«УТВЕРЖДАЮ»
Проректор по научной работе СПбГЭТУ
М.Ю. Шестопалов
2016 г.

ОТЗЫВ

официального оппонента
кандидата технических наук доцента
ВОРОБЬЕВА Евгения Германовича

на автореферат и диссертацию на соискание ученой степени кандидата технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность»

НОСАЛЬ Ирины Алексеевны на тему:

«Обоснование мероприятий информационной безопасности социально-важных объектов»

1. Актуальность выполненного исследования

Актуальность темы исследования обусловлена наличием противоречий между возможностями существующего научно-методического аппарата и потребностью в новых эффективных методах поиска и обоснования мероприятий по информационной безопасности (далее - ИБ). В условиях ограниченных ресурсов и повышенных требований к обеспечению ИБ наиболее остро этот вопрос стоит перед социально-важными объектами (далее - СВО), поскольку нарушение или прерывание работы СВО может привести к нарушению нормальной жизнедеятельности социально-незащищённых слоёв населения, возникновению общественных волнений, дестабилизации политической ситуации и в целом негативно отразиться на социально-экономической системе государства.

Одновременно, настоящее исследование и его результаты представляют интерес не только для специалистов в данной узкой области знаний. Предложенные методы и методы могут найти применение для усовершенствования существующих и проектирования новых информационных структур СВО, а также при разработке интеллектуальных систем управления ИБ.

Качество полученных оценок позволяет выбирать наилучшие варианты обеспечения ИБ, оценить и снизить затраты ресурсов, эффективно управлять системой обеспечения ИБ. Это дает основание утверждать, что научная задача, сформулированная в диссертации как «разработка новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов, повышающих уровень их ИБ», является актуальной.

2. Новизна исследования и полученных результатов, степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Полученные в ходе исследования результаты характеризуются следующей новизной:

1. Предложенный метод управления ИБ СВО на основе комплекса оптимизационных моделей развивает циклическую модель управления Шухарта-Деминга, являющуюся стандартом в области обеспечения ИБ. Управление предложено осуществлять на основе нового комплекса оптимизационных моделей, ориентированных на широкий круг возможных ситуаций.

2. Новизна предлагаемого метода обоснования мероприятий информационной безопасности по критерию минимума интегральных потерь состоит в новой совокупности условий, при которой предлагается обосновывать мероприятия ИБ и комбинации нескольких известных подходов к оценке рисков, ценности информационных ресурсов, на основе

построения моделей дезорганизующих процессов и поиска целесообразных мероприятий ИБ.

3. Каждая из предложенных моделей защищаемых и дезорганизующих процессов ИБ СВО имеет свой смысл, выявленный на основе обширного профессионального опыта, а их структуры отражают реальную ситуацию в моделируемой области. Новизна этих моделей состоит, прежде всего, в предмете моделирования.

4. Предложены новые правила тестирования систем поддержки принятия решений (СППР) для СОИБ СВО и методические рекомендации по использованию предложенных в исследовании методов и моделей при решении типовых задач обеспечения ИБ СВО.

Обоснованность представленных положений, выводов и рекомендаций обеспечивается корректным использованием выбранного математического аппарата, применением системного подхода к решению поставленных задач, и подтверждается рядом экспериментальных проверок, а также внедрением в практику работы научной и производственной организаций.

3. Значимость для науки и практики результатов диссертации, возможные конкретные пути их использования

Ценность положений и выводов диссертационной работы заключается в формализации деловых процессов СВО и типовых нарушений ИБ СВО и развитии научно-методического аппарата обоснования мероприятий ИБ СВО.

Обоснованное введение в предметную область традиционного для иных областей знаний математического инструментария из теории марковских процессов и корректное его использование для решения насущных задач обоснования мероприятий ИБ также усиливает научную составляющую настоящего исследования.

