующие документы изначально ориентированы на традиционные автоматизированные системы и вопрос корректности прямого распространения содержащихся в этих документах норм и правил для систем IoT, учитывая специфику последних, не исследован.

Вместе с тем основные подходы, такие как процессный подход, риско-ориентированный подход, декомпозиция защищаемой системы на информационные активы, - могут быть признаны универсальными не зависимо от класса защищаемой системы.

Основной проблемой практического применения перечисленных нормативных документов при организации процесса управления информационной безопасностью является то, что в их основе лежат неформализованные (часто вербальные) модели, представляющие собой по сути рекомендации и описания

последовательности и содержания этапов оценки рисков информационной безопасности и организации контрмер на неформальном (в данном случае русском) языке. Как известно, основными особенностями неформальных языков является их избыточность и наличие существенной неопределенности. Кроме того, вербальные неформальные модели как правило или вообще не предполагают численных оценок, или допускают использование экспертных групп для численной оценки значений некоторых вероятностных характеристик (например, при актуализации рисков).

Так, в качестве примера неформализованной модели укажем формулировку критерия соответствия мер защиты предъявляемым требованиям в стандарте ГОСТ Р ИСО/МЭК 15408-1-2012 «Введение и общая модель» [8]:

«Для владельца актива важна убежденность в том, что:

- контрмеры являются достаточными, если контрмеры выполняют то, что заявлено, и угрозам;
- угрозам, направленным на активы, обеспечивается противостояние;
- контрмеры являются корректными, если контрмеры выполняют то, что заявлено».

Известно, что применение контрмер для реализации стратегии снижения риска в информационной системе, т.е. фактически применение известных и доступных способов защиты информации требует материальных затрат. Они могут включать стоимость программного и аппаратного обеспечения, расходы на внедрение, эксплуатацию и ремонт, стоимость обучения специалистов и проч. Этот важный аспект также не нашел своего отражения в рассматриваемых нормативных документах [10-15].

Поиски возможности создания формальных моделей процессов управления информационной безопасностью в системах IoT, формализация оценки защищенности информации в системе является важнейшим направлением исследований.

Из приведенной формулировки процесса управления информационной безопасности вытекает, что эффективным будет такое управление, при котором

обеспечивается возможность приведения системы к заданному значению показателя защищенности информации за минимально возможное время.

В качестве критерия эффективности выбрано «поддержание заданного уровня защищенности информации в системе при минимизации затрат» и формализован в общем виде (1.1):

$$K_{\text{эфф}} = \begin{cases} R_t \rightarrow R_0 \\ C_t \rightarrow C_{min}, \\ T_t \rightarrow T_{min} \end{cases} \quad (1.1)$$

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 информационной безопасностью в системах IoT:

1. Критерий K_1 «оперативность управления информационной безопасностью». 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 (1.2):

$$K_1 = T^* \xrightarrow[R_t < R_0]{} min \quad (1.2)$$

2. Критерий K_2 «точность управления информационной безопасностью». Определяется на основе показателя эффективности «стоимость затрат на возврат защищаемой системы к требуемому состоянию $R_t \geq R_0$ после начала действия дестабилизирующего фактора» (1.3):

$$K_2 = C_t \xrightarrow[R_t \geq R_0]{} min \quad (1.3)$$

Выводы

Результаты выполненного анализа проблематики обеспечения информационной безопасности и управления информационной безопасностью в системах Интернета вещей показывают, что информационные системы, использующие технологии Интернета вещей, могут быть рассмотрены как отдельный класс информационных систем, имеющих особенности архитектуры, технологий и организации информационного цикла, роли человека-пользователя в системе, существенные для обеспечения информационной безопасности. Одной из основных особенностей является недостаточность правового регулирования со стороны государства вопросов информационной безопасности в системах IoT, что затрудняет использование общих подходов к их решению, например таких как оценка эффективности систем СЗИ в IoT, а также вопросов, связанных с управлением информационной безопасностью.

В результате проведенного исследования обоснованы необходимость формализации процессов управления информационной безопасностью в информационных системах, использующих IoT-технологии, и моделирования таких процессов в целях поддержания заданного уровня защищенности информации в системе при постоянно изменяющихся условиях. При этом задача управления информационной безопасностью в системах интернета вещей в существующей парадигме угрозы – уязвимости - риски может быть сведена к задаче управления рисками информационной безопасности или альтернативными показателями, так или иначе ассоциированными с рисками информационной безопасности.

Предложен обобщенный критерий эффективности управления информационной безопасности в системах IoT и на его основе введены частные критерии эффективности управления, такие как «оперативность управления информационной безопасностью» и «точность управления информационной безопасностью».

Глава 2. Способ управления информационной безопасностью в системах Интернета вещей посредством формирования и использования в системе управления обратной связи в режиме численной оценки основных параметров

2.1 Анализ современных представлений, моделей и методов в управлении информационной безопасностью

Обеспечение необходимого уровня защищенности информации в информационных системах вообще и в системах, использующих технологии Интернета вещей, является важнейшей задачей информационной безопасности (ИБ).

Синтез и внедрение систем защиты информации (СЗИ) является необходимым, но недостаточным условием для поддержания требуемого уровня защищенности информации в системе. На защищаемый объект (информационную систему) постоянно действуют различные дестабилизирующие факторы, влияние которых направлено на снижение достигнутого уровня защищенности информации в системе. Учитывая, что при решении задачи управления информационной безопасностью основополагающими являются рискоориентированный и процессный подходы [92], в качестве показателя защищенности информации в системе используется понятие риска информационной безопасности.

В государственных нормативных документах [10-15, 21, 22] процесс управления информационной безопасностью включает в себя следующие основные этапы:

1) инвентаризация информационных активов;

2) оценка уровня актуальных угроз информационной безопасности по каждому информационному активу и по системе в целом;

3) анализ уязвимостей в защищаемой системе;

4) оценки рисков и выбор актуальной стратегии управления рисками (способа обработки риска);

5) в случае выбора из возможных способов обработки рисков снижение риска - применения необходимых контрмер для снижения рисков и приведение общего уровня риска по системе к заранее заданному значению.

Основная цель реализации этапов менеджмента ИБ - получение некоторого численного значения текущего риска R_t в защищаемой системе, сравнение его с заранее заданным (требуемым) значением R_0, которое определяется ЛПР и, в случае превышения текущего риска выше заданного определение необходимых контрмер, способных вернуть защищаемую систему в заданное состояние, т.е. $R_t \geq R_0$.

Один из возможных способов формализации понятия «риск» применительно к задаче управления информационной безопасностью (2.1):

$$R_{\text{общ}} = \sum_{i=1}^{n} R_i = \sum_{i=1,j=1}^{n,m} \left(P\left(T_i V_j\right) C_a\right), \quad (2.1)$$

где:

$R_{общ}$ – общий риск информационной безопасности в защищаемой системе;

R_i – элементарный риск в защищаемой системе;

T_i – элементарная угроза конфиденциальности, целостности или доступности;

V_j – уязвимость в защищаемой системе, через которую может реализовываться i-угроза;

$P(T_iV_j)$ – вероятность реализации i-й угрозы через j-ую уязвимость

C_a – стоимость информационного актива (суммарная стоимость нескольких активов), на который (или на которые) направлена i-я угроза.

Определение численных значений параметров входящих в выражение (2.1) является нетривиальной задачей.

Для определения стоимости каждого актива системы выполняется этап «инвентаризация информационных активов». Основными целями этапа является подробное описание программно-аппаратной структуры актива и содержащейся в нем информации. Стоимость актива k-того информационного актива в системе будет определяться как:

$$C_a^k = C_p^k + C_I^k, \quad (2.2)$$

где C_p^k – стоимость программных и аппаратных средств, формирующих k-й информационный актив;

Cl^k – стоимость информации, содержащейся в k-ом информационном активе.

Каждое слагаемое в выражении (2.2), строго говоря, изменяется во времени, однако на коротком временном интервале (2-3 месяца) этим можно пренебречь.

Определение значения стоимости программных и аппаратных средств, формирующих актив, не представляет существенных затруднений, что же касается определения стоимости информации, содержащейся в информационном активе, то известно как минимум два метода такой оценки:

1) определение рыночной стоимости такой информации;
2) определение размера ущерба при утрате такой информации.

Оба метода не являются точными, однако некоторые приближенные значения могут быть получены.

Основная проблема управления информационной безопасностью в информационных системах заключается в определении численного значения величины $P(T_iV_j)$ при очевидной невозможности использовать метод статистических испытаний [32]. Фактически этапы «оценка уровня актуальных угроз информационной безопасности по каждому информационному активу и по системе в целом» и «анализ уязвимостей в защищаемой системе» и должны в результате обеспечить понимание величины $P(T_iV_j)$.

Существующие нормативные документы в области информационной безопасности предполагают для получения количественной оценки применение метода экспертных оценок [21].

Проблематика применения метода экспертных оценок хорошо известна и включает сложно реализуемые этапы, включая формирование экспертной группы, проведение оценки, обработку мнений экспертов и установление доверия к полученным результатам.

Возможность доверия полученным результатам определяется вычислением коэффициента согласованности мнений экспертов, для вычисления которых существует несколько методов (коэффициенты вариации, коэффициенты конкордации и т.д.), при чем выбор конкретного метода может зависеть от предпочтений ЛПР [32]. В любом случае применение метода экспертных оценок

(включая подготовку), при соблюдении всех правил и условий, обеспечении согласованности мнений экспертов (включая применение итерационных методов типа «Дельфи»), обработки полученных результатов требует значительного времени и не могут считаться пригодными для обеспечения оперативности управления ИБ. То есть повышение уровня дестабилизирующих факторов в системе и, как следствие, снижение уровня защищенности информации в системе, может быть выявлено только при следующем проведении экспертной оценки величин $P(T_iV_j)$, а значит защищаемая система может находится в неудовлетворительном состоянии $R_t \leq R_0$ во временном интервале между экспертными оценками, причем это будет неизвестным для ЛПР вплоть до следующей экспертной оценки уровня угроз в системе. В руководящих документах ФСТЭК указывается, что такую оценку необходимо проводить периодически, но продолжительность такого периода не устанавливается и относится на решение ЛПР [21]. Учитывая сложности проведения экспертных оценок, возможно предположить, что продолжительность периода может составлять от 3 месяцев.

Такая ситуация не позволяет владельцу информации быть уверенным, что мероприятия, выполненные в рамках существующей СМИБ, последовательно и полно поддерживают защищаемую систему в требуемом состоянии, то есть что текущее значение показателя защищенности информации R_t в системе не опустилось ниже заданного уровня R_0.

Существующий подход предполагает, что сам факт внедрения СМИБ в соответствии с [10-15] уже является достаточным условием, чтобы считать, что уровень защищенности информации в системе поддерживается на нужном уровне, или, по крайней мере, приближается к нему, а управление информационной безопасностью эффективно.

Известны исследования в данной области, в которых предлагаются альтернативные методы оценки защищенности информации в системах Интернета вещей, однако в большинстве случаев весь процесс управления в целом при этом не рассматривается [49].

Одним из возможных вариантов решения описанной проблемы может стать подход к управлению информационной безопасностью на основе способа управления с обратной связью.

Учет в модели управления ИБ выраженной обратной связи выходной переменной (значения показателя защищенности информации в системе R_t) и входных переменных, описывающих состояние СЗИ, предполагает возможность измерения текущего состояния управляемой системы (процесса) и сравнение его с желаемым (заранее заданным) состоянием в режиме численных оценок.

Текущее состояние системы определяется по одной или нескольким характеристикам системы, которые в модели управления будут являться выходной (выходными) переменными модели. При этом весь цикл управления принято рассматривать как последовательность этапов (рис. 2.1).

Рисунок 2.1 Цикл управления как последовательность этапов.

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, блок управления принимает 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 (процесса) в заданное состояние.

Таким образом, способ управления ИБ с обратной связью обеспечивает возможность системе (процессу) реализации функций саморегулирования и адаптивности, позволяет обеспечить точность, стабильность и надежность работы. Это достигается наделением системы способностью реагировать на изменения различных дестабилизирующих факторов в некотором диапазоне. Размеры диапазонов допустимых изменений дестабилизирующих факторов обусловливают пределы устойчивости систем управления.

Одним из важнейших достоинств применения в управлении различными системами (процессами) метода использования обратной связи является то, что реализованные механизмы обратной связи позволяют автоматизировать процессы управления. Система сама контролирует и корректирует свои действия, что упрощает работу оператора и повышает эффективность системы по критериям оперативности управления ИБ и точности управляющих воздействий.

Вместе с тем, необходимо учитывать и недостатки, присущие методу управления с обратной связью. Наиболее существенными недостатками различные источники указывают:

- замедление реакции системы на изменения дестабилизирующих воздействий в результате анализа и коррекции данных;
- чувствительность к помехам, возникающим главным образом при воздействии шумов различной природы в измерениях.

Также в качестве недостатков часто указывают сложность настройки систем автоматического управления и сложность анализа, что в целом может усложнить анализ работы управляемой системы (процесса), так как измеренные значения параметров системы и значения величин управляющих воздействий могут быть сложными для интерпретации и понимания.

Модели процессов управления, использующих обратную связь для контроля выходной (управляемой) характеристики системы и выработки управляющего

воздействия для возврата управляемой характеристики системы в исходное состояние, представляется возможным разделить на два класса:

1) формализованные модели, в которых все переменные и неизменяемые параметры модели представляют собой численные величины, которые могут быть измерены в реальном процессе, а связи между элементами могут быть описаны в виде формальных зависимостей (например, математическими выражениями, функциями).

2) неформализованные модели, в которых демонстрация наличия возможности управления по обратной связи носит описательный (вербальный) характер и служит для раскрытия содержания процесса управления без возможности проведения численных расчетов.

Что касается формализованных моделей, то аналитические модели с отрицательной обратной связью широко используются в теории автоматического управления и лежат в основе бесчисленного количества примеров их успешной практической реализации.

Неформализованные модели широко применяются в организации управления информационной безопасностью, однако использование моделей с обратной связью в явном виде практически не встречаются, хотя наличие обратной связи учитывают отдельные конструкции, описывающие этапность менеджмента рисков информационной безопасности или оценку защищенности информации [13, 14].

Так на рис. 2.2 представлена в качестве примера модель управления ИБ из монографии А. А. Торокина «Техническая защита информации» [42], в которой учет обратной связи в явном вид отсутствует.

Информационная модель оценки защищенности информации, представленная в [13] (рис. 2.3) также не имеет в явном виде управления по обратной связи.

Известны примеры учета наличия обратной связи в неформальных моделях управления информационной безопасностью, когда она используется для демонстрации содержания процесса управления, т.е. имеет описательный характер. В качестве примера такой модели на рис. 2.4 приведена интерпретация известной

PDCA-модели управления информационной безопасностью (Plan-Do-Check-Act) [43].

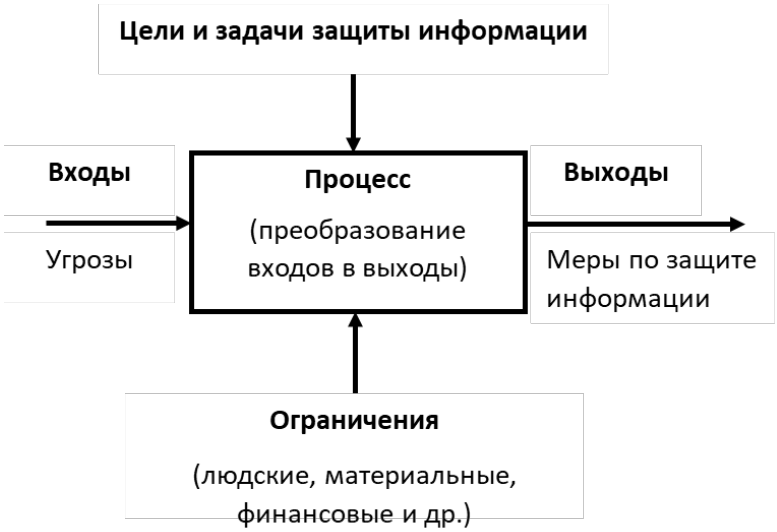

Рисунок. 2.2 Пример модели управления ИБ из монографии А. А. Торокина «Техническая защита информации»

Таким образом, результаты анализа показывают, что способ управления ИБ с выраженной обратной связью в известных методиках управления ИБ или не учитывается, или подразумевается в рамках неформализованных моделей для раскрытия характера процессов управления ИБ.

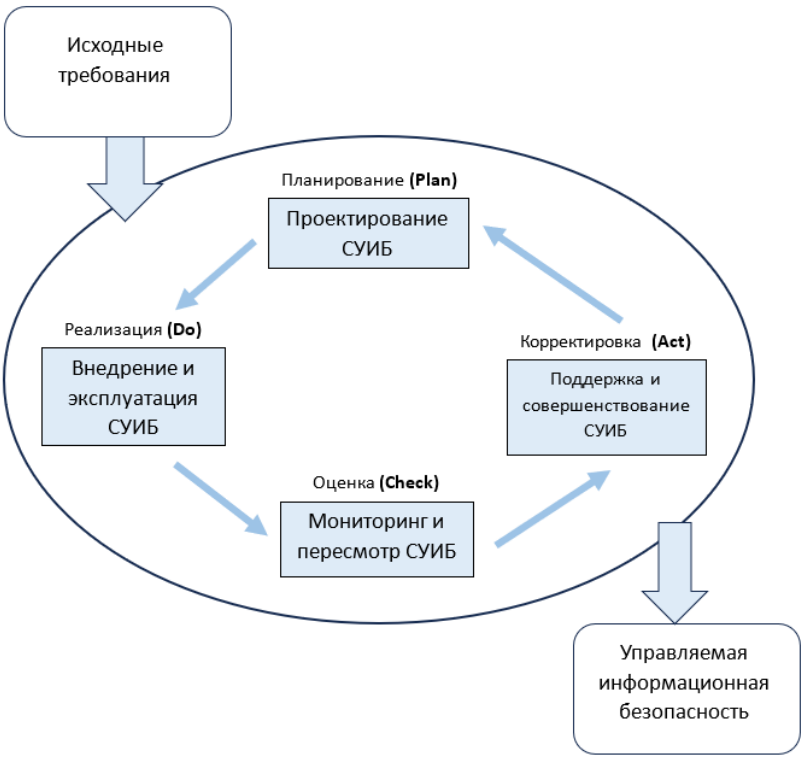

Рисунок 2.4. PDCA-модель управления информационной безопасностью

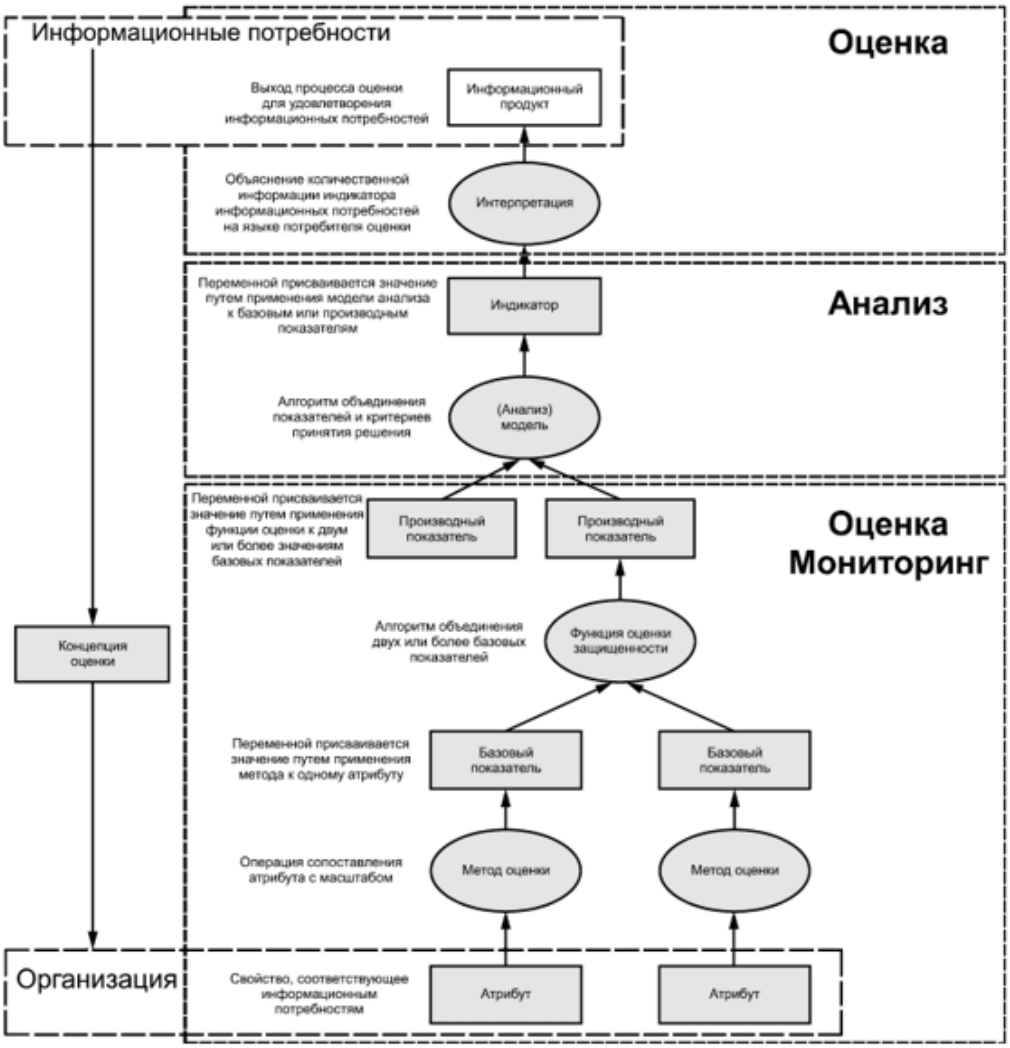

Рисунок 2.3. Модель оценки защищенности информации, по ГОСТР Р ИСО/МЭК 27004-2021

2.2 Способ управления информационной безопасностью в системах IoT на основе учета обратной связи

В качестве интерпретации способа управления с обратной связью для модели управления информационной безопасностью предложена модель управления информационной безопасностью, представленная на рис.2.5.

