ОТЗЫВ
официального оппонента

ведущего научного сотрудника управления научных исследований и подготовки научных кадров ФГОБУ ВПО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», доктора технических наук профессора БУЙНЕВИЧА Михаила Викторовича на диссертационную работу НОСАЛЬ Ирины Алексеевны, выполненную на тему «Обоснование мероприятий информационной безопасности социально-важных объектов» и представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

На отзыв официального оппонента представлена диссертация объемом 159 страниц, иллюстрированная 13 рисунками и 18 таблицами и состоящая из введения, четырех разделов, заключения и списка использованных источников из 151 наименования, а также автореферат на 16 страницах.

1. Актуальность темы диссертационного исследования

Сегодня борьбой с угрозами безопасности информационным системам «всех мастей» занимаются тысячи специалистов в сотнях компаний и государственных организаций. Эти угрозы были и остаются одной из наиболее распространенных причин ущерба конфиденциальности, целостности и доступности информационных ресурсов. Несмотря на огромные усилия научного, технического и экспертного сообщества, убытки, приносимые инцидентами информационной безопасности, не падают и достигают огромных величин. Причем официальные оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

Такое положение обусловлено целым рядом причин, носящих проблемный характер. Среди подобных причин и «правовой вакуум» некоторых аспектов наряду с «галопирующей модернизацией» руководящих документов по защите информационных систем персональных данных, и несистемность вкупе с гигантским объемом пула «нормативки» по вопросам технической защиты информации, и проч. Одной из них, носящей комплексный характер, является примитивность и ограниченность научно-методического аппарата обеспечения ИБ объектов информатизации различного предназначения (может быть, за редким исключение, типа СТО БР ИББС – комплекса документов Банка России, описывающего единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учётом требований российского законодательства).

В этой связи работа Носаль И.А., посвященная научному обоснованию мероприятий информационной безопасности (ИБ) социально-важных объектов (СОВ) на базе математических моделей и методов, несомненно является актуальной.

2. Степень обоснованности научных положений, выводов и рекомендаций

Обоснованность представленных научных положений, выводов и рекомендаций определяется, прежде всего, логически стройной структурой исследования, согласно которой соискатель последовательно ставит и решает научные задачи по каноническрй схеме «анализ – синтез – оценка».

Анализ содержания работы позволяет судить о достаточно высокой степени обоснованности основных научных положений, выводов и практических рекомендаций, приведенных в диссертации.

Автором на защиту выносится четыре основных научных положения.

Первое – метод управления информационной безопасностью социально-важных объектов на основе комплекса оптимизационных моделей. Метод подразумевает разработку новой или использование готовой модели делового процесса, нуждающегося в обеспечении ИБ. Согласно методу управление ИБ предлагается осуществлять на основе нового комплекса оптимизационных моделей, ориентированных на типовые ситуации. Ищется целесообразный набор мероприятий защиты, при котором достигается экстремум целевой функции для сложившейся ситуации.

Второе – метод обоснования мероприятий информационной безопасности по критерию минимума интегральных потерь. Обоснование мероприятий ИБ, согласно предлагаемому методу, рекомендуется осуществлять, исходя из минимума общих потерь, среди которых ключевое место занимают потери из-за снижения ценности защищаемых информационных ресурсов в течении времени.

Третье – модели защищаемых и дезорганизующих процессов применительно к информационной безопасности социально-важных объектов. Разработанный комплекс марковских моделей формализует типовые для СВО деловые процессы и описывает типовые наборы действий нарушителей, компонуя которые можно формализовать большинство атак на ИБ СВО.

И четвертое – обоснованные рекомендации по повышению уровня информационной безопасности социально-важных объектов, которые содержат:

– методические рекомендации по использованию разработанных методов и моделей при решении типовых задач обеспечения ИБ СВО (порядок действий специалиста по ИБ, в случае, если он использует представленные методы и модели вручную);

– новые правила тестирования систем поддержки принятия решений для системы обеспечения ИБ СВО;

– архитектуру комплекса программных средств обоснования мероприятий ИБ СВО с учетом автоматизации разработанных методов и моделей;

– предложения по совершенствованию организации ИБ СВО, в части развития нормативно-правовой базы, оценки рисков, предотвращения типовых нарушений.

Основные рекомендации базируются на основе результатов анализа ИБ СВО и результатов расчетов с использованием предложенных методов и моделей с учетом новых полученных знаний. Разработка основных научных положений, выводов и рекомендаций основана на критическом анализе обширного библиографического списка.

3. Новизна исследования, достоверность основных научных результатов, практическая и научная значимость работы

Новизна работы определяется относительно новым объектом – основными деловыми процессами СВО и процессами нарушения ИБ, который автор исследует на предмет получения нового научно-методического аппарата обеспечения ИБ СВО.

Научная новизна работы заключается в разработке новых правил управления ИБ и нового комплекса оптимизационных моделей мероприятий ИБ, учитывающих ранее не принимаемые во внимание факторы обеспечения ИБ. Оригинальность разработанного метода обоснования мероприятий ИБ заключена, прежде всего, в новой совокупности формализованных условий при которых предлагается это обоснование. Метод ориентирован на широкий круг возможных ситуаций обеспечения ИБ, на учёт ценности защищаемых информационных ресурсов и потенциальной информированности злоумышленников на текущий момент времени; предусматривается возможность синтеза и оценки возможных программ деструктивных воздействий на информационные ресурсы с учетом их ценности. Новизна разработанных комплексов и самих моделей защищаемых и дезорганизующих процессов состоит, прежде всего, в предмете моделирования. С применением математического аппарата марковских процессов построены новые, ранее не рассматриваемые модели процессов, отражающих ИБ СВО. Каждая из этих моделей имеет свой смысл, выявленный на основе обширного профессионального опыта, а их структуры отражают реальную ситуацию в моделируемой области.