Практическая значимость этих результатов заключается в возможности повысить уровень ИБ СВО путем осуществления оперативного поиска

целесообразных мероприятий ИБ. Теоретическая база предложенных методов позволяет использовать их не только при защите информационных систем СВО, но и при обеспечении ИБ самого объекта. Большой интерес также вызывают предложенные оптимизационные модели поиска оптимального периода пересмотра мероприятий по защите, учитывающие различные условия, которыми может руководствоваться практикующий специалист.

4. Оценка содержания диссертации

Диссертация построена по традиционному принципу и состоит из введения, 4-х глав собственных исследований, которые включают анализ текущего уровня исследования в данной области, выводов по каждой главе, практических рекомендаций, заключения и списка литературы, включающего 151 отечественный и зарубежный источник. Работа иллюстрирована 18-ю таблицами и 13-ю рисунками.

По теме диссертации опубликовано 4 статьи в журналах, рекомендованных ВАК Минобрнауки России. Основные результаты диссертации изложены в материалах одной международной и двух российских конференций. Данные диссертации используются практической работе ОПФР по Республике Коми, что подтверждается актом внедрения.

Полученные автором результаты можно использовать при проектировании новых информационных инфраструктур не только СВО, но и других организаций, в том числе использующих для работы стандарты СТО БР и ГОСТ ИСО/МЭК 27001, а также в разработке интеллектуальных систем управления информационной безопасностью.

Метод управления ИБ СВО на основе комплекса оптимизационных моделей; метод обоснования мероприятий ИБ по критерию минимума интегральных потерь; модели защищаемых и дезорганизующих процессов ИБ СВО можно использовать в учебном процессе на старших курсах обучения студентов по специальности «090900 – Информационная

безопасность» по дисциплинам «Управление информационной безопасностью» и «Моделирование систем информационной безопасности».

Из недостатков работы можно отметить следующие:

- в параграфе 1.3 даются рекомендации в области оценки рисков и упоминается, что ущерб рассчитывается не по отношению к СВО, а по отношению к его клиентам, однако в дальнейшем в работе не дается каких-либо комментариев и рекомендаций по расчету этих показателей;

- недостаточное внимание уделено анализу существующих методов оценки уровня ИБ и обоснования мероприятий ИБ, основанных на использовании теории марковских процессов и их сравнении с предлагаемым методом;

- нет указаний на то, чем именно защищаемый «метод управления ИБ СВО на основе комплекса оптимизационных моделей» отличается от аналогичных методов, применяемых для управления ИБ СВО и организаций других типов;

- в параграфе 4.1, при сравнении результатов расчетов Примера 1 и Примера 2 делается заключение о важности роли первоначального распределения вероятностей состояний процесса, без приведения конкретной количественной оценки влияния этих параметров на точность расчетов в рамках предлагаемого метода.

Указанные замечания и недостатки носят частный характер и не снижают общей ценности диссертационной работы и значимости изложенных в ней научных результатов.

5. Заключение о соответствии

Таким образом, диссертационная работа Носаль Ирины Алексеевны на тему: «Обоснование мероприятий информационной безопасности социально-важных объектов», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», является

завершенной научной квалификационной работой, в которой содержится решение важной задачи разработки новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов.

По актуальности, научной новизне, практической значимости и достоверности полученных результатов диссертационная работа Посаль Ирины Алексеевны соответствует требованиям п. 9 «Положения о порядке присуждения учёных степеней», утверждённого постановлением Правительства РФ№ 842 от 24.09.2013 г., предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Заведующий кафедрой «Информационная безопасность»
Санкт-Петербургского государственного электротехнического
университета «ЛЭТИ» им. В.И. Ульянова (Ленина),

к.т.н., доцент Воробьев Евгений Германович

08.12.2016

Наши реквизиты: Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)" (СПбГЭТУ) Минобрнауки России, юр.адрес: ул. Проф. Попова, д.5, С.-Петербург, 197376, Тел.: (812) 346-44-87, [illegible]
58, E-mail: [illegible]