ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 02.07.2020 г. № 3

О присуждении Левоневскому Дмитрию Константиновичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 31 января 2020 г., протокол № 2 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года (с изменениями согласно приказам Минобрнауки России №105/нк от 11 апреля 2012 г. №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г., №301/нк от 23 ноября 2018 г.).

Соискатель Левоневский Дмитрий Константинович, 1991 года рождения, в 2014 году с отличием окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) по направлению «Информатика и вычислительная техника» (диплом № 107824 0710185). Справка о сдаче кандидатских экзаменов №17/207, выдана в 2017 г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии

наук. В настоящее время Левоневский Дмитрий Константинович работает научным сотрудником в лаборатории технологий больших данных социокиберфизических систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук Министерства науки и высшего образования Российской Федерации.

Диссертация выполнена в лаборатории технологий больших данных социокиберфизических систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук Министерства науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, профессор Осипов Василий Юрьевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук, главный научный сотрудник, руководитель лаборатории информационно-вычислительных систем и технологий программирования.

Официальные оппоненты:

ДУШКИН Александр Викторович, доктор технических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники», профессор кафедры информационной безопасности;

ДУБЕНЕЦКИЙ Владислав Алексеевич, кандидат технических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)», доцент кафедры информационных систем

дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

(СПбГУТ), г. Санкт-Петербург в своем положительном отзыве, подписанном Парамоновым Александром Ивановичем, доктором технических наук, профессором кафедры сетей связи и передачи данных и Маколкиной Мариной Александровной, кандидатом технических наук, доцентом кафедры сетей связи и передачи данных, и утвержденном Шестаковым Александром Викторовичем, доктором технических наук, старшим научным сотрудником, проректором СПбГУТ по научной работе, указала, что в целом диссертационная работа Д.К. Левоневского является законченной научно-квалификационной работой, выполненной на актуальную тему, отличается научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая задача моделирования и разработки моделей и методов защиты корпоративных информационных систем от комплексных деструктивных воздействий.

Соискателем предложен метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий, основанный на новой марковской модели анализируемого процесса и алгоритме расчета нового показателя позволяет производить сравнительную оценку и выбор различных мер, направленных на обеспечение защиты. Разработанный метод адаптивной защиты корпоративных информационных систем от комплексных деструктивных воздействий, ориентированный на новую архитектуру системы такой защиты с оптимизацией ее конфигурации позволяет повысить защищенность КИС. Причем эффективность данного метода обеспечивается оптимизацией конфигурации системы защиты путем автоматической адаптации под конкретные условия. Также предложенные способы и средства защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий позволяют повысить эффективность системы защиты и корпоративных информационных систем в целом. Полученные результаты рекомендуется применить в решении научно-исследовательских и опытно-конструкторских задач в таких организациях, как АО «НИИ «РУБИН», ООО «Код Безопасности», в учебных заведениях (ИТМО, СПбГЭТУ «ЛЭТИ») и учреждениях науки. Текст автореферата полностью соответствует содержанию

Диссертационная работа Левоневского Дмитрия Константиновича «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» соответствует пунктам 9, 10, 13 паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность и отвечает всем критериям пп. 9-14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842, а её автор – Левоневский Дмитрий Константинович – заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 35 опубликованных работ, в том числе по теме диссертации 26 работ, опубликованных в рецензируемых научных изданиях 15 работ, из них опубликованных в изданиях, рекомендуемых ВАК – 7, индексируемых в WoS/Scopus – 9, имеется 3 свидетельства о государственной регистрации программы для ЭВМ, 1 патент на изобретение.