В качестве объекта управления выступает защищаемая информационная система (система IoT), а управляемым параметром системы является риск информационной безопасности как показатель защищенности информации в системе.

В качестве механизма, генерирующего управляющие воздействия в системе управления информационной безопасностью, могут быть рассмотрены характеристики конкретной конфигурации системы защиты информации (СЗИ). Изменение конфигурации СЗИ, то есть изменение возможностей в сторону усиления защитных функций системы, может быть рассмотрено в качестве управляющего воздействия.

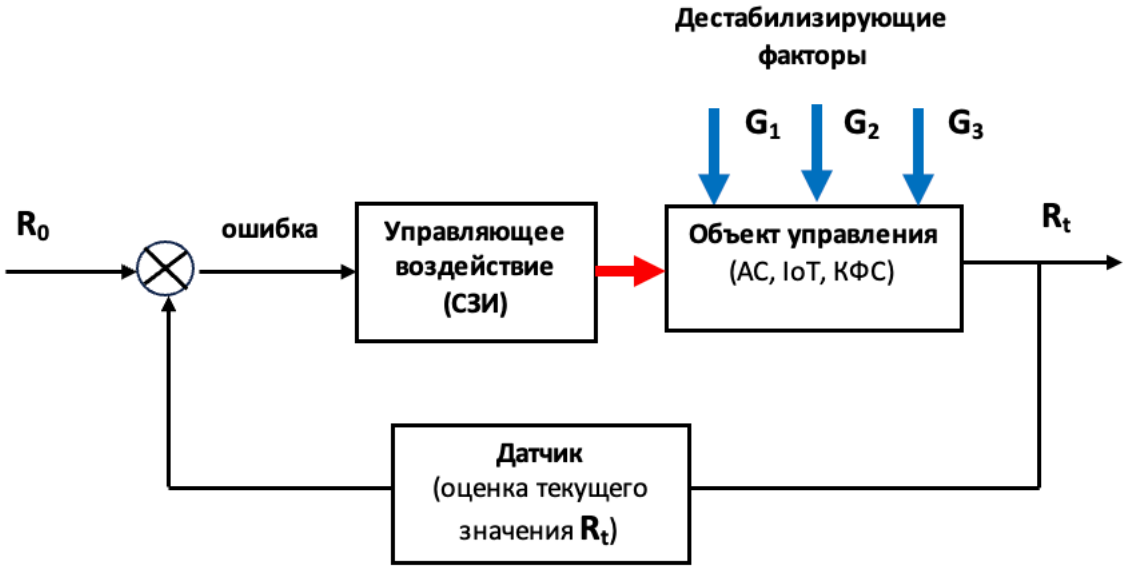

Рисунок 2.5. Структура модели процесса управления ИБ

где:

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;

G_2 – дестабилизирующий фактор, учитывающий изменения в структуре защищаемой системы в соответствии с потребностями бизнеса;

G_3 – дестабилизирующий фактор, учитывающий изменения в политике безопасности организации.

В период, когда защищаемая информационная система IoT 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 и тогда общая структура модели управления информационной безопасностью с обратной связью может иметь вид (рис.2.6).

Основные трудности в формализации представленной модели заключаются в

- формализации текущего уровня актуальных угроз в защищаемой системе (G);
- формализации конфигураций системы защиты информации (U);
- формализации связей (U, G, R_t).

В результате проведенных исследований [93, 94] предложены способы формализации отдельных компонентов комплексной модели. В частности структура подмодели, позволяющей определять текущий актуальный уровень угроз (рис. 2.7). Обозначения Level C, Level A, Level I на рис.2.3 соответствуют начальным уровням угроз конфиденциальности, доступности и целостности соответственно.

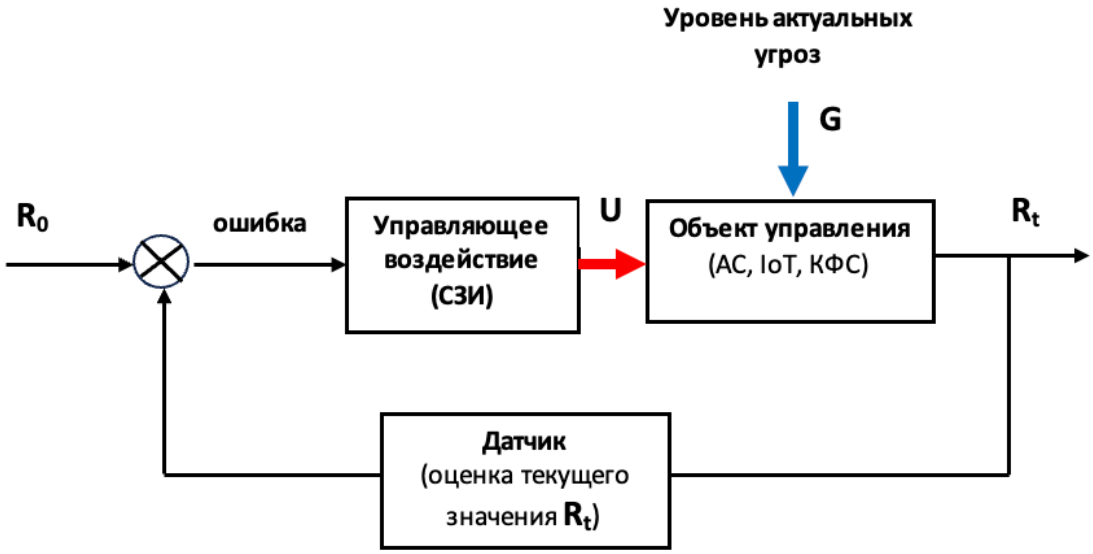

Рисунок 2.6. Структура модели процесса управления информационной безопасностью в условиях относительно стабильного периода.

Подмодель, представленная на рис.2.7, использует несколько методов моделирования, относящихся к классам формального представления систем и методы активизации интуиции и опыта специалистов. Структура модели является комбинированной и содержит вложенные подмодели.

1. Модель экспертных оценок начальных значений уровней угроз, при чем для удобства работы экспертов, им будет предложено оценить отдельно угрозы конфиденциальности (Level C), доступности (Level A) и целостности (Level I) информации. Активизация указанной модели предполагается на начальном этапе, а также при изменении структуры защищаемой системы или изменении политики безопасности организации – владельца защищаемой системы IoT.

2. Модель формализации сообщений об инцидентах ИБ, позволяющая численно определять изменения начального уровня угроз.

3. Нечеткие модели, использующие представления входных и выходных переменных в виде лингвистических переменных и алгоритмы нечеткого вывода Мамдани, позволяющие определять численные значения начального и текущего уровней угроз в системе [35, 50, 51]. Особенности информационных систем, использующих технологии Интернета вещей, например, приоритет в конкретной системе обеспечения доступности информации перед конфиденциальностью и целостностью, могут быть учтены в базе правил нечеткой модели.

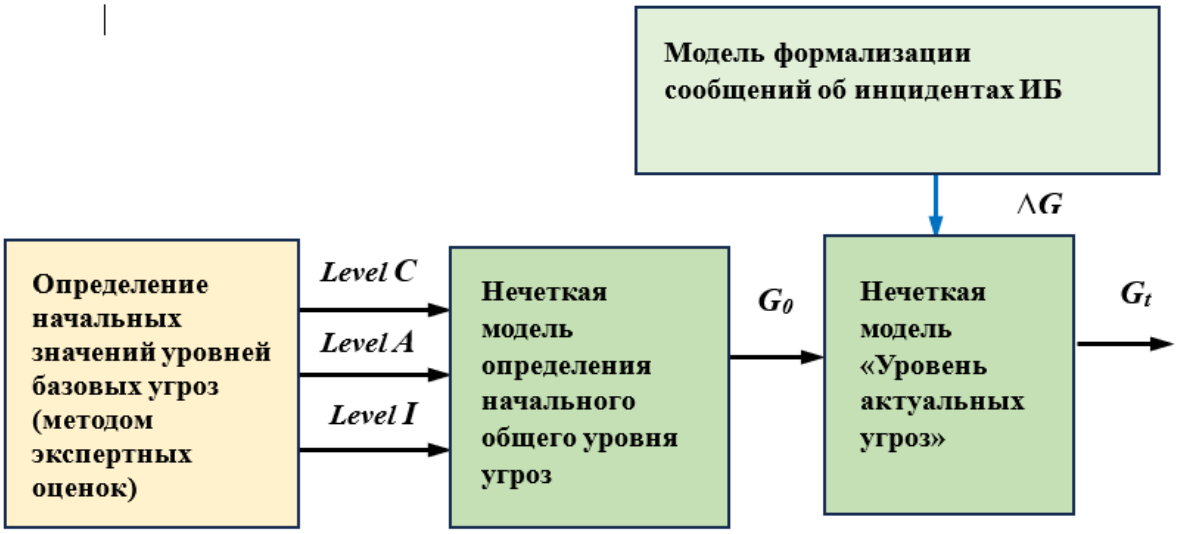

Рисунок 2.7. Структура подмодели определения текущего уровня актуальных угроз в системе

Предложенная конструкция позволяет определять текущий уровень актуальных угроз в системе в виде числового значения в условных единицах, при этом экспертная оценка используется исключительно для определения начального

уровня угроз, а конструкции модели позволяют фиксировать текущие изменения начального уровня по мере поступления в систему информации об инцидентах информационной безопасности в других аналогичных системах.

Любое контролируемое мероприятие, использующее ресурсы в целях преобразования исходных данных в результаты, можно считать процессом. Результат одного процесса может непосредственно формировать исходные данные для следующего процесса. Обычно подобное преобразование происходит в условиях планирования и управления. Применение в рамках организации системы процессов, наряду с их идентификацией, обеспечением взаимодействия, а также управлением ими, можно назвать «процессным подходом». Именно поэтому, в рамках предложенного подхода к управлению информационной безопасности систем IoT и придерживаясь при этом базового процессного подхода, модель управления информационной безопасностью будет рассмотрена как модель процесса.

Структура модели управления информационной безопасностью с учетом обратной связи может быть сведена к оптимизационной модели, которая в качестве выходной переменной имеет величину управляющего воздействия, а в качестве входных переменных модели – текущий уровень защищенности информации в системе и текущий уровень актуальных угроз, который можно характеризовать как начальный уровень угроз и его изменение в связи с появлением новых угроз (рис. 2.8).

Неизменяемыми параметрами модели в таком случае являются:

- максимально возможная стоимость предполагаемых контрмер;
- максимально допустимое время на изменение конфигурации СЗИ (или на реализацию контрмер), которые определяются ЛПР;
- требуемое значение показателя уровня защищенности информации в системе.

Однако следует учитывать, что изменения в политике безопасности организации могут оказать влияние на значения этих параметров.

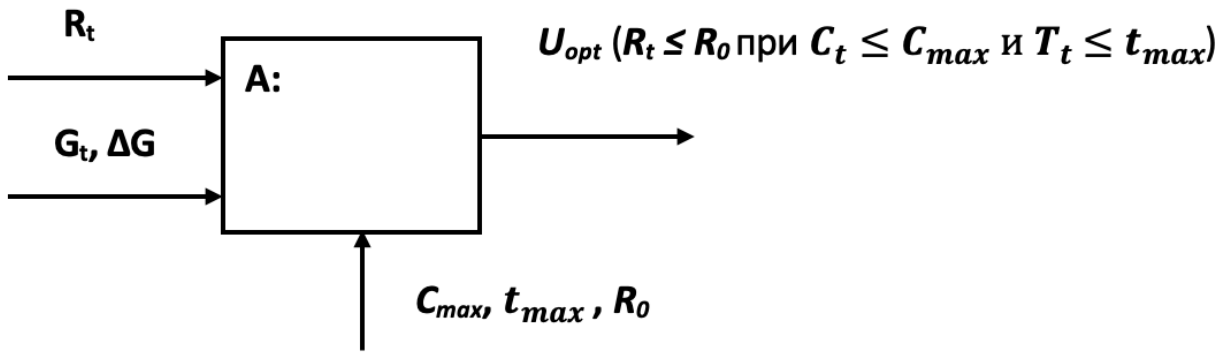

Рисунок 2.8. Структура оптимизационной модели процесса управления информационной безопасностью в защищаемой системе

где:

C_t – стоимость реализации конкретной конфигурации СЗИ;

T_t – время, необходимое для перехода к конкретной конфигурации СЗИ;

G_t – начальный общий уровень угроз в системе;

ΔG – величина изменения уровня угроз в системе относительно начального;

$A:$ – оператор модели.

Методы и способы численной оценки изменяемых и неизменяемых параметров модели управления информационной безопасностью в рамках подхода к управлению с использованием обратной связи представлены в таблице 2.1.

Таблица 2.1. Методы численной оценки параметров модели управления ИБ в рамках предложенного подхода к управлению

Параметр, величина, ед. изм.		**Методы численной оценки**
G_0	Начальный общий уровень угроз в системе, условные единицы, [0,1]	Метод экспертных оценок, методы нечеткого моделирования. Определяются уровни угроз доступности, целостности и конфиденциальности по условной шкале [0, 10] и затем определяется G_0 с учетом значимости базовых угроз в конкретной системе IoT.
ΔG	Текущая величина изменения уровня угроз в системе, условные единицы, [0,1]	Методы структуризации, методы формализации текстовых сообщений об инцидентах ИБ. Выявленная угроза сопоставляется с заранее построенным «деревом» угроз, в

		котором уровни декомпозиции угроз проранжированы.
$\mathbf{R_0}$	Требуемое значение показателя уровня защищенности информации в системе, условные единицы, [0,1]	Определяется ЛПР в предложенной условной шкале.
$\mathbf{R_t}$	Текущее значение показателя уровня защищенности информации в системе, условные единицы, [0,1]	Метод нечеткого моделирования (алгоритм нечеткого вывода Мамдани)
$\mathbf{U_i}$	Показатель возможностей текущей (i-ой) конфигурации СЗИ, условные единицы, [0,10]	Методы структуризации, ранжирования, метод нечеткого моделирования (алгоритм нечеткого вывода Мамдани)
$\mathbf{U_{opt}}$	Величина управляющего воздействия – функция конкретной конфигурации СЗИ, условные единицы, [0,10]	Методы структуризации, ранжирования, метод нечеткого моделирования
$\mathbf{C_t}$	Стоимость реализации конкретной конфигурации СЗИ, руб.	Определяется из предварительной оценки затрат на введение дополнительных контрмер для перехода к *i*+1 конфигурации СЗИ
$\mathbf{C_{max}}$	Максимально допустимая стоимость предполагаемых контрмер, руб.	Определяется ЛПР
$\mathbf{T_t}$	Время, необходимое для перехода к конкретной конфигурации СЗИ, ч	Определяется из предварительной оценки времени, необходимого на введение дополнительных контрмер для перехода к *i*+1 конфигурации СЗИ
$\mathbf{t_{max}}$	Максимально допустимое время на изменение конфигурации СЗИ, ч	Определяется ЛПР

2.3. Оценка эффективности предложенного подхода к управлению информационной безопасностью в системах интернета вещей

Таким образом, способ управления информационной безопасностью в системах Интернета вещей может обеспечить повышение эффективности по критерию «оперативность управления ИБ», так как информация о появлении новых, ранее не учтенных в СЗИ угроз, поступает в защищаемую систему не в момент следующей экспертной оценки, а практически в режиме реального времени.

В дальнейшем может быть выбрана соответствующая конфигурация СЗИ, которая способна вернуть уровень защищенности информации в системе R_t к требуемому R_0, при этом оптимизация выбора может проходить по критерию минимальной стоимости вводимых контрмер, что обеспечит повышение эффективности управления и по критерию «точность управления ИБ».

Частный критерий эффективности «точность управления ИБ», представленный в общем виде (1.3) для оценки эффективности предложенного способа управления ИБ с учетом обратной связи примет вид (2.3):

$$K_2: \begin{cases} U_i \xrightarrow[C_{i+1} \le C_{max}]{} U_{i+1}, R_t \ge R_o, C_{i+1} \to min \\ N_A \in F, F: \{R_t \ge R_o, C_{i+1} \le C_{max}, T_A \le T_{max}\} \end{cases}, \quad (2.3)$$

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 $\boldsymbol{R_t \ge R_0}$ и отвечают ограничениям по затратам и времени на введение C_{max} и T_{max}.

Показатель эффективности управления ИБ «точность управления ИБ» $П_2$ для систем IoT определяется согласно выражению (2.4):

$$П_2 = \left(1 - \frac{1}{N_A}\right)^2 \quad (2.4)$$

Предварительная оценка эффективности способа управления информационной безопасностью в системах IoT представлена на рис. 2.9. и обоснована возможность повышения эффективности управления ИБ более 30% 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 любой из них ЛПР равновероятен.

