ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора военных наук, профессора Лося Владимира Павловича
на диссертацию Вовика Андрея Геннадьевича
на тему «Методика управления информационной безопасностью IoT-системы с непрерывным замкнутым циклом нечеткой оценки угроз», представленную на соискание ученой степени кандидата технических наук
по специальности 2.3.6. — «Методы и системы защиты информации, информационная безопасность»

Актуальность темы исследования обусловлена бурным развитием технологий Интернета Вещей. Появляются новые и мутации ранее известных угроз информационной безопасности для IoT, а также возникают новые уязвимости в защищаемых системах. Все это приводит к динамичному изменению (повышению) рисков ИБ. Обеспечение требуемого уровня защиты информации в системах невозможно без непрерывного по времени и месту мониторинга состояния защищенности информации в защищаемой системе, что является нетривиальной задачей.

Содержание работы по главам. Диссертационная работа Вовика А.Г. состоит из введения, четырех глав, заключения, списка литературы и трёх приложений.

Во введении представлен анализ проблем управления ИБ, связанных с развитием технологий Интернета Вещей, и современного состояния решаемой научной задачи, обоснована актуальность темы исследования, сформулирована цель исследования, определён круг решаемых задач, обозначены общие подходы к достижению поставленной цели, а также приведены основные результаты, выносимые на защиту, показана их роль и сформулирована научная новизна.

В главе 1 выполнен анализ проблематики обеспечения информационной безопасности и управления информационной безопасностью в системах Интернета вещей. Обоснована необходимость формализации процессов управления информационной безопасностью в IoT-системах. Предложены критерии оценки эффективности «оперативность управления информационной безопасностью» и «точность управления информационной безопасностью».

В главе 2 проведен сравнительный анализ существующих способов, подходов и методов управления информационной безопасностью информационных систем, обоснована невозможность их использования для систем Интернета Вещей. Предложен Способ управления информационной безопасностью в системах IoT на основе учета обратной связи и обосновано повышение эффективности управления ИБ при использовании предложенного способа.

В главе 3 разработана комплексная модель управления ИБ IoT-системы, состоящая из разнородных моделей, объединенных между собой нечетким ядром для определения текущего уровня защищенности информации в системе. Обосновано повышение эффективности управления ИБ по критерию «оперативность управления» при использовании предложенных способа и модели управления ИБ.

В главе 4 разработана методика автоматизированного управления ИБ систем Интернета Вещей. Представлены алгоритм реализации методики и разработанное программное обеспечение, реализующее разработанный алгоритм. Разработаны рекомендации по применению методики, способствующие ее правильному использованию для повышения эффективности управления ИБ по введённым критериям.

Заключение и выводы по главам отражают результаты диссертационного исследования и дальнейшие перспективы исследований в данном направлении. Словарь терминов содержит основные понятия и определения, относящиеся к области обеспечения ИБ.

Список литературы включает 112 источников.

В трёх приложениях представлены: копии актов о внедрении и использовании результатов исследований и сведения о государственной регистрации программы для ЭВМ.

В целом диссертация написана хорошим литературным языком и достаточно полно проиллюстрирована.

Достоверность и новизна результатов. Достоверность полученных результатов исследования, научных положений, выносимых на защиту, подтверждается тем, что разработанная методика не противоречат основным задачам, национальным и международным стандартам в области управления ИБ. Корректность разработанной модели системы управления ИБ подтверждена практическим внедрением в повседневную деятельность организации.

Полученные результаты обладают научной новизной, которая заключается в:

1. В разработке 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.

3. В разработке методики автоматизированного управления ИБ IoT-систем и расширении класса способов оценки эффективности управления ИБ введением показателя защищенности информации, как соответствия возможностей СЗИ уровню актуальных угроз в системе.