Основные научные результаты опубликованы в 26 научных трудах общим объемом 24,4 п.л., из которых объем личного вклада соискателя составляет 6,5 п.л. Наиболее значимые работы по теме диссертации:

1. **Левоневский Д.К.,** Ватаманюк И.В, Малов Д.А. Обеспечение доступности сервисов корпоративного интеллектуального пространства посредством управления потоком входных данных // Программная инженерия. 2019. Т. 10. № 1. С. 20-29. *Личный вклад соискателя – 33%.*
2. **Левоневский Д.К.,** Ватаманюк И.В., Савельев А.И, Денисов А.В. Корпоративная информационная система обслуживания пользователей как компонент киберфизического интеллектуального пространства // Известия высших учебных заведений. Приборостроение. 2016. Т. 59. С. 906-912. *Личный вклад соискателя – 40%.*
3. **Левоневский Д.К.** Архитектура облачной системы распределения контента в киберфизических системах // Моделирование, оптимизация и информационные технологии. 2019. № 4 (27). С. 16-17.

4. Осипов В.Ю., Воробьев В.И., **Левоневский Д.К.** Проблемы защиты от ложной информации в компьютерных сетях // Труды СПИИРАН. 2017. № 53. С. 97-117. *Личный вклад соискателя – 40%.*
5. **Levonevskiy D.,** Vatamaniuk I., Saveliev A. Processing models for conflicting user requests in ubiquitous corporate smart spaces // MATEC Web of Conferences. 2019. V. 161, 3006. *Личный вклад соискателя – 33%.*
6. **Levonevskiy D.,** Fedorchenko L., Afanasieva I., Novikov F. Architecture of the software system for adaptive protection of network infrastructure // ACM International Conference Proceeding Series. 2018. V. 17. *Личный вклад соискателя – 25%.*

Оригинальность содержания диссертации составляет не менее 87% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 7 отзывов, все отзывы положительны:

1) ФГАОУ ВО ИТМО. Отзыв составил доцент факультета безопасности информационных технологий, д.т.н., доцент Гришенцев А.Ю. Замечания: в автореферате недостаточно раскрыта необходимость решения задачи разработки новых методов и моделей адаптивной защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий; схема на рис. 2 плохо читаема.

2) ФГАОУ ВО СПбГУАП. Отзыв составил доцент кафедры электромеханики и робототехники, к.т.н., доцент Солёный С.В. Замечания: в автореферате не указано, какие показатели эффективности функционирования объекта защиты использовались при математическом моделировании сервиса интерактивного корпоративного телевидения; в главе 4 говорится об управляющих стратегиях при обработке заявок, но не детализируется, какие именно стратегии рассматриваются.

3) ФГАОУ ВО НИЯУ МИФИ. Отзыв составил заведующий кафедрой компьютерных систем и технологий, д.т.н., профессор Иванов М.А. Замечания: в автореферате не указано, о каких конкретно деструктивных воздействиях идёт речь. Не определён термин «эффект», нет единообразия в его обозначении на стр. 7-10 автореферата. Схема алгоритма адаптивной защиты на стр. 10 оформлена с нарушением общепринятых правил.

4) ФГБОУ ВО РГПУ им. А. И. Герцена. Отзыв составил заведующий кафедрой информационных систем института информационных технологий и технологического образования, д.ф.-м.н., профессор Флегонтов А.В. Замечания: следовало дать более подробное описание существующих работ по теме исследования; на некоторых графиках не указаны единицы измерения.

5) ФГБОУ ВО ГУМРФ имени адмирала С.О. Макарова. Отзыв составил профессор кафедры комплексного обеспечения информационной безопасности, д.т.н., профессор Ныркov А.П. Замечания: из текста автореферата неясно, каковы начальные условия в модели, приведённой на рис. 1; не описано, каким образом определяются интенсивности переходов между состояниями;

6) ФГБВОУ ВО ВКА им. А. Ф. Можайского. Отзыв составили д.т.н., доцент, полковник, начальник 61 кафедры Бирюков Д.Н., к.т.н., майор, преподаватель 61 кафедры Данилов В.В., капитан, адъюнкт 61 кафедры Беляков М.И. Замечания: из автореферата остаётся неясным, как осуществляется переход между состояниями процесса функционирования КИС (нет признаков и правил); в автореферате не представлен набор правил адаптивной конфигурации системы защиты КИС; автор не указывает, какие именно величины он использует в качестве базовых для расчёта эффективности функционирования КИС; присутствуют незначительные погрешности в оформлении: наличие некорректной ссылки [65] на странице 9, очень мелкий шрифт на рисунке 2.