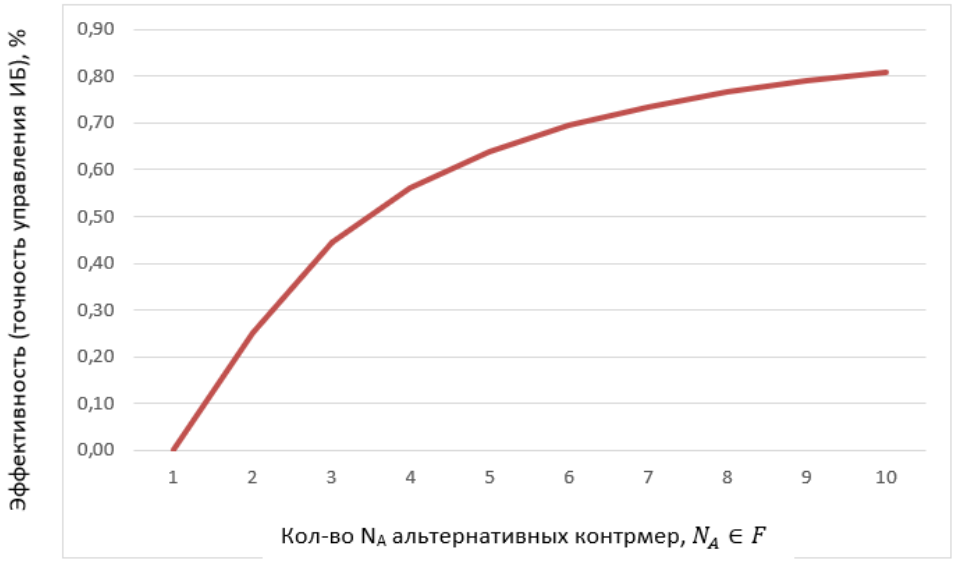

Рисунок 2.9 Оценка эффективности способа управления ИБ в системах IoT с учетом обратной связи по критерию «точность управления ИБ»

Эффективность управления ИБ в системах IoT в случае применения способа управления с обратной связью по критерию «точность управления ИБ» будет возрастать с увеличением количества возможных альтернативных контрмер, вводимых в СЗИ с целью возврата защищаемой системы в требуемое состояние защищенности $R_t \geq R_0$, т.е. переводящих СЗИ из конфигурации U_i в конфигурацию U_{i+1}.

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.

Выводы

В результате выполненных исследований показано, что существующий подход к управлению информационной безопасностью, изложенный в рассмотренных государственных нормативных документах, основан на неформальных (описательных) моделях. Использование исключительно метода экспертных оценок для численной оценки актуальных угроз и рисков не обеспечивает в полной мере эффективность управления по критериям оперативности и точности управления ИБ.

Установлено, что способ управления с обратной связью в задачах управления ИБ в системах IoT либо не используется, либо носит вербальный характер и служит для раскрытия содержания процесса управления. Такой способ управления ИБ не позволяет реализовать оптимизацию управления, например, оптимизацию по стоимости выбираемых контрмер.

Предложен способ управления ИБ в системах IoT на основе управления с обратной связью по аналогии с системами автоматического управления, позволяющий оптимизировать управляющее воздействие в системе для приведения ее в заданное состояние защищенности информации. Обоснована возможность введения численных оценок параметров процесса управления ИБ с применением современных методов моделирования сложных систем, что позволяет использовать в подходе к управлению ИБ способ управления с обратной связью с численными оценками параметров процесса управления.

Введен критерий эффективности управления ИБ «точности управления ИБ» и обосновано повышение эффективности предложенного способа до 30 % в случае наличия 3-4 альтернативных решений по изменению конфигурации СЗИ в ответ на фиксируемое дестабилизирующее воздействие – изменение уровня угроз в системе.

Таким образом обосновано, что предложенный способ управления информационной безопасностью Интернета вещей посредством формирования и использования в системе управления отрицательной обратной связи в режиме численной оценки основных параметров процесса управления практически реализуем и его применение способно повысить эффективность управления ИБ по

сравнению с применяемыми способами по введенному критерию «точность управления ИБ».

Глава 3. Комплексная модель процесса управления информационной безопасностью в системах Интернета вещей

3.1 Постановка задачи моделирования процесса управления ИБ в системах IoT

Задача моделирования процесса управления ИБ в системах IoT сведена к построению оптимизационной модели (рис. 2.8), и выполнена с помощью понятийного (терминологического) аппарата, свойственного аналитическим методам, при этом решение задачи моделирования исключительно аналитическими методами в данном случае вызывает большие затруднения. Прежде всего это связано с неопределенным характером переменных модели и естественных ограничений аналитических методов.

Вместе с тем, следует признать, что именно аналитическими методами пытаются решать эту задачу большинство исследователей [54, 55, 59, 62, 89, 90].

Наибольший интерес здесь может вызывать применение вариационных принципов [32]. В интерпретации для рассматриваемого случая можно представить каждую конкретную конфигурацию системы защиты информации (СЗИ) в виде числовой функции нескольких переменных, вида:

$$y = y(X) = F_i((x_1, x_2 \dots x_n), C_i, T_i, R_0), \quad (3.1)$$

где:

$\boldsymbol{y}$ – числовая функция, описывающая ***i-ю*** конфигурацию СЗИ;

$\boldsymbol{x_1, x_2 \dots x_n}$ – показатели СЗИ, характеризующие ***i-ю*** конфигурацию СЗИ;

$\boldsymbol{C_i}$ – стоимость (расходы) на внедрение ***i-й*** конфигурации СЗИ;

$\boldsymbol{T_i}$ – время, необходимое для перехода к ***i-ой*** конфигурации СЗИ.

$\boldsymbol{R_0}$ – заданный уровень защищенности информации в системе.

Множество $\boldsymbol{W}$ таких функций конечно и ограничено требованиями

$$C_t \le C_{max} \text{ и } T_t \le t_{max},$$

Если при этом рассмотреть функционал

$$J(y) = \int_{R_t}^{R_0} F\big(X, y(X), \dot{y}(X)\big)dX, \quad (3.2)$$

то задача моделирования сведется к нахождению функции $\hat{\boldsymbol{y}} \in \boldsymbol{W}$ для которой функционал ***J(y)*** принимал бы некоторое оптимальное значение для всех ***y***, принадлежащих ***W***, то есть нахождению экстремали функционала ***J(y)***.

На сегодняшний день известны попытки построения аналитических моделей для моделирования различных частных аспектов проблемы управления информационной безопасностью, например некоторых аспектов кибербезопасности.

На основе аналитических представлений существуют различные методики измерения и оценки рисков, например, табличные, с помощью количественных шкал и др.

Основным и наиболее распространенным методом оценки рисков информационной безопасности является метод, основанный на построении модели угроз и уязвимостей, предполагающий использование аналитических и статистических представлений [43].

«Классическая» формула оценки информационного риска, в соответствии с принятыми представлениями:

$$R = P(V)D, \tag{3.3}$$

где ***R*** – информационный риск;

D – величина возможного ущерба;

P(V) – вероятность реализации определенной угрозы через некоторую уязвимость.

Суммарный текущий информационный риск по системе может быть определен как:

$$R_t = \sum_{i,j}^{n,m} P_i(V)D_j, \tag{3.4}$$

где

$\boldsymbol{R_t}$ – общий информационный риск;

$\boldsymbol{D_j}$ – величина возможного ущерба *j*-му информационному активу;

$\boldsymbol{P_i(V)}$ – вероятность реализации *i*-ой угрозы через некоторые уязвимости.

Численная оценка величины возможного ущерба ***D*** в целом возможна, хотя единого подхода здесь не существует. Основной же проблемой такого подхода является численная оценка вероятности $P_i(V)$. Очевидно, что единственно возможным методом для такой оценки является метод экспертных оценок.

Требования к формированию экспертной группы и рекомендации по обработке полученных от экспертов сведений отражены в Приложении 2 к Методике «Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке угроз безопасности информации». Важно отметить, что указанные Требования не содержат четких критериев, которым должны соответствовать сами эксперты.

В качестве шкалы измерений предполагается использовать различные качественные шкалы типа «низкий», «средний», «высокий» или «да», «нет». То есть даже применение экспертного метода оценки не предполагает никаких численных метрик.

Указанный способ проведения экспертной оценки может вызывать вопросы по корректности обработки полученных оценок от каждого эксперта, так как не предполагается проведение оценки коэффициента согласованности мнений экспертов. Кроме того, не предполагается учет «веса», который должен приписываться к оценке каждого эксперта и характеризовать степень его компетентности, хотя в любой экспертной группе маловероятна такая ситуация, что все члены группы окажутся компетентными в равной степени.

При этом необходимо учесть, что понимание сути величины *Pi(V)* при рассматриваемом подходе не совсем соответствует классическому понятию вероятности и трактуется как «мера уверенности появления инцидентов информационной безопасности». При современном уровне развития и доступности информационных технологий, возможности потенциальных нарушителей для нарушения базовых свойств информации чрезвычайно велики и новые угрозы появляются фактически в режиме реального времени, а стоимость информационного актива, на который направлена угроза, также изменяется во

времени, «классическая» формула оценки риска информационной безопасности должна иметь вид:

$$R = \frac{dP(V)}{dt} \frac{dD}{dt} \quad (3.5)$$

Следствием этого можно считать и наличие в нормативных документах требования периодичности к оценке угроз информационной безопасности.

Отсюда очевидно, что такую экспертную группу необходимо собирать каждый раз, когда выявляется новая, ранее не учтенная, угроза или в банк данных угроз безопасности информации ФСТЭК России включена новая угроза: т.е. экспертная группа должна быть постояннодействующей. Учитывая необходимость обеспечения соответствия экспертов предъявляемым требованиям, особенности формирования экспертной группы и обработки полученных от экспертов данных, то становится очевидным: обеспечить необходимую периодичность (то есть, фактически, непрерывность) такой оценки на практике практически невозможно. Если же такая экспертная группа собирается «от случая к случаю», то говорить об эффективном управлении информационной безопасностью в защищаемой системе можно с большой долей условности, так как не реализуется в полной мере принцип непрерывности управления по месту и по времени, другими словами, оперативность управления крайне низкая.

Таким образом, аналитический подход к моделированию процесса управления информационной безопасностью в настоящее время может применяться для постановки и конкретизации задачи моделирования, определения общей структуры модели. Что же касается создания адекватных численных моделей, то использование аналитических представлений, даже в комбинации с статистическими методами моделирования и методом экспертных оценок для определения численных значений переменных модели, не может обеспечить удовлетворительные практические результаты и это утверждение очевидно, учитывая неопределенный характер переменных модели.

Одним из возможных методов моделирования подобных объектов являются методы нечеткого моделирования, основанный на теории нечетких множеств Л.

Заде [34, 82]. Такие методы могут быть отнесены к классу теоретико-множественных.

Задачи управления представляются как эталонные тестовые проблемы для применения методов нечеткого моделирования. Вместе с тем, потенциальные возможности моделирования на основе нечетких алгоритмов значительно шире, чем решение задач синтеза регуляторов с нечеткой логикой (РНЛ) для систем автоматического управления в технических системах [34-36, 38].

В основе идеи построения нечеткой модели управления информационной безопасностью лежит возможность человека делать достаточно справедливые суждения типа:

- «если общий уровень угроз в системе $\boldsymbol{G_t}$ высокий, и текущее значение показателя уровня защищенности информации $\boldsymbol{R_t}$ в системе значительно ниже требуемого $\boldsymbol{R_0}$, то необходимо значительное повышение возможностей СЗИ (сильное управляющее воздействие $\boldsymbol{U}$)»;
- «если изменение уровня угроз в системе $\Delta\boldsymbol{G}$ малое, а текущее значение показателя защищенности информации $\boldsymbol{R_t}$ в системе превышает требуемое значение $\boldsymbol{R_0}$, то управляющее воздействие $\boldsymbol{U}$ не требуется».

Такого рода суждения могут быть получены из интервью со специалистом (экспертом), который хорошо знаком с конкретной структурой защищаемой системы, особенностями информационного процесса в системе и с контекстом (средой безопасности) функционирования такой системы в течение некоторого времени. В результате может быть получено понимание структуры нечеткой модели – ее размерность, характер лингвистических переменных и другие параметры (вид базы правил, тип нечеткой импликации, способ агрегации правил, метод дефаззификации).

Основными преимуществами нечетких алгоритмов являются:

1) возможность формализации качественных переменных модели в виде лингвистических переменных;

2) использование в качестве оператора модели базы правил, составленной на основании вербальных заключений специалистов о поведении моделируемого

процесса и нечеткого вывода на правилах, позволяющих получать численные значения на выходе модели в условных единицах.

При таком подходе становится важным не абсолютные значение полученных оценок, а возможность численно оценивать их изменения [93,95,96].

С 2007 года в качестве альтернативы нечетким алгоритмам моделирования отдельными специалистами рассматривается т.н. серый реляционный анализ (Grey relational analysis, GRA) [117, 118, 119, 120].

GRA использует информационный подход и понятие информационной ситуации. Он определяет информационную ситуацию без информации как «черную», а ситуацию с полной информацией как «белую». Поскольку таких ситуаций в реальности не бывает, то на практике всегда существует определенность и неопределенность. Ситуации между этими двумя крайностями относятся к «серым». Таким образом, «серая» система анализа означает, что исследуется ситуация, в которой часть информации известна и часть информации неизвестна.

При таком определении количество и качество информации образуют континуум, от полного отсутствия информации до полной информационной определенности. Серый анализ заключается в поиске системных решений. Для «черной» ситуации решений нет. Для «белой» ситуации существует одно решение. «Серые» системы анализа будут давать различные возможные решения по информации в ситуации. Серый анализ не пытается найти лучшее решение. Он заключается в категоризации и группировке решений по признакам: «допустимое решение», «хорошее решение», «подходящее решение» и т.д. для реальных проблем. По сути, он решает задачи поддержки принятия решений, а не задачи принятия решений. При этом, он допускает последующий когнитивный или интеллектуальный анализ.

GRA включает следующие основные этапы: нормирование исходных данных, вычисление последовательности отклонений, серых реляционных коэффициентов, серых реляционных оценок, на основании которых может быть произведен выбор и ранжирование полученных оценок.

Если увеличение значения параметра *w* и приводит к повышению качества *Q*, или его уменьшение - к повышению качества *Q*, то нормализованное значение параметра определяется как:

$$\overline{w}_{i.j} = \begin{cases} \dfrac{w_{i,j} - \min\limits_{j}(w_i)}{\max\limits_{j}(w_{i,j}) - \min\limits_{j}(w_{i,j})} \mid \uparrow w \to Q \uparrow \\ \dfrac{\max\limits_{j}(w_i) - w_{i,j}}{\max\limits_{j}(w_{i,j}) - \min\limits_{j}(w_{i,j})} \mid \downarrow w \to Q \uparrow \end{cases}, \quad (3.6)$$

где w_{max} и w_{min} - максимально и минимально возможные значения параметра w, соответственно.

Последовательность отклонений для нормализованных данных:

$$\delta_{i,j} = \max_{i}(\overline{w}_{i,j}) - \overline{w}_{i,j} \quad (3.7)$$

Серые реляционные коэффициенты $\gamma_{i,j}$ оцениваются как:

$$\gamma_{i,j} = \frac{\max\limits_{i}(\delta_{i,j}) + \varsigma \min\limits_{i}(\delta_{i,j})}{w_{i,j} + \varsigma \max\limits_{i}(\delta_{i,j})} \quad (3.8)$$

где ς - коэффициент различия или идентификации; $\varsigma \in [0, 1]$, в большинстве случаев используется значение 0,5.

На основе (3.8) вычисляются серые реляционные оценки:

$$G_i = \sum_{j=1}^{s} \eta_j \gamma_{i,j}, \quad (3.9)$$

где $\eta, \in [0, 1]$ - весовые коэффициенты значимости соответствующих параметров, $\sum_{j=1}^{s} \eta_j = 1$. Чем выше значение, тем важнее альтернатива.

Определение этих коэффициентов в системах, характеризующихся высокой неопределенность, к которым относится система управления информационной безопасностью, возможна с использованием субъективных и объективных методов взвешивания. Субъективные методы определения веса основаны на экспертной оценке. Наибольшее распространение получили такие методы, как SMART, AHP, SIMOS и метод Delphi. В методах объективного взвешивания вес определяется в

результате анализа данных, собранных по каждому критерию с использованием математических алгоритмов и моделей и без участия ЛПР. Наиболее распространёнными методами являются метод наименьших средних квадратов (LMS), минимальное максимальное отклонение, энтропия, TOPSIS и многокритериальная оптимизация.

Ранжирование факторов производится в порядке уменьшения значений серых реляционных оценок. Фактор с наибольшим значением серой реляционной оценки будет считаться наиболее значимым, то есть его значение будет наиболее близким к эталонному значению по всем критериям.

Модели серого реляционного анализа используются в случаях, когда применение статистических методов затруднено или невозможно.

Его ключевым преимуществом является небольшая вычислительная сложность, что позволяет реализовывать его практически на любых вычислительных устройствах. Это преимущество определяет метод серого реляционного анализа как один из наиболее подходящих для маршрутизации данных в сетях IoT [111].

При этом, в условиях, когда вычислительная мощность и уровень энергопотребления не оказывают существенного влияния на функционирование системы, использование методов нечеткого моделирования позволяет учесть индивидуальные особенности конкретной системы за счет имеющейся возможности гибкой настройки параметров модели.

Кроме того, методы нечеткого моделирования позволяют объединять в единую комплексную модель различные подмодели, созданные с применением других методов моделирования – аналитических, статистических, экспертных и проч. Для этого используется методика преобразования числовых переменных в лингвистические и обратно. Такой инструмент позволяет не использовать нормирование для разномасштабных и разнородных величин, используемых в качестве параметров модели.

В результате проведенного анализа обоснован выбор методов моделирования: методы нечеткого моделирования, экспертные методы, методы,

основанные на структуризации моделируемой системы, методы формализации неструктурированной текстовой информации.

3.2 Показатель защищенности информации в системе

При существующем риско-ориентированном подходе применительно к проблематике управления информационной безопасностью, изложенном в серии стандартов «Менеджмент информационной безопасности» [8-15], в качестве показателя, характеризующего степень защищенности информации в системе, предполагается понятие «риск информационной безопасности» (information security risk), который определяется как возможность того, что данная угроза может воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [14].

Для установления значения риска стандарт предполагает следующие этапы:

- идентификация информационных активов в защищаемой системе;
- определение перечня актуальных угроз;
- выявление уязвимостей информационных активов;
- определение вероятностей возникновения угроз;
- оценка предполагаемого ущерба в случае реализации конкретной угрозы;
- установление значений рисков ИБ;
- оценка рисков и выбор способа обработки рисков.

Методология установления значения риска в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 [14] предполагает установление как качественного, так и количественного значения. Для реализации способа управления ИБ с обратной связью интерес имеет способ установления количественного значения риска ИБ.

Указывается, что для установления количественной оценки необходимо введение шкалы с числовыми значениями как последствий, так и вероятности, с применением данных из различных источников. Единственным недостатком

количественного подхода указывается то, что фактические проверяемые данные для такого установления значения риска чаще всего недоступны.

В результате анализа предложенной неформальной (вербальной) модели установления значения риска ИБ в режиме количественной оценки может быть определен как вероятность реализации i-й угрозы через j-ю уязвимость и соотнесенный с величиной возможного ущерба k-му активу, на который направлена угроза (3.10):

$$R_i = P(G_i V_j) C_k, \tag{3.10}$$

где:

R_i – i-й риск ИБ

G_i – i-я актуальная угроза ИБ

C_k – оцененный ущерб k-му активу в защищаемой системе

V_j – j-я уязвимость k-го актива, на который направлена G_i

В зависимости от уровня угрозы, учитываемой для определения риска ИБ предлагается использовать понятия риска низкого и среднего уровня. Совокупность множества рисков низкого и среднего уровня в итоге может иметь результатом общий риск более высокого уровня или, в конечном итоге общий риск ИБ по всей защищаемой системе. Для определения такого уровня риска при количественной оценке может быть использовано выражение (3.11)

$$R_{\text{общ}} = \sum_{i=1}^{n} R_i, \tag{3.11}$$

где:

$R_{\text{общ}}$ – общий риск ИБ в защищаемой информационной системе;

n – количество идентифицированных рисков.

