Эшелон
комплексная безопасность

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

107023, г. Москва, ул. Электрозаводская, д. 24, стр. 1, тел.: +7 (495) 223 23 92, факс: +7 (499) 753-04-14, mail@npo-echelon.ru, npo-echelon.ru

В диссертационный совет
99.2.038.03
г. Санкт-Петербург, пр.
Большевиков, д. 22, корп. 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук, доцента
Цирлова Валентина Леонидовича
на диссертационную работу
Вовика Андрея Геннадьевича
«Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз»,
представленную к защите на соискание ученой степени кандидата технических наук по специальности 2.3.6. — «Методы и системы защиты информации, информационная безопасность»

I. Актуальность направления и темы диссертационного исследования

Актуальность направления диссертационного исследования обусловлена потребностью в разрешении противоречия между возрастающим распространение систем класса «интернет вещей» (IoT) и недостаточным уровнем развития теоретических исследований в области анализа их уязвимостей и обеспечения построения эффективных систем управления информационной безопасности для данного класса решений.

Диссертационное исследование А.Г. Вовика посвящено решению актуальной научной задачи в области обеспечения информационной безопасности (ИБ) в системах интернета вещей.

В условиях роста числа подключенных устройств и увеличения объемов передаваемой информации, проблематика защиты IoT-систем приобретает особую значимость. Автор справедливо отмечает, что существующие методы и подходы к управлению ИБ недостаточно формализованы, а, кроме того, не всегда применимы к IoT-системам из-за их специфических особенностей.

Тема диссертации, направленность проведённых исследований и полученных результатов соответствует Паспорту специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

II. Обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна

В диссертационном исследовании автор, опираясь на проведенный анализ современных методов управления информационной безопасностью, демонстрирует системность и комплексность своего подхода к решению научной задачи.

В работе автор аргументированно показал необходимость формализации процессов управления информационной безопасностью в системах IoT и моделирования таких процессов в целях поддержания заданного уровня защищенности информации, а также обосновал эффективность предложенной методики по введенным критериям

эффективности – «точность управления» и «оперативность управления» информационной безопасностью.

Обоснованность научных положений, выводов и рекомендаций, представленных в диссертации, подтверждается:

1. Тщательным анализом нормативных документов, научных публикаций и практического опыта в области ИБ и IoT.
2. Корректным применением методов моделирования, включая методы нечеткого моделирования.
3. Результатами компьютерного моделирования и натурных исследований, демонстрирующими эффективность предложенной методики.
4. Апробацией результатов исследования в научно-производственной деятельности и учебном процессе.

На наш взгляд, к наиболее существенным новым научным результатам, полученным в диссертационном исследовании, можно отнести следующие:

1. Предложен способ управления ИБ систем IoT посредством формирования и использования в системе управления отрицательной обратной связи в режиме численной оценки основных параметров процесса управления информационной безопасностью;
2. Разработана комплексная модель процесса управления ИБ в системах IoT, реализующей принцип управления с обратной связью и обеспечивающей непрерывный замкнутый цикл оценки угроз;
3. Разработана методика управления информационной безопасностью в системах IoT с непрерывным замкнутым циклом нечеткой оценки угроз на основе разработанной комплексной модели.

Достоверность полученных результатов подтверждается, на наш взгляд, корректностью используемых методов исследования, согласованностью теоретических выводов с результатами моделирования и экспериментальных данных, а также внедрением результатов в практику.

III. Теоретическая значимость и практическая ценность результатов исследований

Работа носит ярко выраженный теоретический характер. Теоретическая значимость исследования состоит в развитии 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.

Практическая значимость полученных результатов заключается в возможности их использования для повышения эффективности управления ИБ в IoT-системах, что подтверждается внедрением результатов в ООО «Эмбеддед Системс Рус» и учебный процесс МТУСИ.

Конкретные пути использования результатов исследования включают:

— Разработку и внедрение систем автоматизированного управления ИБ в IoT-системах.

— Повышение уровня защищенности информации и снижение рисков в IoT-системах.

— Совершенствование методов обучения и подготовки специалистов в области ИБ.

IV. Характеристика опубликованности результатов и положений, выносимых на защиту

Опубликованность научных результатов диссертационной работы подтверждается (согласно РИНЦ) шестью журнальными статьями, опубликованными в рецензируемых изданиях, рекомендованных ВАК. Материалы работы получили положительную апробацию на множестве научно-технических конференций.

Ознакомление с работой и другими научными трудами автора позволяет сделать однозначный вывод, что диссертация является единолично написанной научно-квалификационной работой.

V. Замечания, недостатки и рекомендации диссертационной работы

Отмечая высокий уровень диссертационной работы, следует указать на ряд вопросов и замечаний:

1. Диссертация носит сугубо теоретический характер, результаты практического внедрения предложенного способа управления ИБ в IoT-системах изложены достаточно кратко.
2. На наш взгляд, следовало уделить отдельное внимание анализу возможности реализации компьютерных атак, характерных для систем, использующих методы управления с обратной связью.
3. В диссертации, на наш взгляд, недостаточно внимания уделено сравнению предложенной методики с другими известными подходами к управлению ИБ в IoT-системах.
4. Недостаточно подробно описаны критерии выбора параметров для нечетких моделей и их влияние на результаты моделирования.
5. На наш взгляд, в работе недостаточно полно раскрыты вопросы нормализации данных, собираемых из множественных источников, для их последующей формализации.

Хотелось бы получить пояснения автора по следующим вопросам:

1. Какие существуют ограничения применимости предложенной методики в различных типах IoT-систем?
2. Какие дополнительные меры необходимо предпринять для обеспечения безопасности IoT-систем, помимо предложенной методики управления ИБ?

Следует отметить, что перечисленные недостатки и рекомендации принципиально не снижают научную значимость работы по причине того, что поставленная цель в полной мере достигнута.

К достоинствам диссертации необходимо отнести несомненную востребованность, оригинальность, математическую аккуратность, академический интерес. Выносимые положения понятны. Автореферат отражает основные положения диссертационной работы. Основные положения соответствуют содержанию.

VI. Вывод

Диссертация А.Г. Вовика представляет собой законченную научно-квалификационную работу, выполненную лично соискателем на высоком научном уровне. В диссертации предложен новый подход к управлению ИБ в IoT-системах, основанный на использовании обратной связи и нечеткой логики.

Основные результаты диссертационного исследования опубликованы в рецензируемых научных изданиях, в том числе 5 работ в журналах из перечня ВАК. Автореферат адекватно отражает содержание и выводы диссертации.

В диссертации решена задача повышения эффективности управления информационной безопасностью IoT-систем, имеющая существенное значение для развития методов и систем защиты информации.

Полагаем, что диссертационная работа А.Г. Вовика на тему «Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз» соответствует критериям, установленным в пп. 9-14 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 г. (с изменениями), а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

кандидат технических наук, доцент,
НПО Эшелон АО
Генеральный директор
Московский государственный технический
университет имени Н. Э. Баумана МГТУ
доцент [redacted] В.Л. Цирлов

Личную подпись кандидата технических наук, доцента Цирлова Валентина Леонидовича удостоверяю.
Начальник отдела кадров [redacted] И.С.Грибова

« 12 » мая 2025 года