7) АО «НИИ «РУБИН». Отзыв составил старший научный сотрудник, д.т.н., профессор Бухарин В.В. Замечания: из содержания автореферата не совсем понятно, какой именно показатель эффективности защиты КИС предлагает автор; в автореферате указывается использование модуля анализа эффектов системы защиты, но не определено, какие именно эффекты анализируются; предложенный

метод адаптивной защиты КИС от деструктивных информационных воздействий ограничивается поиском оптимальной конфигурации системы и недостаточно учитывает возможные изменения их реализаций; в качестве апробации полученных результатов диссертации автор использует систему сервиса интерактивного корпоративного телевидения, которая не в полной мере отражает все особенности функционирования современных КИС.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., доцент Душкин А.В. является известным ученым в области защиты от киберугроз, в том числе в автоматизированных системах обработки информации и управления и в автоматизированных системах управления критически важными объектами; к.т.н., доцент Дубенецкий В.А. – известный специалист в области корпоративных информационно-управляющих систем; ведущая организация, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ), является известной как в России, так и за рубежом организацией в области разработки и создания систем защиты информации и сетей связи, кроме того, широко известны достижения ее специалистов в области проектирования защищённых информационных систем.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны оригинальные способы и средства, отличающиеся новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность корпоративных информационных систем;

предложены:

новая математическая модель корпоративной информационной системы, функционирующей в условиях комплексных деструктивных информационных воздействий, отличающаяся новым пространством состояний и множеством переходов между ними, что позволяет шире исследовать и точнее прогнозировать поведение системы при наличии этих угроз;

метод оценивания эффективности функционирования корпоративной информационной системы с использованием предложенной математической модели, отличающийся новым показателем эффективности КИС и правилами его расчета, позволяющий расширить возможности оценивания влияния информационных угроз на работу систем;

метод адаптивной защиты корпоративной информационной системы от информационных угроз, отличающийся новой математической формулировкой задачи поиска оптимальной программы защиты и алгоритмом ее решения, позволяющий адаптировать эту защиту от комплексных деструктивных воздействий;

архитектура системы адаптивной защиты КИС от комплексных деструктивных информационных воздействий, которая отличается новой совокупностью связанных блоков сбора, предобработки и анализа данных и выбора контрмер для защиты от сетевых атак и иных деструктивных воздействий, позволяющая расширить функциональные возможности такой защиты;

доказана перспективность использования разработанных методов высокоуровневой формализации процессов функционирования корпоративных информационных систем на производственных предприятиях, в социальных учреждениях и других подобных объектах и обеспечения их адаптивной защиты;

введены:

набор состояний, характеризующий условия, в которых функционирует защищаемая система в заданный момент времени;

новый показатель эффективности функционирования корпоративной информационной системы в условиях информационных угроз;

набор частных показателей качества обслуживания, позволяющих оценивать выполнение сценариев многомодального взаимодействия пользователей с обеспечивающими устройствами киберфизического пространства.

Теоретическая значимость исследования обоснована тем, что:

сформулированные в работе теоретические утверждения **доказаны** с использованием моделирования и экспериментов. Эти утверждения составляют

основу обеспечения адаптивной защиты корпоративных информационных систем от комплексных деструктивных воздействий;

применительно к проблематике диссертации результативно использованы методы системного и математического анализа, положения теории вероятности и математической статистики, теории информационной безопасности;

изложены методологические и методические основы использования математического аппарата марковских процессов для разработки модели функционирования корпоративной информационной системы в условиях угроз;

раскрыты

существенные для обеспечения информационной безопасности особенности процесса взаимодействия пользователей и корпоративных информационных систем;

известные угрозы доступности, целостности и конфиденциальности в корпоративных информационных системах;

проблемные аспекты применения имеющихся методов и систем защиты в корпоративных информационных системах;