Практическое использование значения риска ИБ в качестве показателя защищенности информации в системе IoT, а именно установления количественных значений рисков в конкретной защищаемой системе связанно с рядом труднопреодолимых проблем, основными из которых являются следующие.

1. Определение численного значения ущерба информационным активам. В представленной методологии предлагается две альтернативные меры: определение восстановительной стоимости актива и определение последствий для бизнеса от потери или компрометации актива. Обе меры не формализованы, а значит применение любой из них носит субъективный характер и не позволяет говорить о точности такой оценки, а значит и точности оценки рисков. Кроме того, никак не рассмотрены т.н. продолжающиеся последствия, когда не представляется возможным оценить ни временной период такого продолжения, ни окончательную оценку ущерба. В качестве, примера продолжающегося ущерба можно привести последствия аварии на Чернобыльской АЭС. Аналогичные ситуации с различным масштабом последствий вполне вероятны в случае систем промышленного интернета вещей, когда такие системы управляют сложными технологическими процессами и категорированы как объекты КИИ.

2. Определение численного значения вероятности реализации угрозы. Входные данные для определения и количественной оценки вероятности возникновения угроз предложено получать у владельцев активов или пользователей, персонала отдела кадров, руководства организации и специалистов в области ИБ, экспертов в области физической безопасности, специалистов юридического отдела и других структур, а также от юридических организаций, метеорологических служб, страховых компаний, национальных правительственных учреждений. Кроме того, предлагается использовать опыт, извлеченный из инцидентов, и предыдущие оценки угроз должны быть учтены в текущей оценке. При необходимости для заполнения перечня общих угроз может быть целесообразным обратиться к другим реестрам угроз (возможно, специфичным для конкретной организации или бизнеса). Списки угроз и их статистику можно получить от промышленных предприятий, федерального правительства, юридических организаций, страховых компаний и т.д. Все эти сведения могут быть использованы только при применении метода экспертных оценок, так как для более точного метода статистических испытаний, очевидно, доказательства репрезентативности выборки представлены быть не могут.

3. Обеспечение требования непрерывности мониторинга рисков ИБ в системе для выявления изменений. Использование количественных значений рисков ИБ в качестве показателя защищенности информации в системе по изложенным в п.2 соображениям также не может обеспечить непрерывность мониторинга в связи с большими затратами времени для определения количественных значений рисков ИБ.

Указанные проблемы существенны и для известных решений, также основанных на риско-ориентированном подходе. Так в работе [91] для оценки защищенности информации в системе IoT предложено в качестве показателя защищенности информации вычисление интегральных оценок рисков нарушения защищенности информации и конфиденциальности персональных данных, при этом такую оценку проводят в отношении одного конкретного устройства, входящего в систему IoT. Интегральный показатель защищенности информации определяется на основе оценки рисков составляющих – компонентов, таких как рисков, связанных с обработкой персональных данных, рисков, связанных удобочитаемостью политик конфиденциальности и т.д.

В качестве показателя защищенности информации в системе IoT в настоящем исследовании вводится 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:

$$R_t = F(G_t, U) \tag{3.12}$$

В (3.12) оператор F не обязательно является числовой функцией или функционалом. Связь между параметрами модели может определяться, например, с помощью нечеткого вывода на правилах [34].

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 (3.13). 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.

$$R_{\text{общ}} = R_t * C_{max}, \tag{3.13}$$

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

Для оценки C_{max} в конкретной защищаемой системе IoT может быть применен подход, использованный для определения показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений в части определения материального ущерба [112].

3.3 Общая структура комплексной модели процесса управления ИБ в системах IoT

Под комплексным моделированием сложных объектов любой природы понимаются методологии и технологии их описания, а также комбинированное использование методов, алгоритмов и методик многокритериального анализа, синтеза и выбора наиболее предпочтительных управленческих решений, связанных с созданием и развитием рассматриваемых объектов в динамически изменяющихся внешних и внутренних условиях [104].

Структура комплексной модели процесса управления ИБ в системах IoT, представленная на рис. 3.1, включает нескольких взаимосвязанных модулей (подмоделей).

Центральное место занимает нечеткое ядро модели (на рис.3.1 ограничена пунктиром), которое состоит из последовательности двух- или трех-входовых 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.

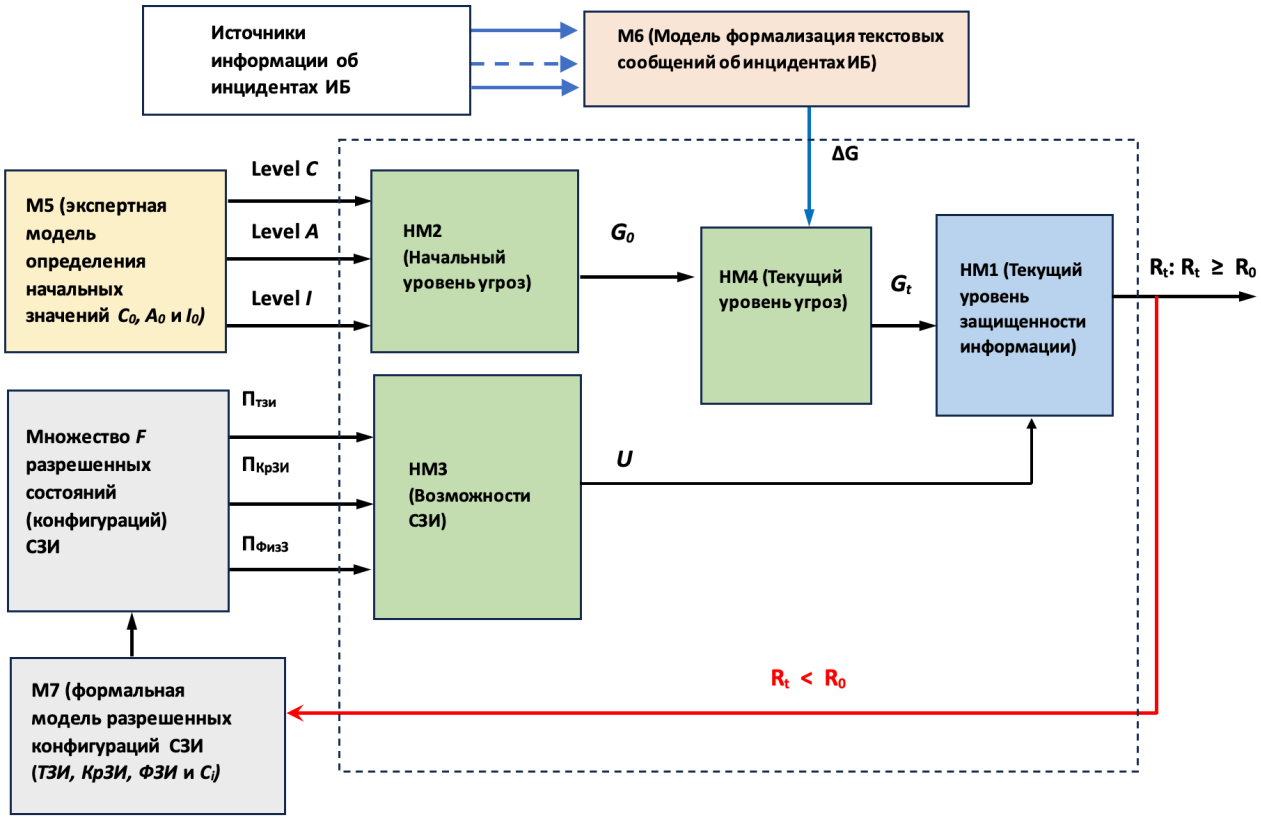

Рисунок 3.1 Общая структура комплексной модели управления ИБ в IoT системах

Нечеткое ядро модели поддерживается экспертной моделью **М5** определения начальных значений уровней актуальных угроз конфиденциальности C_0, доступности A_0 и целостности I_0.

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» [21], однако в целях повышения точности полученных оценок и определения доверия к полученным оценкам, указанная экспертная модель подверглась доработке и уточнению:

- внесены изменения в порядок формирования экспертной группы (в отношении численности группы и выбора экспертов);
- введена оценка согласованности мнения экспертов с помощью коэффициента вариации (3.14):

$$S = \sqrt{\frac{\sum_{i=1}^{n}(X_i - X_{\text{ср}})^2}{n-1}}, \qquad (3.14)$$

где: X_i – оценка i-го эксперта;

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

n – количество экспертов.

- для повышения согласованности мнений экспертов в случае невыполнения неравенства предусмотрены процедуры «Дельфи» (не более 2-х процедур), при достижении согласованности мнений экспертов также повышается и точность оценки.

Экспертная модель М5 активируется в следующих случаях:

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

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

3) в случае изменения политики безопасности.

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 результаты работы модели **М6** обеспечивают обнаружение изменений выходной переменной нечеткой модели **НМ2** и тем самым отслеживание изменение уровня защищенности информации в системе (выходной переменной нечеткой модели **НМ1**) в постоянном режиме.

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 стратегии «уменьшение риска» по ГОСТ Р ИСО/МЭК 27005-2014.

5. Аспекты, связанные с организационно-правовыми методами защиты информации не учитываются.

3.3.1 Нечеткое ядро комплексной модели (НМ1-НМ4)

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 (рис. 3.1) по масштабу и размерности через инструментарий лингвистических переменных.

Нечеткая модель НМ1.

Выходные переменные модели представлены в виде лингвистических переменных с 4 нечеткими множествами на непрерывной условной области определения [0…1] (Рис. 3. 2 и 3. 3). При отсутствии информации об особенностях конкретной информационной системы область определения разбита на термы равномерно.

Лингвистическое терм-множество переменной «Общий уровень угроз в защищаемой IoT системе» A_L = {низкий, средний, высокий, критический}.

Лингвистическое терм-множество переменной «Возможности СЗИ» B_L = {слабый, средний, сильный, высший}.

В качестве функции принадлежности нечетким множествам использованы функции gauss2mf, и trimf как функции, позволяющие получить более сглаженный отклик на выходе модели: функция вычисляет нечеткие значения членства с помощью основанной на сплайне функции принадлежности, имеющей форму пи (*y = gauss2mf (x, params)* или *(y = trimf (x, params)* возвращает вычисленное использование значений нечеткого членства основанной на сплайне функции принадлежности, имеющей форму пи). Задание лингвистической переменной возможно с помощью params пакета fuzzy в MatLab.

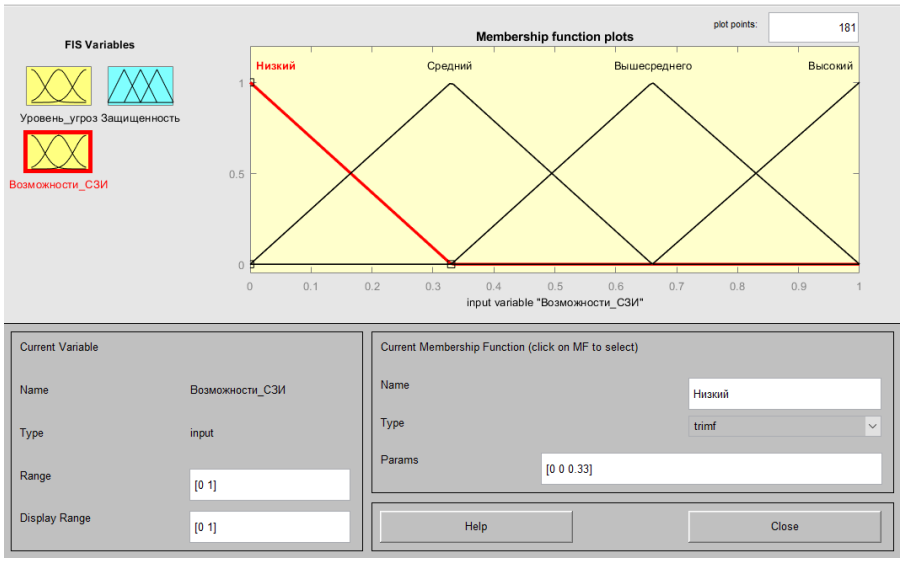

Рисунок 3.2 Представление входной переменной «Общий уровень актуальных угроз в защищаемой системы» в виде лингвистической переменной средствами MatLab Fuzzy.

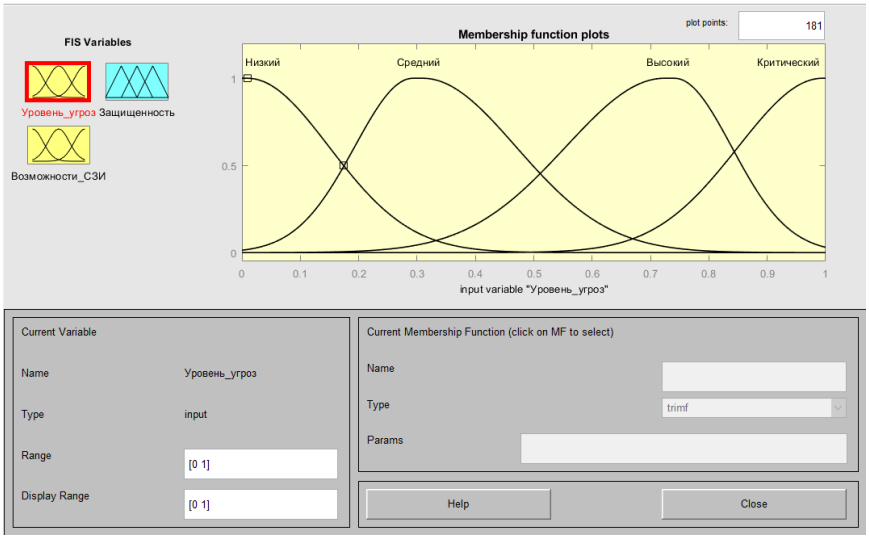

Рисунок 3.3 Представление входной переменной «Возможности СЗИ» в виде лингвистической переменной средствами MatLab Fuzzy (вариант)

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

$$f(x;a,b,c) = max\left(min\left(\frac{x-a}{b-a},\frac{c-x}{c-b},0\right)\right) \quad (3.15)$$

Для задания параметров a, b и c, использован params.

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

База правил нечеткой модели Мамдани представлена в таблице 3.1 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 3.1 База правил нечеткой модели НМ1 (вариант)

Уровень угроз / Возможности СЗИ	A1 (низкий)	A2 (средний)	A3 (высокий)	A4 (критич.)
B1 (низкий)	C2	C2	C1	C1
B2 (средний)	C3	C2	C2	C1
B3 (в-средний)	C4	C3	C3	C2
B4 (высокий)	C4	C4	C3	C3

№п п	Наименование	Значение
1	OR method	MAX
2	Implication	MIN
3	Agregation	MAX
4	Defuzzification	Centroid
5	Кол-во правил	64
6	Кол-во входных и выходных состояний	50

Рисунок 3.4 Параметры нечеткой модели НМ1

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

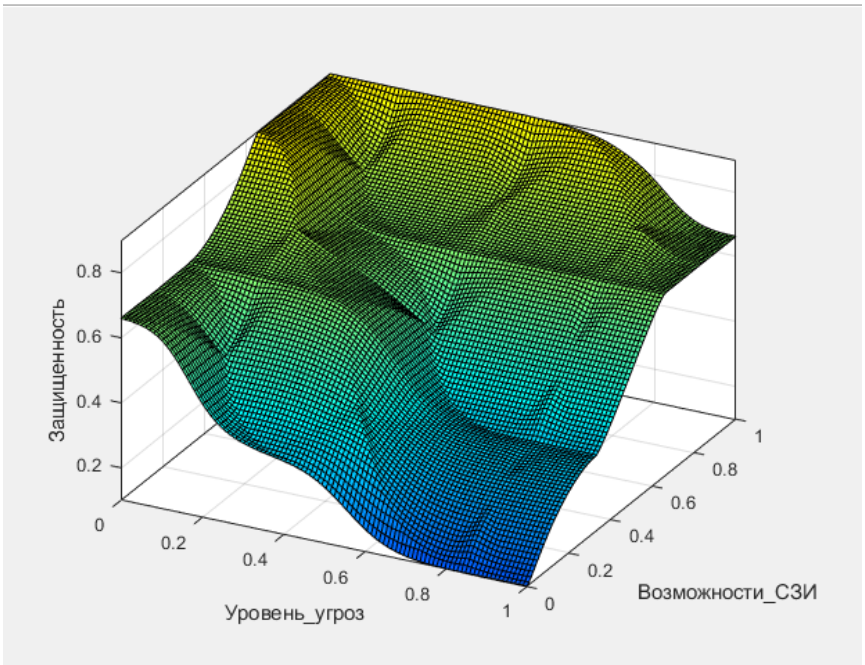

Рисунок 3.5 Графическая интерпретация поверхности нечеткой модели НМ1

В результате анализа полученной поверхности решения модели НМ1 установлено следующее:

1) применение нечетких методов моделирования (алгоритм Мамдани) позволяет получить неразрывную и чувствительную поверхность модели управления информационной безопасностью (изменение любой входной переменной в области определения приводит к изменению значения выходной переменной);

2) наличие гибких инструментов настройки нечеткой модели (как грубой – с изменением структуры модели, так и тонкой) позволит добиваться заданной точности;

3) полученная нечеткая модель качественно адекватна моделируемому процессу управления информационной безопасностью информационной системы;

4) применение на практике полученной модели позволяет оперативно отслеживать изменения показателя защищенности информации в системе при любых изменениях входных переменных. Эти изменения выражаются численно.

Нечеткие модели НМ2 и НМ3 строятся по аналогичным принципам. Пример графической интерпретации решения нечеткой модели НМ2 показан на рис. 3.6.

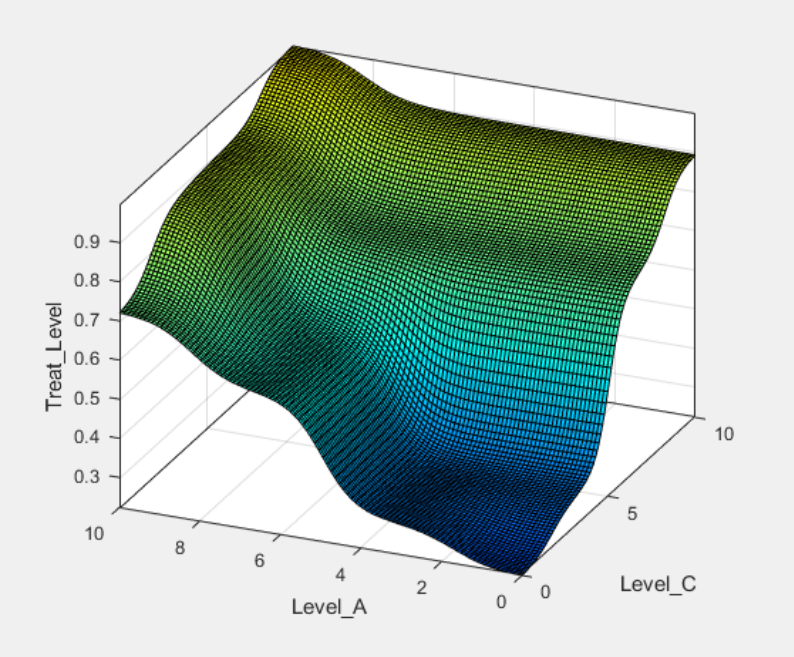

Рисунок 3.6 Зависимость общего уровня угроз в защищаемой системе (Treat Level) от уровня угроз конфиденциальности (Level C) и доступности (Level A) информации (вариант).

