ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.073.02, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ «ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ИНФОРМАТИКА И УПРАВЛЕНИЕ» РОССИЙСКОЙ АКАДЕМИИ НАУК», ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ ДОКТОРА НАУК

аттестационное дело № _____

решение диссертационного совета от «03» марта 2021 г. протокол № 1

О присуждении МИЛОСЛАВСКОЙ НАТАЛЬЕ ГЕОРГИЕВНЕ, гражданке Российской Федерации, ученой степени доктора технических наук.

Диссертация «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях» по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность, в виде рукописи принята к защите 19.11.2020, протокол № 5 диссертационным советом Д 002.073.02, созданным на базе Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) (119333, г. Москва, ул. Вавилова, д. 44, корп. 2; приказ Министерства образования и науки РФ от 24.06.2016 №771/нк).

Соискатель Милославская Наталья Георгиевна, 1962 года рождения, диссертацию на соискание ученой степени кандидата технических наук по теме «Инструментальные средства расчета сложных линейных систем по частям тензорным методом» защитила в 1989 году в диссертационном совете, созданном на базе Московского ордена Трудового Красного Знамени инженерно-физического института (МИФИ). С 2001 года имеет ученое звание доцента. В настоящее время работает в Федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ) в должности доцента отделения интеллектуальных кибернетических систем офиса образовательных программ.

Диссертация выполнена в отделе №63 «Методы и программные средства накопления и обработки данных» отделения №6 ФИЦ ИУ РАН.

Научный консультант – доктор технических наук, Будзко Владимир Игоревич, академик Академии криптографии РФ, заместитель директора по научной работе Института проблем информатики ФИЦ ИУ РАН.

Официальные оппоненты:

1. Стрельцов Анатолий Александрович, гражданин Российской Федерации, доктор технических наук, доктор юридических наук, профессор, ведущий научный сотрудник Центра проблем информационной безопасности МГУ имени М.В.Ломоносова;
2. Лось Владимир Павлович, гражданин Российской Федерации, доктор военных наук, профессор, директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования "МИРЭА – Российский технологический университет" (РТУ МИРЭА);
3. Сычев Артем Михайлович, гражданин Российской Федерации, доктор технических наук, доцент, первый заместитель директора Департамента информационной безопасности Центрального банка Российской Федерации,

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого" (ФГАОУ ВО "СПбПУ") в своем положительном заключении, подписанном В.В. Сергеевым, доктором технических наук, профессором, проректором по научной работе, указала, что диссертация Милославской Натальи Георгиевны является законченной научно-квалификационной работой, в которой решена крупная научно-техническая проблема развития теоретических и методических основ создания центров интеллектуального управления сетевой безопасностью информационно-телекоммуникационных сетей, внедрение которых позволяет повысить эффективность обеспечения информационной безопасности критической информационной инфраструктуры Российской Федерации; диссертационная работа полностью соответствует требованиям к диссертациям на соискание ученой степени доктора технических наук, установленным Положением о порядке присуждения ученых степеней, а ее автор, Н.Г. Милославская, заслуживает присуждения ей ученой степени доктора технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Соискатель имеет 292 опубликованных работы, в том числе по теме диссертации – 58, из них в рецензируемых научных изданиях – 16. Общий объем публикаций по теме диссертации – 567.43 п.л.; вклад автора в них является определяющим. Сведения, представленные соискателем об опубликованных работах, в которых изложены основные научные результаты диссертации, являются достоверными. В них

достаточно полно изложены материалы исследования.

Наиболее значимые работы по теме диссертации:

1. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. – М., Горячая Линия-Телеком, 2021. – 431 с.

2. Miloslavskaya, N. Security Zone Infrastructure for Network Security Intelligence Centers // In: Samsonovich A., Klimov V. (eds) Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019 // Procedia Computer Science. – 2020. – Pp. 51-56.

3. Miloslavskaya, N. Stream Data Analytics for Network Attacks' Prediction // In: Samsonovich A., Klimov V. (eds) Postproceedings of BICA 2019 // Procedia Computer Science. – 2020. – Pp. 57-62.

4. Miloslavskaya, N. Network Security Intelligence Center as a combination of SIC and NOC // Postproceedings of BICA 2018 // Procedia Computer Science. – 2018. – Vol. 145. – Pp. 354-358.

5. Милославская, Н.Г. Вопросы практического применения технологий блокчейна/ Н.Г.Милославская, В.И.Будзко // Безопасность информационных технологий. – 2018. – Том 26, № 1. – С. 36-45.

6. Miloslavskaya, N. Designing Blockchain-based SIEM 3.0 System // Information and Computer Security. – Emerald Publishing (UK), 2018. – Vol. 26 (N 4). – Pp. 491-512.

7. Miloslavskaya, N. Information Security Management in SOCs and SICs // Journal of Intelligent & Fussy Systems. – IOS Press (Netherlands), 2018. – Vol. 35, № 3. – Pp. 2637-2647.

8. Милославская, Н.Г. Визуализация процессов управления информационной безопасностью / Н.Г.Милославская, А.И.Толстой // Научная визуализация. – 2017. – Том 9, № 5. – С. 117-136.

9. Милославская, Н.Г. Центры управления информационной безопасностью // Безопасность информационных технологий. – 2016. – Том 23, № 4. – С. 38-51.

10. Милославская, Н.Г. Компетентностные требования стандартов ISO/IEC к профессионалам в области информационной безопасности / Н.Г.Милославская, А.И.Толстой // Безопасность информационных технологий. – 2017. – Том 24, № 4. – С. 6-18.