изучены существующие методы и системы защиты корпоративных информационных систем от рассмотренных угроз, основанные на сборе, предобработке и анализе информационных сигналов различного типа;

проведена модернизация существующих подходов к адаптивной защите корпоративных информационных систем, основанная на использовании новых функциональных блоков и правил сбора, предобработки и анализа данных и выбора контрмер для защиты от сетевых атак и иных деструктивных воздействий, позволяющая расширить функциональные возможности защиты.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены следующие результаты диссертационной работы:

• математическая модель корпоративной информационной системы, функционирующей в условиях комплексных деструктивных информационных воздействий;

• метод оценивания эффективности функционирования корпоративной информационной системы с использованием предложенной модели

использованы в составной части опытно-конструкторской работы «Разработка устройства сопряжения инфракрасного анализатора с локальной сетью предприятия» в ООО «ЭКАН»;

• метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий;

• метод адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий

использованы при проведении исследований в проекте “Разработка методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них” в рамках соглашения с Минобрнауки России № 05.607.21.0322 в СПИИРАН; внедрены в образовательный процесс факультета БИТ Университета ИТМО по направлениям подготовки бакалавриата 10.03.01, магистратуры 10.04.01 в виде использования материалов исследования для подготовки лекционных и практических занятий по дисциплинам «Основы информационной безопасности», «Теория и методы управления корпоративной информационной безопасностью», «Комплексное обеспечение функциональной безопасности»;

определены возможности и перспективы практического использования полученных результатов диссертации при исследовании конкретных технологий обеспечения информационной безопасности корпоративных информационных систем;

создана обобщённая архитектура адаптивной защиты корпоративной информационной системы от деструктивных воздействий;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные модель, методы и технические решения.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ достоверность полученных результатов подтверждена проведением всестороннего анализа работ по исследуемой проблеме, корректным применением научно-методического аппарата в виде использованных методов и теорий, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях, положительными итогами практической реализации результатов работы;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области обеспечения информационной безопасности корпоративных информационных систем;

использованы полученные характеристики для сравнения с данными, полученными с помощью известных подходов к защите корпоративных информационных систем;

установлено качественное и количественное соответствие результатов решения задачи разработки новых методов и моделей адаптивной защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий, определена область преимущества предложенного подхода перед результатами, полученными другими авторами;

использованы современные методики сбора и обработки исходной информации, представительные выборочные совокупности с обоснованием выбора объектов наблюдения и измерения.

Личный вклад соискателя состоит в:

- анализе процесса обеспечения информационной безопасности корпоративных интеллектуальных систем от информационных угроз;
- постановке задачи разработки новых методов и моделей адаптивной защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий;

- построении математической модели корпоративной информационной системы как объекта защиты в условиях информационных угроз;
- разработке метода оценивания эффективности функционирования корпоративной информационной системы в условиях воздействия информационных угроз;
- разработке метода адаптивной защиты корпоративной информационной системы от информационных угроз;
- разработке архитектуры программной системы адаптивной защиты корпоративной информационной системы от информационных угроз;
- создании решений для защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий;
- разработке обоснованных рекомендаций по повышению эффективности защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий;
- подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что в соответствии с требованиями п. 9 «Положения о присуждении ученых степеней», предъявляемыми к кандидатским диссертациям, и пп. 3, 6, 7, 8, 9, 10 и 14 паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, Левоневский Д.К. в своей диссертационной работе решил научную задачу разработки новых методов и моделей адаптивной защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий, имеющую важное значение для развития теории и практики обеспечения информационной безопасности корпоративных информационных систем.

На заседании 02.07.2020 г. диссертационный совет принял решение присудить Левоневскому Д.К. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 20 человек, из них 4 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 20, против нет, недействительных бюллетеней нет.

Председатель диссертацион
доктор технических наук,
член-корреспо Юсупов Рафаэль Мидхатович

Ученый секре
кандидат техн Зайцева Александра Алексеевна
02.07.2020 г.