Основным достоинством решения ядра комплексной модели на основе нечетких моделей является возможность учитывать такие особенности защищаемой системы IoT, как неравнозначность базовых свойств информации в конкретной защищаемой системе. Например, обеспечение конфиденциальности информации может иметь приоритетный характер по сравнению с свойствами доступности и целостности в некоторой конкретной системе. В другом случае обеспечения свойств доступности и целостности может иметь больший приоритет. Такие особенности могут быть учтены настройкой базы правил, а также выбором способа разбиения вещественной области лингвистических переменных входных и выходных параметров нечеткой модели.

3.3.2 Экспертная модель М5

Модель М5 - экспертная модель определения начальных значений уровней угроз нарушения конфиденциальности C_0, угроз нарушения доступности A_0 и угроз нарушения целостности I_0.

Назначение модели – преобразование интуиции и опыта специалистов в численные значения уровня угроз базовым свойствам информации как объекта

защиты. То есть экспертная группа выступает в роли точного измерителя («измерительного прибора»).

Проблема численной оценки уровня актуальных угроз в защищаемой системе является одной из важнейших в решении задачи управления информационной безопасностью и, в частности, при решении задачи построения формальной модели такого управления.

Современные представления в области управления информационной безопасностью предполагают качественные и количественные способы оценки [21].

В структуре предложенной модели экспертная модель М5 играет чрезвычайно важную роль. От точности и объективности численной оценки исходных уровней базовых угроз зависит адекватность всей модели. Вместе с тем, для управления ИБ будет важна оценка именно изменения итогового уровня угроз в защищаемой системе, которая решается другими компонентами комплексной модели.

Известна экспертная модель для оценки угроз информационной безопасности, предложенная в Методическом документе ФСТЭК «Методика оценки угроз безопасности информации» (утверждена 05.02.2021) и содержащаяся в Приложении 2 к Методике «Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке угроз безопасности информации» [21].

Модель включает рекомендации по:

- формированию экспертной группы (качественные и количественные);
- характеру проблем, выносимых на экспертную оценку (негативного последствия от реализации угроз безопасности информации, целей нарушителей по реализации угроз безопасности информации, сценария действий нарушителей при реализации угроз безопасности информации);
- форме проведения экспертного опроса (анкетный метод);
- способа обработки полученных от экспертов оценок (среднее не включая минимальной и максимальной оценки).

Оценку предлагается проводить в 2 раунда с последующим усреднением полученных оценок от каждого эксперта в каждом раунде. Цель проведения оценки в двухраундовом варианте не заявлена, однако по смыслу понятно, что она применяется для повышения точности результата и является подобием метода «Дельфи».

Известно, что многораундовый или итерационный способ проведения экспертной оценки, известный как метод «Дельфи», применяется прежде всего для повышения согласованности мнений экспертов, то есть для повышения доверия к полученным результатам и для этого требуется введение критерия согласованности, например коэффициента вариации [32]. В каждом раунде вычисляется значение показателя, выбранного в качестве критерия согласованности мнений, и если его значение не изменяется, то следующий раунд не проводят, если же значение показателя согласованности улучшается, но все еще не достигает требуемой величины, то тогда есть смысл проводить следующий раунд.

Основным недостатком приведенной экспертной модели является отсутствие рекомендаций по оценке согласованности мнений экспертов. Поэтому нет никаких оснований считать, что полученная оценка по рекомендованной ФСТЭК Методике (экспертной модели) может быть использована как доверенная.

Еще одним недостатком можно считать отсутствие рекомендаций по ранжированию уровня квалификации экспертов при формировании экспертной группы.

Таким образом, рассмотренный способ проведения экспертной оценки [21] (экспертная модель) вызывает вопросы относительно корректности обработки полученных от экспертов оценок, так как не проводится оценка коэффициента согласованности (или непротиворечивости) и не учитываются веса, приписываемые к оценке каждого эксперта, так как даже в группе из 3 человек ситуация идентичности компетенции всех членов группы маловероятна.

Для утверждения объективности полученных при экспертной оценке результатов требуется соблюдение заранее определенных правил и строгое выполнение последовательности действий – алгоритма экспертного опроса и

обработки полученных от экспертов оценок. Каждый элемент алгоритма экспертного опроса представляет собой отдельную задачу, от обоснованности и правильности решения которой зависит успешность всего экспертного опроса в целом. К таким элементам применительно к поставленной задаче моделирования относятся:

- проблемы формирования экспертной группы, включая разработку требований к экспертам, размер экспертной группы, способы оценки их компетентности;
- форма экспертного опроса (наиболее распространенные формы – анкетирование, интервью, смешанные формы), а также собственно методика организации опроса;
- подход к оцениванию экспертом (определение шкалы оценки);
- метод обработки оценок, полученных от каждого эксперта;
- способ определения согласованности экспертных оценок, полученных от каждого эксперта и достоверности полученного результата.

Последний из перечисленных элементов носит определяющий характер в вопросе «можно ли вообще воспользоваться результатом такой оценки?». Для определения согласованности известны различные методы, наиболее применяемыми следует считать:

- статистические методы определения дисперсии;
- вероятности для заданного диапазона изменений оценок;
- ранговой корреляции Кендалла;
- ранговой корреляции Спирмена;
- коэффициента конкордации;
- коэффициента вариации.

Временная структуризация процесса экспертной оценки начальных уровней угроз конфиденциальности, доступности и целостности в защищаемой IoT-системе (модель М5) представлена на рис. 3.7 в виде последовательного алгоритма.

Предъявление более строгих требований к проведению экспертной оценки в модели М5 по сравнению с [21], включая итерационные процедуры в рамках метода

«Дельфи» для обеспечения согласованности мнений приглашенных экспертов и, тем самым, обеспечения высокого уровня доверия полученным результатам приведен к увеличению времени на выполнение такой оценки.

Вместе с тем, активизация модели М5 предполагается только для определения начального уровня базовых угроз внедрение в СУИБ способа управления на основе предложенной модели, изменение политики безопасности владельца системы IoT и изменение структуры защищаемой системы. Активизация модели М5 для периодической оценки уровня защищенности информации в системе не предполагается, поэтому этот недостаток может быть признан несущественным.

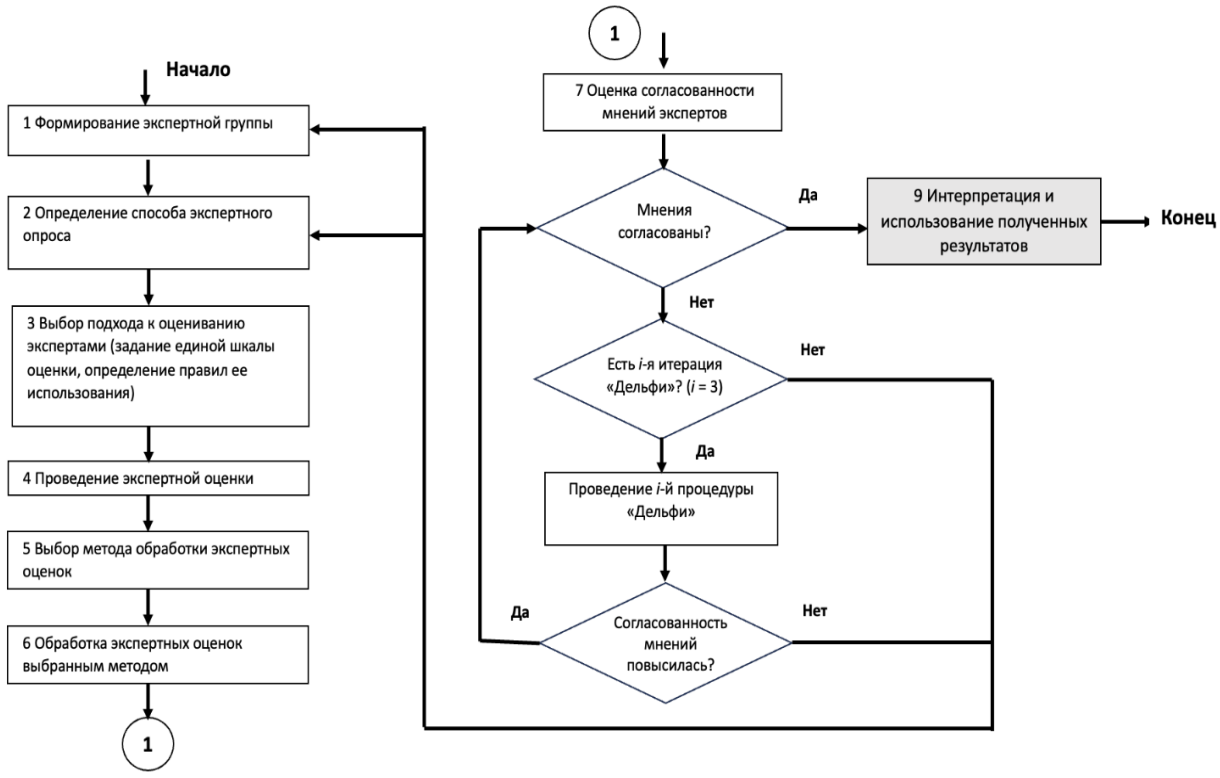

Рисунок 3.7 Обобщенный алгоритм проведения экспертной оценки

Для оценки согласованности мнений экспертов в модели М5 (этап 7 обобщенного алгоритм проведения экспертной оценки рис.3.7) вводится коэффициент вариации (3.12) [32].

$$K = \frac{1}{X_{\text{ср}}} \sqrt{\frac{\sum_{i=1}^{m} \left(X_i - X_{\text{ср}}\right)^2}{m-1}}, \tag{3.12}$$

где

X_{cp} – среднее значение оценки экспертов,

X_i – оценка i-го эксперта,

m – количество экспертов.

Мнения экспертов считаются согласованными, если $K \leq 0{,}25$.

3.3.3 Модель М6 формализации тестовых сообщений об инцидентах ИБ

В качестве источников информации для модели М6 могут быть использованы любые разнородные источники, содержащие информацию об инцидентах информационной безопасности в информационных системах любого класса, например ленты новостей информационных агентств в открытом доступе, внутрикорпоративную специализированную информацию и т.д.

Задачами модели М6 являются:

1) поиск в различных источниках информации, связанной с инцидентами информационной безопасности

2) формализация найденной информации (неструктурированного текстового сообщения) по заранее определенным параметрам формализации (например, определение типа реализовавшейся угрозы);

3) соотнесение идентифицированной угрозы с заранее построенным деревом актуальных в защищаемой системе угроз и определение величины ΔG.

В качестве модели, обрабатывающей непрерывный новостной текстовый поток, в модели М6 применяется следующий алгоритм [88].

Предполагается существование непрерывного потока добавляющихся в список ожидания новостных статей. В качестве входа принимается новостная статья в виде текстового документ произвольной тематики.

На первом шаге работы алгоритма определяется принадлежность самой статьи к классу интересующей предметной области – информационной безопасности (класс А). В случае, если было принято решение о непринадлежности новости d_m к требуемому для анализа классу А, находящаяся в обработке новость пропускается и выбирается следующий в очереди документ. В противном случае,

при принятом решении о принадлежности документа к нужному классу, весь находящийся текст статьи разделяется на смысловые объекты (слоги, слова, пары слов, предложения, абзацы и т.п.) методами токенизации [105] с возможной дальнейшей лемматизацией [106] и тегированием [88].

Полученные смысловые объекты принимаются на вход функции, отвечающей за непосредственно автоматическое заполнение полей соответствующей формы, выходом которой будут значения заполняемых полей. Следующим шагом является автоматическое заполнение полей и составление формализованной формы (карточки). Таким образом, результатом работы после этого шага является структурированная формализованная карточка. Форма отправляется в базу данных (дерево актуальных угроз), откуда может быть использована системами анализа данных.

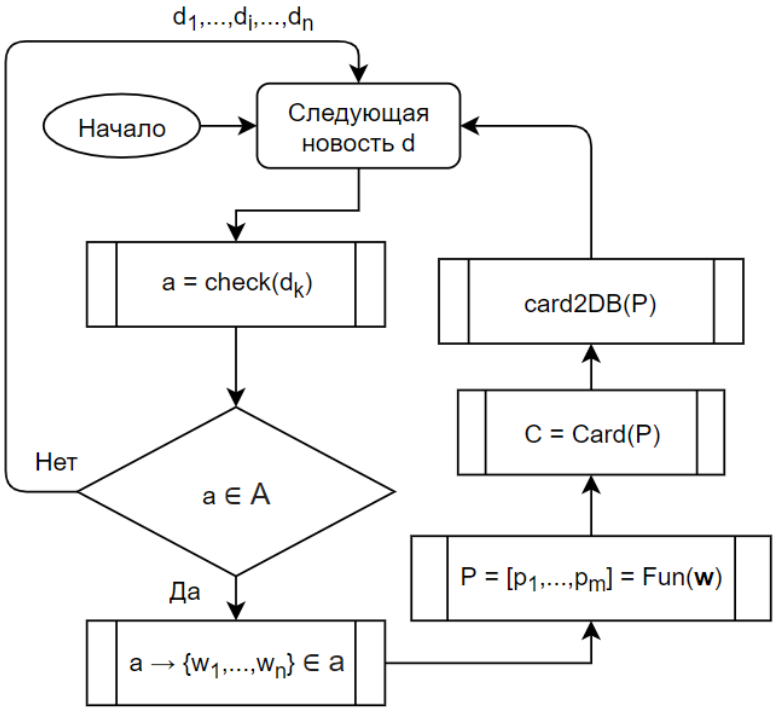

Рисунок 3.8 Блок-схема алгоритма способа формализации новостной ленты

В качестве модели использовался заранее обученный на полном национальном корпусе русского языка и статей сайта «Википедия» на русском языке набор [88], состоящий из примерно 515 миллионов слов, к каждому из которых соответствует свое векторное представление, размерностью 300. Пример вида и структуры векторизованного слова в модели представлен на рис. 3.9

```
широкий_ADJ -0.06787845 0.07847797
0.22332212 0.25629637 -0.47903422
-0.27830434 0.2827277 -0.14415039
-0.16623174 -0.6123661 0.15934642
0.54796106 -0.27388203 0.4346452
0.089563616 -0.0500748 0.36103764
0.26260573 0.36467606 0.009646658
```

Рисунок 3.9 Вид векторизованного слова в модели M6

Каждое слово в обученной модели было предобработано, присвоив метку части речи с помощью UDPipe и соответствует формату Universal POS tags.

Для проверки работы классификатора было вручную отобрано 15 статей различной тематики (7 из которых принадлежат тематике информационной безопасности). Каждая статья была разделена на смысловые объекты (слова) и во всех текстах удалены все знаки препинания. После чего каждому слову была присвоена метка части речи для соответствия с обученной моделью и формату Universal POS tags. Затем, каждый смысловой объект был векторизован согласно предложенной модели, а совокупность всех объектов статьи усреднена, получив таким образом среднее арифметическое вектора, являющееся по сути, усредненным смысловым объектом в виде всего документа. Далее, используя в качестве меры подобия косинусную метрику, была составлена матрица сходства между документами, значения которой для наглядности были визуализированы (рис. 3.10).

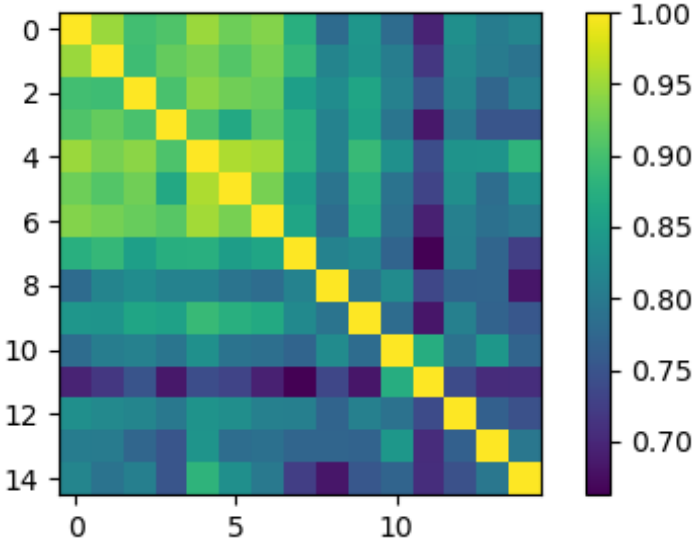

Рисунок 3.10 Тепловая карта для матрицы подобия документов в рамках классификатора модели M6

На тепловой карте отмечена степень подобия между всеми статьями (чем ближе значение к единице, тем сильнее степень сходства). На рис. 3.10 не трудно видеть квадрат 7x7 с тесными связями подобия друг с другом. Этой области соответствуют статьи, принадлежащие тематике информационной безопасности. Также видно, что со статьями других тематик степень связи у них ниже. Соответственно, критерием принятия решения будет являться степень подобия классифицируемой статьи с усредненным вектором статей на тему информационной безопасности. Таким образом, если степень подобия более порогового значения, то статья близка по смыслу к тематике информационной безопасности и будет считаться таковой в системе формализации неструктурированной текстовой информации. Для этого экспериментального случая была построена зависимость вероятности верного предсказания тематики всех статей выборочных статей от значения такого порогового значения рис. 3.11.

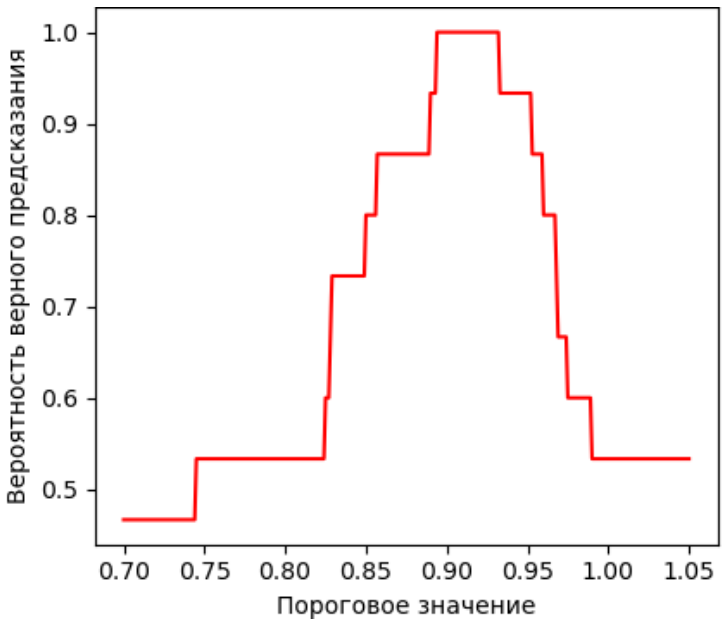

Рисунок 3.11 Зависимость вероятности предсказания тематики сообщения от значения выбранного порога

Таким образом, если выбрать пороговое значение меры косинусной близости между статьями в промежутке от 0.89 до 0.93, то классификатор верно распознает тематику статей у всех предложенных ему текстов.

$$sim(\bar{d}_i, \bar{d}_j) = \cos(\theta) = \frac{\sum_{k=1}^{n} \bar{d}_{i_k} \times \bar{d}_{j_k}}{\sqrt{\sum_{k=1}^{n} (\bar{d}_{i_k})^2} \times \sqrt{\sum_{k=1}^{n} (\bar{d}_{j_k})^2}}, \quad (3.16)$$

где $\bar{d}_i, \bar{d}_j$ - документы (сообщения), для которых требуется найти степень подобия, n - размерность вектора.

3.4 Оценка влияния разработанной модели на повышение эффективности управления ИБ

В основе разработанной комплексной модели управления информационной безопасностью в системах, использующих технологии интернета вещей, лежит предложенный способ управления ИБ с использованием отрицательной обратной связи. Повышение эффективности управления ИБ по частному критерию $К_2$ «точность управления» для предложенного способа справедливо и для реализованной на его основе модели.