Степень обоснованности научных положений, выводов и рекомендаций. сформулированных в диссертации. В диссертационной работе использовались Методы моделирования сложных систем: методы нечеткого моделирования, методы экспертных оценок, методы структуризации типа «дерево целей». Исследование основано на процессном и риско-ориентированном подходах.

Исследование также опиралось на российские ГОСТы и международные стандарты, материалы научно-практических конференций и публикаций в периодической печати, отечественные и международные методики управления ИБ, что доказывает высокую степень обоснованности полученных научных результатов.

Подтверждение опубликования основных результатов диссертации в научной печати. Основные результаты диссертационной работы были апробированы на 5-ти всероссийских, международных научных и научно-практических конференциях. Они с достаточной полнотой изложены в 10 научных работах, из них 4 публикации в изданиях, рекомендованных ВАК для опубликования основных научных результатов диссертаций на соискание учёной степени кандидата наук. Таким образом, можно заключить, что основные результаты и выводы диссертации строго обоснованы, являются новыми и получены автором самостоятельно.

Замечания по работе.

Следует отметить следующие недостатки в работе:

1. В диссертации недостаточно подробно описаны конкретные способы практической реализации предложенной методики.

2. В работе не полностью раскрыты вопросы масштабируемости предложенной методики. Необходимо более подробно рассмотреть, как методика может быть применена к большим и сложным IoT-системам с тысячами или миллионами устройств.

3. Необходимо более детально рассмотреть вопросы валидации и верификации предложенной модели и методики управления ИБ. Какие методы и подходы использовались для подтверждения корректности работы модели и соответствия результатов моделирования реальным процессам?

4. В диссертации не полностью учтены вопросы, связанные с организационно-правовыми методами защиты информации. Необходимо пояснить, как предложенная

методика может быть интегрирована с существующими нормативными требованиями и стандартами в области ИБ.

Отмеченные замечания не снижают научной ценности проведённого лично автором исследования и содержания основных положений, выносимых на защиту.

Соответствие содержания автореферата основным положениям диссертации.
Автореферат достаточно полно и адекватно отражает основные результаты диссертации.

Соответствие диссертации требованиям, предъявляемым к диссертациям на соискание учёной степени кандидата наук.

Считаю, что диссертация Вовика А.Г. является законченной научно-квалификационной работой, имеющей ярко выраженную научную и практическую значимость при решении задач управления ИБ в системах Интернета Вещей. Полученные результаты обладают актуальностью, научной новизной и практической ценностью. Тема диссертационной работы соответствует паспорту специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Содержание диссертации соответствует отрасли наук, по которой присуждается учёная степень, - «технические науки».

Заключение по работе. 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».

ОФИЦИАЛЬНЫЙ ОППОНЕНТ:

Лось Владимир Павлович
Федеральное государственное автономное образовательное учреждение высшего образования "Российский государственный гуманитарный университет", главный научный сотрудник кафедры «Информационная безопасность»,
Президент Ассоциации защиты информации, профессор, доктор военных наук.
20.01.03 - «Оперативное искусство в целом, по видам Вооружённых Сил, родам войск и специальным войскам», 20.02.12 - Военная кибернетика (в настоящее время - Системный анализ, исследование операций, моделирование боевых действий и систем военного назначения, компьютерные технологии в военном деле).
Тел. +7(903)740-32-61, email: los-vladimir@yandex.ru

[redacted] Лось В.П.

19.05.2025 г.

Сведения об организации:
Федеральное государственное автономное образовательное учреждение высшего образования "Российский государственный гуманитарный университет", 125047, Г.МОСКВА, ВН.ТЕР. Г. МУНИЦИПАЛЬНЫЙ ОКРУГ ТВЕРСКОЙ, ПЛ. МИУССКАЯ, Д. 6, СТР. 6, +7 (495) 250-61-18, rsuh@rsuh.ru.

Подпись Лося В.П. заверяю
Директор департамента
по управлению персоналом
и социальным вопро
А Лекс
19.05
[redacted]
Департамент по управлению персоналом социальным