Достоверность полученных в работе основных научных результатов обеспечивается применением апробированных общенаучных и специальных методов исследования, опорой на современную научно-методическую базу, использованием в ходе исследования свыше полутора сотен литературных источников (включая монографии, статьи, материалы докладов, ресурсы Интернет) и подтверждается проведенными вычислительными экспериментами, положительной апробацией на научных (в том числе, международной) конференциях, а также публикациями результатов исследования в рецензируемых научных изданиях.

Теоретическая значимость работы определяется развитием научно-методического аппарата обоснования мероприятий ИБ СВО в части доказательства возможности количественного обоснования мероприятий ИБ в различных условиях, а также получения новых знаний о сущности защищаемых деловых и дезорганизующих процессов СВО.

Практическая значимость состоит в том, что предложенные методы и решения могут найти применение при разработке интеллектуальных систем управления ИБ, в том числе при проектировании новых информационных инфраструктур СВО и организаций. Использование заранее разработанных моделей позволяет значительно повысить скорость поиска целесообразных мероприятий ИБ и качество принятия решений.

4. Степень завершенности работы и качество ее оформления, замечания и недостатки

Представленная на отзыв рукопись характеризуется полнотой изложения поставленных вопросов и обладает внутренним единством. Название работы полностью соответствует ее содержанию, а полученные результаты – паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Работа хорошо структурирована и иллюстрирована, изложена хорошим научно-литературным языком, что способствует легкому восприятию.

Список работ, опубликованных соискателем по теме диссертации, является гарантией высокого качества проведенного исследования.

Автореферат в целом отражает содержание диссертационной работы, позволяет сделать аргументированный вывод о качестве проведенного исследования и полученных научных результатах.

По содержанию и оформлению оппонируемой работы можно высказать следующие замечания.

1) Автором постулируется повышение уровня ИБ СВО в результате применения предложенных моделей и методов обоснования мероприятий ИБ, но не указано в каких шкалах предполагается измерять повышение ее уровня.

2) В формуле (18) модели 6 (стр. 62 диссертации, стр. 9 автореферата) не ясно, что за переменная $P_{k_н}(\Delta t_k, T)$ и с какой целью она введена.

3) Имеет место отклонение от соблюдения ГОСТ 7.0.11-2011, в частности: в автореферате отсутствует структурный элемент «ЗАКЛЮЧЕНИЕ», а библиографические записи документов в списке литературы не оформлены в строгом соответствии с Приложением Б.

4) Присутствует небрежность отдельных формулировок (например: процессы нарушения vs дезорганизующие процессы) и ссылок (например, на несуществующую формулу 49 на стр. 102). На стр. 9 диссертации при определении ключевых понятий ИБ «Доступность» и «Целостность», неверно указаны библиографические ссылки, а именно: [1] ГОСТ Р 52143-2013 «Социальное обслуживание населения. Основные виды социальных услуг» вместо [2] ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». В автореферате отсутствует расшифровка сокращений ИЛС, НС, ПТК СПУ, ПТК НВП (стр. 11) и ЗИР (стр. 13).

Отмеченные недостатки и упущения не умаляют вышеприведенных достоинств диссертационной работы и не ставят под сомнение ценность полученных научных результатов.

5. Заключение

1) Диссертация Носаль И.А. на тему «Обоснование мероприятий информационной безопасности социально-важных объектов» написана автором самостоятельно, обладает внутренним единством и содержит новые научные результаты и положения, выдвигаемые для публичной защиты, что свидетельствует о личном вкладе автора диссертации в науку и соответствует критериям, изложенным в **п. 10 «Положения о присуждении ученых степеней»**.

В диссертации приводятся сведения о практическом использовании полученных автором диссертации научных результатов (в частности, при обеспечении информационной безопасности государственного учреждения – отделения Пенсионного Фонда РФ по Республике Коми), а также рекомендации по повышению уровня информационной безопасности социально-важных объектов.

2) В соответствии с **п. 11 «Положения...»** основные научные результаты диссертации Носаль И.А. опубликованы в следующих рецензируемых научных изданиях:

– Информационно-управляющие системы, № 2(63) за 2013 г. и № 1 за 2014 г.;

– Информация и безопасность, № 2 за 2011 г.;

– Труды СПИИРАН, вып. 2(39) за 2015 г.

3) В соответствии с **п. 12 «Положения…»** вышеприведенные рецензируемые издания на момент опубликования своих работ соискателем входили в «Перечень российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук».

4) Количество публикаций, в которых излагаются основные научные результаты диссертации Носаль И.А. на соискание ученой степени кандидата технических наук – 4, что соответствует требованиям **п. 13 «Положения…»**.

5) В соответствии с **п. 14 «Положения…»** в диссертации соискатель ученой степени ссылается на 151 источник, включая монографии, статьи, материалы докладов, ресурсы Интернет. В диссертации использована ссылка на 7 научных работ автора: из них 4 выполнены соискателем лично и 3 – в соавторстве, что отмечено в списке публикаций по теме диссертации

С учетом вышеизложенного можно заключить, что диссертация Носаль Ирины Алексеевны на тему «Обоснование мероприятий информационной безопасности социально-важных объектов», представленная на оппонирование и соискание ученой степени кандидата технических наук, является научно-квалификационной работой, в которой содержится решение актуальной

научно-технической задачи разработки новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов, имеющей значение для развития отрасли информационной безопасности и защиты информации (**п. 9 «Положения…** »), а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

ОФИЦИАЛЬНЫЙ ОППОНЕНТ
доктор технических наук, профессор