Частный критерий эффективности управления ИБ $К_1$ «оперативность управления» (1.2) определяется на основе показателя эффективности $П_1$ «продолжительность Т* пребывания защищаемой системы в состоянии $R_t < R_0$ после начала действия дестабилизирующего фактора», например выявления новой, ранее не учитываемой актуальной угрозы. Показатель эффективности $П_1$ может быть формализован как (3.14)

$$П_2 = \sqrt{\left(1 - \frac{T_1}{T_{max}}\right)}, \quad (3.17)$$

где: $Т_1$ – временной период от идентификации новой, не учитываемой ранее, угрозы ИБ в системе IoT до определения и принятия контрмер в системе IoT;
$Т_{max}$ – максимальная продолжительность $Т_1$ при использовании для оценки текущих рисков в системе только метода экспертных оценок (6 месяцев).

На рис. 3.12 и 3.13 показаны результаты оценки эффективности управления ИБ по критерию «оперативность управления ИБ» для случая, когда оценка уровня

угроз производится только методом экспертных оценок (рис.3.12) и для случая, когда используется предложенная комплексная модель управления ИБ (рис.3.13).

В качестве значение T_{max} принято значение 2200 ч (примерно 3 месяца). Оперативность управления в рамках разработанной комплексной модели при оптимальном использовании источников информации может принимать значения, не превышающие 10-14 дней, то есть T_1 не превысит 330 ч. Таким образом эффективность управления ИБ по критерию «оперативность управления» может составить не менее 0,95, в то же время, эффективность «ручного» управления с использованием для оценки угроз только метода экспертных оценок, с частотой сбора экспертной группы 3 месяца – 0,7. При таких параметрах эффективность управления ИБ по введенному критерию будет выше нормативных методов управления (СМИБ) в пределах 25% (рис. 3.13).

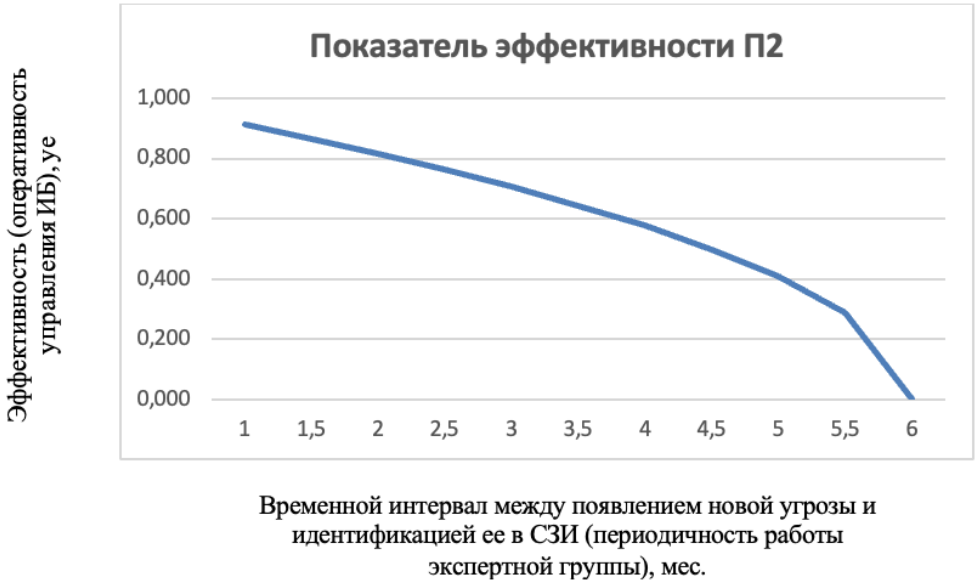

Рисунок 3.12. Зависимость эффективности управления ИБ от продолжительности T_1 (традиционный способ управления)

Рисунок 3.13. Зависимость эффективности управления от продолжительности Т1, (способ на основе разработанной модели)

Выводы

Используя предложенный способ управления информационной безопасностью в системах IoT на основе обратной связи в режиме численных оценок параметров процесса управления, разработана комплексная модель управления ИБ, реализующая непрерывный замкнутый цикл нечеткой оценки угроз и представлена ее структура.

Структура разработанной комплексной модели управления информационной безопасностью в системах IoT подразумевает параллельное (совместное) использование нескольких разнородных моделей, с достаточной полнотой отражающих различные свойства моделируемого процесса и включает нечеткое ядро – четыре последовательных нечетких модели на основе алгоритмов нечеткого вывода Мамдани, составляющие нечеткое ядро модели, экспертную модель определения начальных уровней угроз конфиденциальности, доступности и целостности, модель формализации сообщений об инцидентах информационной безопасности, а также формальную модель разрешенных конфигураций СЗИ.

Введен критерий эффективности управления по оперативности управления и обосновано повышение эффективности в предложенном способе в пределах 20 % по сравнению с традиционным способом, показана зависимость повышения эффективности от количества и качества используемых источников информации.

Глава 4 Методика автоматизированного управления информационной безопасностью в системах IoT на основе разработанной комплексной модели

Разработанная Методика автоматизированного управления информационной безопасностью в системах IoT представляет собой реализацию разработанной комплексной модели управления информационной безопасностью для практического применения в защищаемой системе.

С другой стороны, Методика управления может быть рассмотрена как формализация стандартизированной СМИБ [10-15] в части процессов управления рисками, управления защитными контрмерами, управление изменениями, управление контрольными мероприятиями и управление эффективностью деятельности.

Формализация указанных процессов, включенных в СМИБ, выполняется с целью получения преимуществ, позволяющих существенно повысить эффективность управления ИБ, а именно:

- осуществлять практически непрерывный по времени контроль изменения уровня актуальных угроз в защищаемой системе, а значит и контроль уровня защищенности информации, при этом используемый показатель защищенности ассоциирован с понятием общего риска ИБ по системе;
- численно определять достаточность вводимых защитных контрмер еще до практического ввода этих контрмер.

Таким образом обеспечивается повышение точности управления ИБ (в части выбора таких контрмер, которые гарантированно обеспечат заданную защищенность по критерию минимальной стоимости), оперативности управления (обнаружение факта, что показатель защищенности информации понизился, происходит за значительно меньшее время), а также реальное обеспечение принципа непрерывности управления ИБ по времени.

4.1 Анализ известных методик управления ИБ

Существующий подход к управлению информационной безопасностью, разработанный в первую очередь для АС, отражен в серии нормативных

документов – государственных стандартов ГОСТ Р 2700х – 2021 и основан на риско-ориентированном и процессном подходах. Стандарты вводят понятие системы менеджмента информационной безопасности (СМИБ), т.е. рассматривают процесс управления ИБ как систему (рис. 4.1), то есть взаимосвязанную совокупность подпроцессов. При этом указывается, что «используя семейство стандартов СМИБ, организации могут разрабатывать и совершенствовать систему управления защитой информационных активов и подготовиться к независимой оценке своей СМИБ».

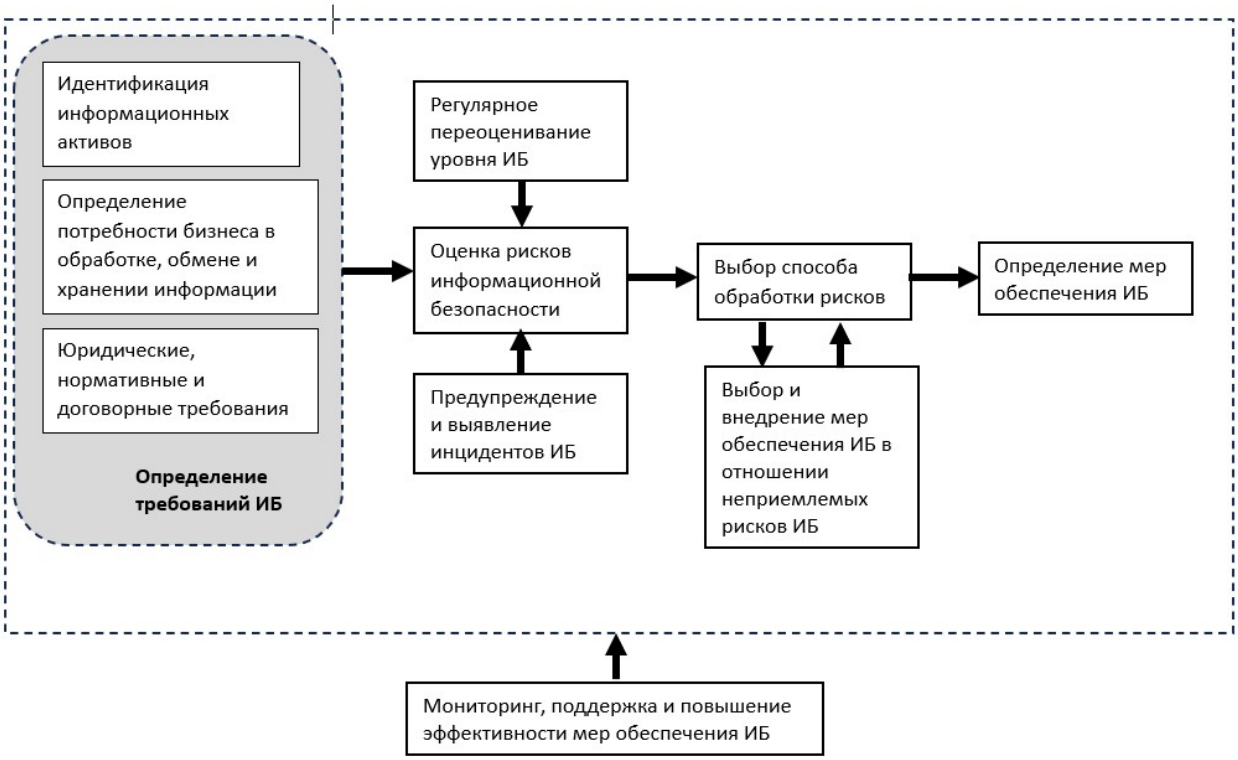

Рисунок 4.1 Интерпретация структуры СМИБ в соответствии с требованиями ГОСТ 2700х

Сам термин «информационная безопасность» отнесен к информации, которую рассматривают как актив, представляющий собой ценность, требующую соответствующей защиты, например, от потери доступности, конфиденциальности и целостности. Обеспечение возможности санкционированного своевременного получения точной и полной информации способствует эффективности бизнеса.

Эффективность СМИБ определена в самом общем виде как степень реализации запланированных мероприятий и достижения намеченных результатов.

При этом описание СМИБ [10-14] не содержит сведений о конкретизации и формализации показателей и критериев эффективности и предполагается, что они вводятся лицом, принимающим решения (ЛПР) для конкретной защищаемой системы. Вообще говоря, свободная трактовка понятия «эффективность управления информационной безопасностью», отсутствие единого подхода к оценке такой эффективности при наличии требований «повышения эффективности мер обеспечения ИБ» и, особенно, разработки плана мероприятий по повышению эффективности управления создает некую неоднозначную ситуацию и не способствует решению главной задачи – обеспечению ИБ в информационных системах, в частности системах интернета вещей, в смысле поддержания в защищаемой системе требуемого уровня защищенности информации.

Представленная на рисунке 4.1 структура СМИБ может рассматриваться как методика управления ИБ и обладает рядом достоинств, главными из которых является структуризация процесса управления ИБ – определение последовательности и содержания этапов управления, выделение критических узлов (точек принятия решения), а также неформальное определение целей управления.

Вместе с тем, по мнению автора, имеются существенные недостатки:

- методика носит неформальный характер;
- не учитывается специфика систем IoT;
- достаточность и оптимальность применяемых мер защиты определяется правильной последовательностью и полнотой выполненных рекомендаций на каждом этапе реализации методики.

Методика управления ИБ, содержащаяся в серии ГОСТ Р ИСО/МЭК 2700х может считаться развитием еще более неформальной методики, основанной на модели Деминга (модели PDCA), содержащейся в стандарте ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью». Типовая реализация модели Деминга представлена на рис. 2.4. Основным её достоинством является раскрытие содержания процесса управления информационной безопасностью как

непрерывный замкнутый процесс протяженностью, равной жизненному циклу защищаемой системы. При этом возможность проведения численных оценок и расчетов также не конкретизируется.

Кроме того, обе рассматриваемые методики управления ИБ нацелены на определение уровня риска ИБ (количественно или качественно) в защищаемой системе и далее предлагается несколько возможных способов обработки идентифицированного риска в случае, если этот риск превышает минимально допустимый уровень, определяемый ЛПР. При этом способы, связанные с передачей риска или отказом от риска наиболее актуальны при проектировании информационной системы (в модели Деминга – планировании), так как применение таких способов в реально функционирующей информационной системе влечет за собой пересмотр политики безопасности и, как следствие, изменение структуры системы или даже архитектуры системы.

Наиболее распространенным способом обработки риска в функционирующей системе можно считать способ снижения или уменьшения риска, который реализуется через применение различных контрмер, которые можно рассматривать как реакцию системы на изменение внешних дестабилизирующих факторов, главным из которых является повышение уровня актуальных угроз.

Наиболее важным аспектом здесь является неформальный характер таких методик. Отсутствие формализации не позволяет проводить численные оценки основных параметров процесса управления ИБ, делает неконкретной интерпретацию полученных результатов, то есть возможность сравнения альтернативных решений по каким-либо формализованным критериям.

Задача формализации моделей управления ИБ и построение на их основе методик управления осознается научным сообществом, что подтверждается значительным объемом публикаций, направленных на ее решение.

Так известны методики FRAP, OCTAVE Allegro, методика на основе программного инструмента RiskWatch for Information Systems, направленные на повышение формализации и прозрачности процедур экспертных оценок, но при этом ориентированные на качественную оценку рисков ИБ [15, 21, 100].

Формализованная методика управления системой информационной безопасности объекта критической инфраструктуры определяет эффективность управления информационной безопасностью как скалярную величину D:

$$D = F(s, u), \tag{4.1}$$

зависящую от безопасного состояния системы ***s*** и применяемых методов управления ***u*** (т.е. как функцию от состояния и управления). В качестве критерия эффективности управления определено «уменьшение пространства состояний управляемого объекта» [54].

Методика поддержки принятия решений администратором информационной системы в условиях кибератак предполагает достижение повышения эффективности системы управления ИБ за счет уменьшения времени необходимого на анализ и обработку рисков, а также за счет повышения точности прогнозов и обработки событий. При этом в большинстве реализаций предложенные показатели эффективности не формализуются и возможность их численной оценки не рассматривается. В отдельных случаях предлагаются различные способы количественной оценки отдельных параметров процессов управления, таких как критичность угроз, критичность активов, значения рисков ИБ по отдельным видам угроз, однако практически во всех случаях предполагается применение методов экспертных оценок на безальтернативной основе, различия заключаются лишь в технологиях выполнения таких оценок.

Все рассмотренные методики управления информационной безопасностью также предложены для традиционных автоматизированных систем, то есть специфика систем IoT не учитывается.

Результаты анализа известных методик управления информационной безопасностью представлены в табл.4.1.

Таблица 4.1. Сравнительный анализ методик управления ИБ

№ пп	Наименование	Где содержится	Область применения	Достоинства	Недостатки
1	Методика управления информационной безопасностью ФСТЭК	ГОСТ Р ИСО/МЭК 2700х «Менеджмент информационной безопасности» МД ФСТЭК «Оценка угроз…»	Управление ИБ в автоматизированных системах (АС)	Учитывает весь процесс управления	Носит неформальный характер. Не учитывает специфику систем IoT. Достаточность мер защиты определяется правильной последовательностью и полнотой выполненных рекомендаций.
2	Методика управления ИБ на основе модели Деминга (PDCA)	ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management» (Практическое руководство по управлению информационной безопасностью)	Управление ИБ в автоматизированных системах (АС)	Учитывает весь процесс управления	Носит неформальный характер Не учитывает специфику систем IoT Достаточность мер защиты определяется правильной последовательностью и полнотой выполненных рекомендаций.
3	Методики FRAP, OCTAVE Allegro	Научные публикации	Отдельные аспекты процесса управления ИБ	Понятна и проста в применении	Ориентирована на качественную оценку рисков ИБ Используется только метод экспертных оценок

4.2 Методика автоматизированного управления информационной безопасностью в системах IoT на основе разработанной комплексной модели

Методика автоматизированного управления информационной безопасностью в системах интернета вещей (далее Методика), основанная на реализации предложенных в СМИБ [10-15] риско-ориентированного и процессного подходов к управлению информационной безопасностью, интерпретированным для систем интернета вещей, представляет собой совокупность взаимосвязанных этапов, реализующих разработанную комплексную модель процесса управления ИБ в системах IoT (рис. 3.1).

Основными характеристиками комплексной модели управления ИБ в системах IoT, лежащей в основе Методики является использование управления по обратной связи, реализация непрерывного замкнутого цикла нечеткой оценки угроз, наличие нечеткого ядра, возможность оптимизировать управляющее воздействие по критериям стоимости и быстродействия, а также возможность численно оценивать эффективность по критериям «точность управления ИБ» и «оперативности управления ИБ».

Разработанная Методика

- реализует предложенный способ управления информационной безопасностью на основе использования обратной связи;
- представляет собой совокупность взаимосвязанных этапов, реализующих разработанную комплексную модель;
- реализует разработанную формальную модель управления ИБ в части основных подпроцессов СМИБ [10-15].

Методика управления ИБ в системах IoT реализуется в два этапа

- этап 1 – предварительный, подготовка исходных данных
- этап 2 - автоматизированное управление информационной безопасностью.

Алгоритм реализации предлагаемой Методики представлен на рис. 4.2.

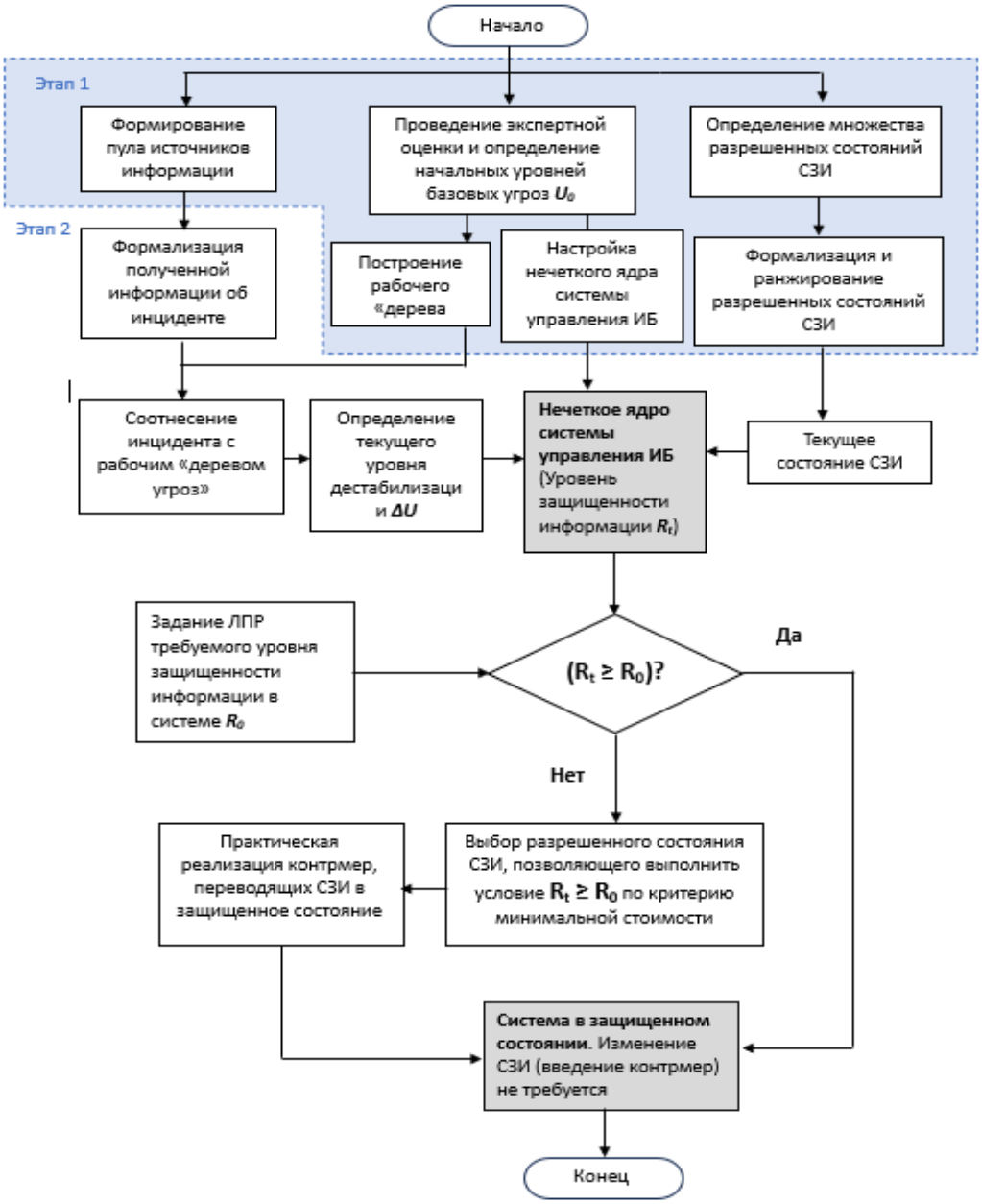

Рисунок 4.2 Алгоритм методики автоматизированного управления информационной безопасностью в системах Интернета вещей

Методика включает два последовательных этапа:

1) этап 1 - предварительный этап, целью которого является подготовка данных, определение конфигурации системы управления, задание неизменяемых параметров, определяемых ЛПР

2) этап 2, реализующий автоматизированное управление информационной безопасностью.

Этап 1 (Предварительный этап)

1. Проведение экспертной оценки начальных уровней базовых угроз информации в системе IoT и реализует предложенную экспертную модель. Основное назначение модели – определение численных значений начального уровня угроз конфиденциальности (level C_0), целостности (level A_0) и доступности (level I_0) информации в защищаемой системе на основании активации интуиции и опыта экспертов и предоставленных им сведений о структуре защищаемой системе, характере информационного массива и информационного процесса, а также характеристик среды безопасности. Вся информация в системе интернета вещей представляется как единый информационный актив, применительно к системам с централизованной обработкой. Технологически реализация экспертной процедуры проводится на основе «Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке угроз безопасности информации» [15, 16], дополненной обязательным требованием обеспечения согласованности мнений экспертов не ниже 0,25 по коэффициенту вариации.

В отличие от методики оценки угроз ФСТЭК [15], активизация экспертной модели предполагается в следующих случаях:

1) при внедрении предложенной Методики управления информационной безопасностью системы IoT;

2) при изменении конфигурации защищаемой системы (масштабировании);

3) при изменении политики безопасности организации.

Таким образом, в нормативно закрепленной методике владелец имеет возможность определить уровень защищенности информации в системе только в результате анализа результатов работы экспертной группы, при этом, временной интервал между проведением экспертных оценок в реальных условиях может составлять от 4 до 6 месяцев [17, 18]. В течение периода между работой экспертной группы, управление ИБ практически будет сводиться к

введению дополнительных контрмер на выявленные и не учитываемые ранее угрозы. При этом уровень защищенности информации в системе никак не контролируется, а это означает, что не существует объективной возможности оценить достаточность введенных контрмер.

2. Формирование пула используемых источников информации. Необходимо определить источники информации об информационных инцидентах 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. Основными параметрами формализации являются:

1) определение типа угрозы исходя из базовых свойств информации как объекта защиты – угрозы конфиденциальности, доступности или целостности;

2) соотнесение угрозы с одним из уровней «рабочего дерева угроз» для конкретной защищаемой системы;

3) определение того, является ли угроза уже учтенной в «рабочем дереве угроз» или же это неучтенная угроза;

4) присвоение неучтенной угрозе весового индекса исходя из соответствующего уровня дерева угроз.

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 в защищаемой системе;

- стоимость i-й конфигурации C_i не превышает стоимости C_{lim}, установленной ЛПР, при этом ЛПР исходит из своих возможностей и предпочтений, которые отражены в политике безопасности;
- время T_0, затрачиваемое на переход от ***i***-ой конфигурации к конфигурации (***i+1)*** (т.е. введение необходимых контрмер) не превышает времени T_{lim}, установленного ЛПР.

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

Каждое разрешенное состояние СЗИ представляется трехмерным вектором, определяющим возможности СЗИ:

$$\boldsymbol{F = s_i = \left(s_{i_{\text{ТЗИ}}}, s_{i_{\text{КЗИ}}}, s_{i_{\text{ФЗИ}}}\right)}, \quad (4.2)$$

где $s_{i_{\text{ТЗИ}}}$ - уровень технической защиты информации в i-й конфигурации СЗИ;

$s_{i_{\text{КЗИ}}}$ - уровень криптографической защиты информации в i-й конфигурации СЗИ;

$s_{i_{\text{ФЗИ}}}$ - уровень физической защиты элементов системы в i-й конфигурации СЗИ.

i – все возможные состояния СЗИ (*i = 1, 2, 3,..., I*)

При этом каждая координата трехмерного вектора определяется как

$$\boldsymbol{s_{im} = s_{im_1}, s_{im_2}, s_{im_3}, \dots, s_{im_n}}, \quad (4.3)$$

где *m = {ТЗИ, КЗИ, ФЗИ}*

m_n – параметры состояния отдельного элемента *m*.

В частности, для подсистемы технической защиты информации элементами m будут являться способы реализации идентификации и аутентификации, разграничения доступа к информации, способы сетевой защиты, протоколирование и аудит и т.д.

4. Настройка нечеткого ядра системы управления ИБ под конкретные особенности защищаемой системы интернета вещей. На этом

этапе, изменяя базы правил нечеткого вывода вложенных нечетких моделей возможно учесть такие особенности системы как приоритет защиты от одной из базовых угроз по сравнению с другими, например защита от угроз нарушения конфиденциальности более значима чем защита от угроз нарушения доступности или целостности. Общая структура нечеткого ядра системы управления ИБ представлена на рис. 4.3.

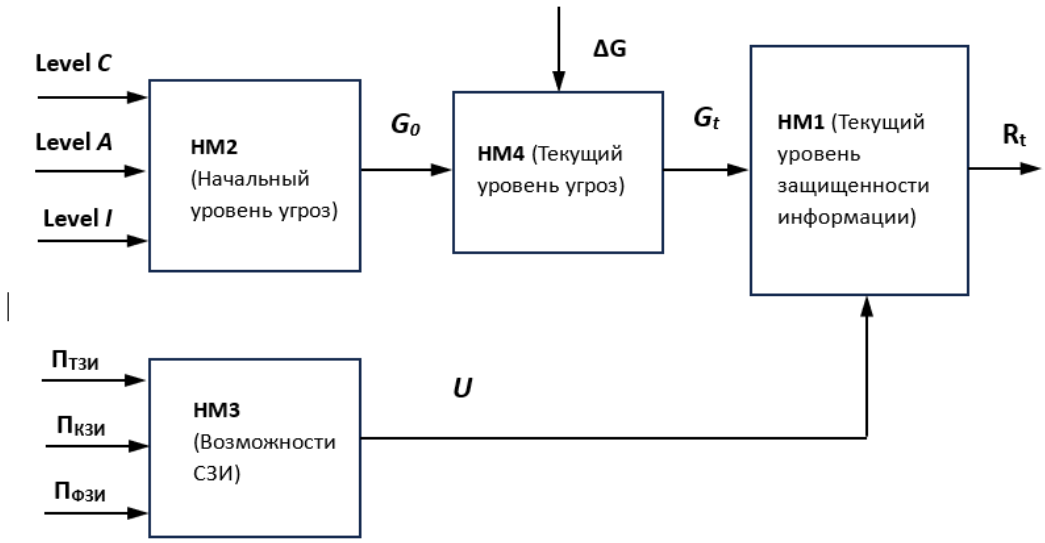

Рисунок 4.3 Структура нечеткого ядра системы управления информационной безопасностью

Нечеткое ядро системы имеет мультимодельную структуру и представляет собой четыре последовательные нечеткие модели Мамдани с 2-мя или 3-мя входами НМ1… НМ4. Такое решение позволяет осуществлять простую настройку каждой модели и графически интерпретировать результаты моделирования, что позволяет делать выводы о качественной адекватности каждой подмодели. На вход нечеткого ядра поступают:

- численные значения уровней базовых угроз, полученные в результате проведения экспертной оценки (Level A, Level C и Level I);
- численное изменение уровня угроз (уровень дестабилизации защищаемой системы) ΔG, полученное в результате формализации поступающей информации от подключенных источников;

- показатели реализации СЗИ в части мер технической, криптографической и физической защиты, полученные в результате формализации разрешенных состояний СЗИ ($П_{ТЗИ}$, $П_{КЗИ}$, $П_{ФЗИ}$).

На выходе нечеткого ядра системы управления ИБ возвращается численное значение текущего уровня защищенности информации в системе R_t.

Этап 2 (реализация автоматизированного управление информационной безопасностью)

Этап подразумевает использование специализированного программного обеспечения [19], реализующего нечеткое ядро системы управления ИБ IoT.

При вводе исходных данных, полученных на предварительном этапе, 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 $C_i \leq C_{lim}$, $C_i \rightarrow \mathbf{min}$. Такой выбор может быть осуществлен администратором безопасности или в автоматизированном режиме как реализация рекомендаций системы управления ИБ.

4.3 Рекомендации по практическому применению предложенной Методики управления информационной безопасностью в системах IoT

Рекомендации к практическому применению предложенной Методики направлены на максимальное повышения эффективности по введенным критериям:

- 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;
- использование разработанного ПО «Программа для управления информационной безопасностью систем Интернета вещей» свидетельство 2024615772 от 13.03.2024г.

В результате выполненной работы разработана Методика автоматизированного управления информационной безопасностью в системах IoT на основе разработанной Комплексной математической модели процесса управления ИБ, выполнена оценка эффективности предложенной Методики по критерию оперативности управления, обосновано повышение эффективности управления ИБ по введенному критерию по сравнению с известными методиками управления ИБ, основанными на неформальных описательных моделях.

Выводы

На основе разработанной комплексной модели процесса управления информационной безопасностью в системах IoT предложена Методика управления информационной безопасностью в виде алгоритма реализации, включающий два этапа - предварительный (подготовка исходных данных) и этап, реализующий автоматизированное управление информационной безопасностью на основе программной реализации нечеткого ядра модели ПО «Программа для управления информационной безопасностью систем Интернета вещей» свидетельство 2024615772 от 13.03.2024г.

Разработаны рекомендации по практическому применению предложенной Методики, направленные на повышение эффективности управления по критериям «Точность управления ИБ» и «Оперативность управления ИБ».

Выполнена оценка полученных результатов моделирования путем компьютерного и натурного испытаний (Приложения А, Б, В).

Разработана Методика управления информационной безопасностью в системах IoT с непрерывным циклом нечеткой оценки угроз, представленная в виде алгоритма выполнения последовательных и связанных этапов: предварительный (подготовка исходных данных) и этап, реализующий автоматизированное управление информационной безопасностью.

Особенностями предложенной Методики являются:

- учет особенностей информационных систем, использующих технологии Интернета вещей;
- постоянный контроль уровня защищенности информации в системе в режиме численной оценки;
- обеспечение возможности выбора контрмер как реакции системы на снижение уровня защищенности информации в системе по критерию минимальных затрат.

Указанные особенности обеспечивают значительное повышение эффективности управления информационной безопасностью по предложенным критериям «оперативности управления ИБ» и «точности управления ИБ» при соблюдении рекомендаций по внедрению Методики.

Таким образом, практическая значимость работы заключается в повышении эффективности управления информационной безопасностью в системах, использующих технологии Интернета Вещей, за счет сокращения времени пребывания системы в состоянии сниженного уровня защищенности информации по причине несвоевременного введения контрмер, а также за счет повышения точности управления, выражающегося в выборе контрмер для приведения защищаемой системы к требуемому уровню защищенности информации по критерию минимальных затрат.

Заключение и вывод по работе

В результате исследования современного состояния проблемы управления информационной безопасностью в системах Интернета вещей обоснована необходимость формализации процессов управления информационной безопасностью.

В результате 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.

Используя полученные результаты предложен способ формализации основных параметров процесса управления на основе управления на основе обратной связи в режиме численных оценок параметров процесса управления. На основе предложенного способа разработана комплексная модель процесса управления информационной безопасностью в системах Интернета вещей. Обоснована корректность и качественная адекватность модели.

Выполнена оценка полученных результатов моделирования путем компьютерного и натурного испытаний, в результате чего подтверждено повышение эффективности управления ИБ по введённым критериям.

На основе разработанной комплексной модели, предложена методика автоматизированного управления информационной безопасностью в системах Интернета вещей с непрерывным циклом нечеткой оценки угроз.

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

Результаты исследований внедрены в учебный процесс МТУСИ и в практическую деятельность организации.

Все задачи диссертационного исследования выполнены, цель исследования достигнута.

Список сокращений и обозначений

АС	Автоматизированная система
СЗИ	Система защиты информации
ИБ	Информационной безопасность
ЛПР	Лицо, принимающее решение
IoT	Интернет вещей
IIoT	Промышленный интернет вещей
СМИБ	Система менеджмента информационной безопасности
КИС	Корпоративные информационные сети
IT	Информационные технологии
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации
КИИ	Критическая информационная инфраструктура
M2M	Machine-to-Machine, взаимодействие «от машины к машине»
ИВ	Интернет вещей

Список использованной литературы

1 Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента РФ от 2 июля 2021 г. N 400

2 Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5.12.2016г. № 646.

3 Федеральный закон № 63-ФЗ от 06.04.2011 г. «Об электронной подписи» (ред. от 08.06.2020г.).

4 Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006г.

5 Федеральный закон РФ № 187-ФЗ «О безопасности критической информационной инфраструктуры» от 26.07.2017г.

6 Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006г.

7 Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008г. № 351.

8 ГОСТ Р ИСО/МЭК 15408-1 2012 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Часть 1
«Введение и общая модель». Москва Стандартинформ 2014.

9 ГОСТ Р ИСО/МЭК 15408-2 2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Часть 2
«Функциональные требования безопасности». Москва Стандартинформ 2009.

10 ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

11 ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

12 ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации».

13 ГОСТ Р ИСО/МЭК 27004-2021 «Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

14 ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Москва Стандартинформ 2011.

15 ГОСТ Р 51897-2011/Руководство ИСО 73:2009. Менеджмент риска. Термины и определения.

16 РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992г.

17 РД «Защита от несанкционированного доступа к информации. Термины и определения». Утверждено решением председателя Гостехкомиссии России
от 30 марта 1992г.

18 РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992г.

19 РД «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
Утверждены приказом ФСТЭК России от 18.02.2013 г. № 21

20 РД «Требования о защите информации, содержащейся в информационных системах общего пользования». Приложение к Приказу ФСБ России, ФСТЭК России от 31.08.2010 г. № 416/489

21 Методический документ «Методика оценки угроз безопасности информации»
Утвержден ФСТЭК России 5 февраля 2021 г.

22 Методический документ «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11.02.2014 г.

23 ПНСТ 518-2021 (ИСО/МЭК 20924:2018) Предварительный национальный стандарт Российской Федерации «Информационные технологии. Интернет вещей. Термины и определения».

24 ГОСТ Р ИСО/МЭК 29161-2019 Информационные технологии. Структура данных. Уникальная идентификация для интернета вещей.

25 ГОСТ Р 59026-2020 Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе стандарта LTE в режиме NB-IoT. Основные параметры.

26 ISO/IEC TR 30166:2020 Internet of things (IoT) — Industrial IoT.

27 Предварительный национальный стандарт Российской Федерации
ПНЕТ 419-2020 Информационные технологии. Интернет вещей. Общие положения.

28 Предварительный национальный стандарт Российской Федерации ПНЕТ 420-2020
Информационные технологии. Интернет вещей промышленный. Типовая архитектура.

29 Предварительный национальный стандарт Российской Федерации ПНЕТ 433-2020 Информационные технологии. Интернет вещей. Требования к платформе обмена данными для различных служб интернета вещей.

30 Предварительный национальный стандарт Российской Федерации ПНСТ 642-2022 Информационные технологии. Интернет вещей промышленный. Общие положения.

31 Маликов Р.Ф. Основы математического моделирования. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2010. – 368 с.: ил. ISBN 978-5-9912-0123-0/

32 Моделирование систем и процессов: учебник для академического бакалавриата / В.Н.Волкова и др. ; под ред. В.Н.Волковой, В.Н.Козлова. – М. : Издательство Юрайт, 2018. – 450с. ISBN 978-5-534-02422-7.

33 Кутузов О. И. Моделирование систем. Имитационный метод: учебник для вузов / О. И. Кутузов, Т. М. Татарникова.— 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 224 с. : ил. — Текст : непосредственный. ISBN 978-5-507-48872-8

34 Пегат А. Нечеткое моделирование и управление / А.Пегат : пер. с англ. – 2-е изд. – М.: БИНОМ. Лаборатория знаний, 2017. – 798с.: ил. – (Адаптивные и интеллектуальные системы). ISBN 978-5-9963-1495-9.

35 Кудинов Ю.Н. и др. Нечеткие модели и системы управления / под ред. Проф. Ф.Ф.Пащенко – М.: ЛЕНАНД, 2017. – 328с. ISBN 978-5-9710-4960-9.

36 Штовба С. Д. Проектирование нечетких систем средствами MATLAB //М.: Горячая линия–телеком. – 2007. – Т. 288. – С. 35.

37 Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ – Петербург, 2005. – 736.: ил. ISBN 5-94157-087-2.

38 Новак Вилем, Перфильева Ирина, Мочкорж Иржи. Математические принципы нечеткой логики / Пер с англ.; Под ред. Аверкина А.Н. – М.: ФИЗМАТЛИТ, 2006. – 352 с. – ISBN 5-9221-0399-7.

39 Воронов, Ю. Е. Основы системного анализа : учебное пособие / Ю. Е. Воронов, А. А. Баканов. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2023. — 133 с. — ISBN 978-5-00137-381-0.

40 Перри Ли. Архитектура интернета вещей / пер с англ. М.А. Райтмана. - М.: ДМК Пресс, 2020. – 454 с.: ил. ISBN 978-5-97060-8.

41 Грингард С. Интернет вещей: Будущее уже здесь / Самюэль Грингард ; Пер. с англ. – М.: Альпина Паблишер, 2019. – 188 с. ISBN 978-5-9614-6472-6.

42 Торокин, Анатолий Алексеевич. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А.Торокин.-М.: Гелиос АРВ, 2005. 960 с.: ил. – ISBN 5-85438-140-0.

43 Цирлов В. Л. Теоретические основы информационной безопасности автоматизированных систем //М.: Просвещение.—2006.—173 с. – 2008.

44 Дойникова, Е. В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью / Е. В. Дойникова, И. В. Котенко. – Москва : Российская академия наук, 2021. – 184 с. – ISBN 978-5-907366-23-7. – EDN QZALSO.

45 Бутенко Е. Д., Черников И. С. Киберпреступность как тормозящий фактор развития цифровой экономики //Глобальные и региональные аспекты устойчивого развития: современные реалии. – 2020. – С. 361-374.

46 Гагарин А. Е. Методы противодействия угрозам применения цифровой подписи в постквантовый период / А. Е. Гагарин, А. И. Ларин // Телекоммуникационные и вычислительные системы 2020 : Труды международной научно-технической конференции, Москва, 14–17 декабря 2020 года / Московский технический университет связи и информатики. – Москва: Научно-техническое издательство "Горячая линия-Телеком", 2020. – С. 502-522. – EDN VCCDPI

47 Громыко П. С., Осанов В. А. Безопасность интернета-вещей. (ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»). Проблемы техники и технологий телекоммуникаций ПТиТТ-2020: Материалы XXII Международной научно-технической конференции (г. Самара, 17 – 20 ноября 2020 г.) : материалы конференции. — Самара : ПГУТИ, 2020. — 393 с. — ISBN 978-5-907336-06-3.

48 Зегжда Д.П. Подход к обнаружению инцидентов безопасности в Интернете вещей с использованием технологии SIEM / Д.П. Зегжда, Д.С. Лаврова // Интеллектуальные технологии на транспорте. — 2017. — № 1. — С. 35-41. — ISSN 2413-2527.

49 Дойникова Е. В. и др. Методика оценивания защищенности на основе семантической модели метрик и данных //Вопросы кибербезопасности. – 2021. – №. 1 (41). – С. 29-40.

50 И. В. Котенко, И. Б. Паращук. Нечеткое управление информацией и событиями безопасности: особенности построения функций принадлежности. DOI: 10.24143/2072-9502-2021-3-7-15. УДК 004.942

51 И.Б. Паращук, проф., д-р техн. наук, И.В. Котенко, проф., д-р техн. наук, И.Б. Саенко, проф., д-р техн. наук. Управление информацией и событиями безопасности на основе нечетких алгоритмов. Доклад УДК 004.056.53.

52 Федорченко Е.В., Новикова Е.С., Котенко И.В., Гайфулина Д.А., Тушканова О.Н.,

Левшун Д.С., Мелешко А.В., Муренин И.Н., Коломеец М.В. Система измерения защищенности информации и персональных данных для устройств интернета вещей. DOI:10.681/2311-3456-2022-5-28-46.

53 Довгаль В.А., Довгаль Д.В. - Анализ проблем обеспечения информационной безопасности беспроводных сенсорных сетей и методов обеспечения безопасности Интернета вещей. Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки - 2021г. №1 (276). УДК 004.738.5:004.056

54 М.А. Карпов. Методика управления системой информационной безопасности

Объекта критической инфраструктуры. Известия ТулГУ. Технические науки. 2021. Вып. 12 УДК 621.37.39.001.5. DOI: 10.24412/2071-6168-2021-12-235-247

55 И.В. Аникин. Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики. СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ 2023. Т. 5, № 3 (12). С. 93–113. ISSN 2658-5014 (Print). УДК 004.056.5.

56 Купцова А.С. Правовое регулирование использования интернета вещей. DOI:10.24412/2076-1503-2021-7-225-230б NIION: 2018-0076-7/21-037 MOSURED: 77/27-023-2021-07-236

57 В.А. Минаев, К.М. Бондарь, Е.В. Вайц, И.А. Беляков. Дискретно-событийное моделирование процессов мониторинга и управления информационной безопасностью. Вестник Российского нового университета. Серия «Сложные системы» 32 Выпуск 3/2019. DOI: 10.25586/RNU.V9187.19.03.P.032, УДК 004.94

58 Л.В. Астахова, В.И. Цимбол. Применение самообучающейся системы корреляции событий информационной безопасности на основе нечеткой логики при автоматизации систем менеджмента информационной безопасности. Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника».

2015. Т. 16, № 1. С. 165–169. УДК 004.056 DOI: 10.14529/ctcr160116.

59 Липатников В.А., Синдеев М.А., Косолапов В.С. Методика поддержки принятия решений администратором информационной системы в условиях кибератак. ТРАНСПОРТ РОССИИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ – 2021. 09-10 ноября 2021 года

Материалы Международной научно–практической конференции. Том 1. Санкт-Петербург – 2021г.

60 Гвоздик Я.М. Модель и методика оценки систем защиты информации автоматизированных систем: дисс. канд. техн. наук: 05.13.19 / СПИИРАН. – Санкт-Петербург. – 2011. – 137с.

61 Коломойцев В.С. Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации.: дисс. канд. техн. наук: 05.13.19 / Университет ИТМО. – Санкт-Петербург. – 2018. – 175с.

62 Чемин А.А. Разработка методов оценки эффективности систем защиты информации в распределенных информационных системах специального назначения: дисс. канд. техн. наук: 05.13.19 / ФГОУ «Московский государственный институт электроники и математики» (Технический университет). – Москва. – 2009. – 211с.

63 Лившиц И.И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами: дисс. доктора техн. Наук: 05.13.19 / СПИИРАН. – Санкт-Петербург. – 2018. – 407 С.

64 Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь, – 2021, № 4. – с.66-73.

65 Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С. Маркова - М.: ДМК Пресс. – 2017. – 224с.: ил.

66 Scott Barman. Writing Information Security Policies. Landmark (New Riders) 2002. – 216c. ISBN: 9781578702640.

67 Jason T. Luttgens, Matthew Pepe, Kevin Mandia. Incident Response & Computer Forensics. 3rd Edition. McGraw-Hill 2014. ISBN: 9780071798693.

71 Brian Carrier. File Systems Forensic Analysis. Addison-Wesley Professional, 17 мар. 2005 г. – 600с. Library of Congress Catalog Number: 2004116962.

72 Дмитриев А.В. Информационная безопасность интернета вещей. «Прикладные проблемы системной безопасности: материалы Всероссийской конференции с международным участием. 21-22 сентября 2023 г.»: материалы конференции. — Елец: ЕГУ им. И.А. Бунина, 2023. — ISBN 978-5-00151-397-1. — С. 31.

73 Н.А. Камалян, А.С. Ершов. Моделирование угроз безопасности интернет-вещей. «Научно-практическая конференция. Материалы научно-практической конференции «Прикладные процессы в области информационной безопасности» и научно-практической конференции «Тенденции развития методов защиты информации» и научно-практической конференции «Тенденции развития методов защиты информации»: материалы конференции. — Самара: ПГУТИ, 2023. — ISBN 978-5-907336-52-0. — С. 16.

74 Вьющенко О.О., Маслова М.А. Об обеспечении безопасности в сфере интернета вещей. // Научный результат. Информационные технологии. – Т.6, №3, 2021.

75 Мошак, Н. Н. Основы управления информационной безопасностью: учебное пособие / Н. Н. Мошак ; под редакцией В. В. Овчинникова. — Санкт-Петербург: ГУАП, 2022. — 141 с. — ISBN 978-5-8088-1711-1.

76 Е. Ю. Головина, А. В. Журавлева, Л. И. Татарникова. Оценка состояния безопасности ИТ-инфраструктуры в организации. // Молодежный вестник ИрГТУ. — 2022. — № 2. — С. 266-272. — ISSN 1683-0407.

77 Л. А. Баранов, Н. Д. Иванова, И. Ф. Михалевич, Б. В. Желенков. Нечеткая система оценки рисков информационной безопасности интеллектуальных систем водного транспорта» (нечеткая система оценки рисков информационной безопасности интеллектуальных систем водного

транспорта // Автоматика на транспорте. — 2024. — № 1. — С. 7-17. — ISSN 2412-9186.

78 Обзор TAdviser «Интернет вещей». Интернет вещей, IoT, M2M рынок России, 2023/03/24 — URL: https://www.tadviser.ru/index.php/Статья:Интернет_вещей%2C_IoT%2C_M2M_%28рынок_России%29#

79 Гиб Соребо «Интернет Вещей»: Управление рисками. CONTROL ENGINEERING РОССИЯ #1 (61), 2016. — URL: https://controleng.ru/perspektiva/riski_iot/.

80 Риски и угрозы в Интернете вещей. Блог компании Доктор Веб «Интернет вещей» — URL: https://habr.com/ru/companies/drweb/articles/460433/

81 Патент № 2717721 C1 Российская Федерация, МПК G06F 21/00. Способ создания автоматизированных систем управления информационной безопасностью и система для его осуществления : № 2019129630 : заявл. 20.09.2019 : опубл. 25.03.2020 / А. Б. Еркин, А. С. Антипинский, В. В. Богданов. – EDN RDSDRK.

82 Заде, Л. Понятие лингвистической переменной и его применение к принятию приближенных решений [Текст] / Л. Заде, под ред. Н.Н. Моисеева, С.А. Орловского; пер. с англ. – М.: Мир. – 1976. – 168 С.

83 Серова А.Г. Анализ эффективности системы управления информационной безопасностью государственного учреждения. ЭКОНОМИКА И УПРАВЛЕНИЕ. №6 (140) 2017.

84 Миняев А.А., Будько М.Ю. Методика оценки эффективности системы защиты персональных данных информационной системы // Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур: Межвузовский сборник трудов VI

Всероссийской научно-технической конференции (ИКВО НИУ ИТМО, 10 декабря 2015 г.). – 2016. – С. 43-45.

85 Миняев А.А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных. // IX Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: Сборник научных статей, СПбГУТ, – 2020. – С. 716-719.

86 Бухарин В.В., Липатников В.А., Сахаров Д.В. Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии. – 2013. № 3 (77). – С. 102-109.

87 Андрианов В.И., Красов А.В., Липатников В.А. Инновационное управление рисками информационной безопасности. Санкт-Петербург: СПбГУТ, – 2012. – 396 с.

88 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. – EDN HGYJAJ.

89 Информационные технологии: учебник / Л.Н.Демидов, В.Б.Терновсков, С.М.Григорьев, Д.В.Крахмалев. - Москва: КНОРУС, 2020. – 222с. ISBN 978-5-406-07568-5.

90 Костюк А.В., Бобонец С.А., Флегонтов А.В., Черных А.К. Информационные технологии. Базовый курс: Учебник. – СПб.: Издательство «Лань», 2018. – 604 с.: ил. ISBN 978-5-8114-2906-6.

91 Федорченко Е.В., Новикова Е.С., Котенко И.В. и др. Система измерения защищенности информации и персональных данных для устройств интернета вещей. Вопросы кибербезопасности. 2022. № 5(51). с. 28-44.

92 Милославская Н. Г., Толстой А. И. Управление информационной безопасностью: Конспект лекций. Учебное пособие. М.: НИЯУ МИФИ, 2020. – 536 с. УДК 004.056.5 (075.8) ББК 32.973.26-018.2я7.

93 Вовик А. Г. О возможности численных метрик в управлении информационной безопасностью / А. Г. Вовик, А. И. Ларин // Наукоемкие технологии в космических исследованиях Земли. – 2022. – Т. 14, № 6. – С. 12-19. – DOI 10.36724/2409-5419-2022-14-6-12-19. – EDN BRHJMS.

94 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

95 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.

96 Вовик, А. Г. Комплексная математическая модель процесса управления информационной безопасностью в системах IoT / А. Г. Вовик // 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. (РИНЦ)

97 Вовик А.Г., Ларин А.И., Вовик В.С. Количественные оценки в формальных моделях управления информационной безопасностью систем Интернета Вещей // Инновационное развитие: потенциал науки и

современного образования: монография. – Пенза: «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2024. – С. 64-74. ISBN 978-5-00236-358-2.

98 Вовик А. Г. Подход к управлению информационной безопасностью систем Интернета вещей посредством формирования и использования в системе управления сигнала отрицательной обратной связи // Материалы XIX Санкт-Петербургской международной конференции «Региональная информатика (РИ-2024)»

99 Вовик, А. Г. Проблемы моделирования процессов управления информационной безопасностью в автоматизированных системах / А. Г. Вовик // Приборы и системы. Управление, контроль, диагностика. – 2024. – № 9. – С. 28-39. – DOI 10.25791/pribor.9.2024.1524. – EDN DRPKJA.

100 Вовик, А. Г. Методика автоматизированного управления информационной безопасностью в системах интернета вещей / А. Г. Вовик, Л. И. Воронова // Наукоемкие технологии в космических исследованиях Земли. – 2024. – Т. 16, № 4. – С. 4-11. – DOI 10.36724/2409-5419-2024-16-4-4-11. – EDN SJWHGZ.

101 Клипов, Д.Д. Проблемы обеспечения безопасности в IoT [Текст] / Д.Д. Клипов, А.А. Рябцев// 55-я Междунар. науч. конф. «МНСК-2017: Информационные технологии» (материалы конференции): тр. конф. – Новосибирск, – 2017. – С. 37.

102 Уппит, О. Опасные предметы: кто и зачем взламывает интернет вещей и как с этим быть [Электронный ресурс] / URL: https://apparat.cc/world/internet-of-things/ (д.о. 24.09.20).

103 ГОСТ Р 70924-2023 ИСО/МЭК 30141:2018 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Информационные технологии. ИНТЕРНЕТ ВЕЩЕЙ. Типовая архитектура

104 Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. 410 с

105 Graën, Johannes & Bertamini, Mara & Volk, Martin. (2018). Cutter – a Universal Multilingual Tokenizer.

106 Skorkovská, Lucie. (2012). Application of Lemmatization and Summarization Methods in Topic Identification Module for Large Scale Language Modeling Data Filtering. 7499. 10.1007/978-3-642-32790-2_23

107 Liu S., Yang Y., Forrest J.Y.-L. Grey Systems Analysis: Methods, Models and Applications. Singapore:Springer; 2022. DOI:10.1007/978-981-19-6160-1

108 Patil AN., Walke G, Mahesh G. Grey Relation Analysis Methodology and its Application. Research Review. 2019;4(2): 409-411. DOI:10.5281/zenodo.2578088

109 Yang W., Wu Y. A Novel TOPSIS Method Based on Improved Grey Relational Analysis for Multiattribute Decision-Making Problem. Mathematical Problems in Engineering. 2019;2019:8761681. DOI:10.1155/2019/8761681

110 Hsiao S.-W., Lin H.-H., Ko Y.-C. Application of Grey Relational Analysis to Decision-Making during Product Development. Eurasia Journal of Mathematics, Science and Technology Education. 2017;13(6):2581-2600. DOI:10.12973/eurasia.2017.01242a].

111 Марочкина А.В., Парамонов А.И. Метод маршрутизации трафика в трехмерной сети Интернета вещей высокой плотности с применением серого реляционного анализа // Труды учебных заведений связи. 2023. Т. 9. № 4. С. 75-85. DO1:10.31854/1813-324X-2023-9-4-75-85

112 Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Приложения

Приложение А. Сведения о государственной регистрации «Программа для управления информационной безопасностью систем Интернета Вещей»

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

RU2024615772

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства): **2024615772** Дата регистрации: **13.03.2024** Номер и дата поступления заявки: **2024614411 06.03.2024** Дата публикации и номер бюллетеня: **13.03.2024 Бюл. № 3** Контактные реквизиты: **нет**	Автор(ы): **Вовик Андрей Геннадьевич (RU)** Правообладатель(и): **Вовик Андрей Геннадьевич (RU)**

Название программы для ЭВМ:
Программа для управления информационной безопасностью систем Интернета Вещей

Реферат:
Программа предназначена для практической реализации модели процесса управления информационной безопасностью в системах Интернета Вещей. Программа обеспечивает возможности ввода численных значений уровня актуальных угроз целостности, доступности и конфиденциальности; уровня возможности технических, криптографических и физических средств защиты информации; изменение уровня актуальных угроз и получение численного значения уровня защищенности информации в системе Интернета Вещей. Программа включает четыре модуля: первый модуль позволяет получить численное значение, характеризующее возможности конфигурации системы защиты информации; второй модуль позволяет численно оценить уровень актуальных угроз в защищаемой системе; третий модуль предназначен для корректировки уровня актуальных угроз в защищаемой системе с учетом информации о появлении новых актуальных угроз из доступных источников; четвертый модуль позволяет получить оценку текущего уровня защищенности информации в защищаемой системе Интернета Вещей. Программа может использоваться владельцем информационной системы, использующей технологии Интернета Вещей, для автоматизированного управления информационной безопасностью. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows, MacOS.

Язык программирования: Python

Объем программы для ЭВМ: 442 КБ

Приложение Б. Копия акта внедрения в ООО «Эмбеддед Системс Рус»

ООО «Эмбеддед Системс Рус»

embedded systems

111024, г. Москва, 1-я ул. Энтузиастов, д. 3, стр. 1, ком.46.
Тех. поддержка: 8-800-775-06-34, +7 (495) 988-09-91
Сайт: logicmachine.net.ru Почта: zakaz@lm.net.ru
ИНН: 7720383487 КПП: 772001001 ОКПО: 15845677
ООО "Банк Точка"
р/с 40702810301500050876, к/с 30101810745374525104
г. Москва БИК: 044525104

LogicMachine.net LogicMachine.net LogicMachine.net LogicMachine.net

Исх. № 240515/1
от 15 мая 2024 г.

АКТ
об использовании результатов диссертационной работы
Вовика Андрея Геннадьевича,
представленной на соискание ученой степени кандидата

Комиссия в составе: генеральный директор Сасс Дмитрий Владимирович, заместитель директора Фуртат Андрей Викторович, инженер Сасс Василий Дмитриевич, составила настоящий акт о том, что результаты диссертационной работы Вовика Андрея Геннадьевича на тему: «Исследование и разработка методов построения моделей управления информационной безопасностью IoT систем» используются в работе технического отдела ООО «Эмбеддед Системс Рус», а именно:

- методика автоматизированного управления информационной безопасностью в системах IoT используется для определения контрмер, необходимых для поддержания уровня защищенности информации в защищаемой системе тестовых стендов с открытым доступом в сеть Интернет в техническом отделе компании на заранее заданном уровне,
- комплексная математическая модель процесса управления информационной безопасностью в системах IoT в части нечеткого ядра модели в виде последовательных нечетких моделей типа Мамдани (программная реализация), а также и формальной модели разрешенных конфигураций системы защиты информации (СЗИ) используется в повседневной деятельности для оценки уровня защищенности информации в системе IoT тестовых стендов с открытым доступом в сеть Интернет.

Результаты диссертационного исследования позволили сократить временной интервал между актуализацией угрозы информационной безопасности и применением контрмеры (повысить эффективность управления информационной безопасностью в системе по критерию оперативности) и повысить уверенность у лица, принимающего решение, о достаточности введенной контрмеры и отсутствия перерасхода материальных средств.

Инженер Сасс В.Д

«ЭМБЕДДЕД СИСТЕМС РУС»

Заместитель директора Фуртат А.В.

Генеральный директор Сасс Д.В.

Приложение В. Копия акта внедрения в учебный процесс Московского технического университета связи и информатики

УТВЕРЖДАЮ
Проректор по учебной работе
Московского технического университета
связи и информатики
_____ А.С. Аджикова
«23» апреля 2024 г.

АКТ
об использовании результатов диссертационной работы
Вовика Андрея Геннадьевича на тему:
«Исследование и разработка методов построения моделей управления информационной безопасностью IoT систем» в учебном процессе кафедры «Информационная безопасность»

Комиссия в составе: заведующий кафедрой «Информационная безопасность» д.т.н., профессор Шелухин Олег Иванович; декан факультета «Кибернетика и информационная безопасность» к.т.н., доцент Иевлев Олег Павлович; начальник Отдела планирования и организации учебного процесса МТУСИ Кузнецова Виктория Анатольевна составили настоящий акт о том, что результаты диссертационной работы Вовика Андрея Геннадьевича на тему: «Исследование и разработка методов построения моделей управления информационной безопасностью IoT систем» используются в учебном процессе кафедры «Информационная безопасность», 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»

Эффективность внедрения заключается в формировании у студентов глубокого понимания и усвоения основ управления информационной безопасностью, усвоении целей, задач и условий обеспечения эффективности управления, позволяет конкретизировать требования основных нормативных документов в области управления информационной безопасностью, формализовать способы количественной оценки информационных рисков в защищаемой системе.

Заведующий кафедрой ИБ _____ Шелухин О.И.

Декан факультета КиИБ _____ Иевлев О.П.

Начальник ОПиОУП _____ Кузнецова В.А.