11. Miloslavskaya, N. Application of Big Data, Fast Data and Data Lake Concepts to Information Security Issues / N.Miloslavskaya, A.Tolstoy // Proceedings the 3rd International Symposium on Big Data Research and Innovation. – 2016. – Pp. 148-153.

12. Милославская Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие. Вопросы управления информационной безопасностью. Книга 3 / Н.Г.Милославская, А.И.Толстой, М.Ю.Сенаторов. – 2-е изд. испр. – М., Горячая Линия-Телеком. – 2016. – 170 с.

13. Милославская, Н.Г. Понятие устойчивости организации инфраструктуры финансового рынка в условиях угроз кибербезопасности / Н.Г.Милославская, С.А.Толстая // Безопасность информационных технологий. – 2015. – Том 22. № 4. – С. 75-85.

14. Милославская, Н.Г. Information Security Intelligence – основа современного управления информационной безопасностью / Н.Г.Милославская, А.И.Толстой // Безопасность информационных технологий. – 2013. – Том 20, № 4. – С. 88-96.

15. Securing Information and Communication Systems: Principles, Technologies, and Applications // Chapter 8: Network Security / S.Katsikas, N.Miloslavskaya. – Artech House, 2008. – Pp. 139-170.

16. Информационная безопасность открытых систем: учебник (гриф Министерства образования РФ). В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В.Запечников, Н.Г.Милославская, А.И.Толстой, Д.В.Ушаков. – М., Горячая Линия-Телеком, 2006. – 536 с.

На автореферат дали положительные, не содержащие критических замечаний, отзывы:

1. И.В. Аникин, д.т.н., профессор, заведующий кафедрой систем информационной безопасности Федерального государственного бюджетного образовательного учреждения (ФГБОУ) высшего образования (ВО) «Казанский национальный исследовательский технический университет им. А.Н.Туполева»;
2. Т.В. Борботько, гражданин Белоруссии, д.т.н., профессор, заведующий кафедрой защиты информации Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»;
3. Н.А. Егорова, д.т.н., доцент кафедры «Информационная безопасность систем и технологий» ФГБОУ ВО «Пензенский государственный университет»;
4. А.С. Марков, д.т.н., с.н.с., президент АО «Научно-производственное объединение «Эшелон» (г. Москва);
5. Л.К. Бабенко, д.т.н., профессор кафедры «Безопасность информационных технологий» Южного федерального университета;
6. А.А. Шелупанов, д.т.н., профессор, директор Института системной интеграции и безопасности, президента ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники»;
7. А.Г. Якунин, д.т.н., профессор, заведующий кафедрой «Информатика, вычислительная техника и информационная безопасность» ФГБОУ ВО «Алтайский государственный технический университет имени И.И. Ползунова»;
8. А.А. Хорев, д.т.н., профессор, заведующий кафедрой «Информационная безопасность» Федерального государственного автономного образовательного учреждения (ФГАОУ) ВО «Национальный исследовательский университет «Московский институт электронной техники»;
9. С.М. Рацеев, д.ф.-м.н., профессор кафедры информационной безопасности и теории управления ФГБОУ ВО «Ульяновский государственный университет»;
10. В.И. Васильев, д.т.н., профессор, профессор кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет»;
11. А.Г. Остапенко, д.т.н., профессор, заведующий кафедрой систем информационной безопасности ФГБОУ ВО «Воронежский государственный технический университет»;
12. И.А. Калмыков, д.т.н., профессор, профессор кафедры информационной безопасности автоматизированных систем ФГАОУ ВО «Северо-Кавказский федеральный университет»;
13. А.Ю. Щербаков, д.т.н., профессор, академик РАЕН, начальник Центра развития криптовалют и цифровых финансовых активов Федерального государственного бюджетного учреждения науки «Всероссийский институт научной и техни-

ческой информации Российской Академии наук».

Выбор официальных оппонентов обосновывается их высокой квалификацией, наличием научных трудов, соответствующих теме оппонируемой диссертации, и следующими обстоятельствами:

– А.А. Стрельцов является крупным специалистом в области правовых аспектов информационной безопасности (ИБ) и построения систем управления; заслуженный деятель науки РФ; член-корреспондент Академии криптографии РФ;

– В.П. Лось является известным специалистом в области ИБ, включая вопросы подготовки специалистов, разработки архитектур управления ИБ и процессов управления инцидентами ИБ; Президент Ассоциации защиты информации;

– А.М. Сычев ведет активную деятельность в области обеспечения ИБ банковской системы; защитил степень к.т.н. по тематике средств обеспечения сетевой безопасности – межсетевых экранов; Лауреат профессиональной премии в области информационной безопасности «Серебряный кинжал».

Выбор ведущей организации обосновывается тем, что ФГАОУ ВО "СПбПУ" является крупным научным центром и активно занимается проблематикой по теме диссертационной работы Н.Г. Милославской, что подтверждается приоритетными направлениями работ и публикациями сотрудников.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– впервые **проведен** широкий комплекс исследований, позволивший определить базовые эффективные решения построения Центров интеллектуального управления сетевой безопасностью (ЦИУСБ) в составе систем обеспечения информационной безопасности (СОИБ) информационно-телекоммуникационных сетей (ИТКС) объектов критической информационной инфраструктуры (КИИ);

– **осуществлена** теоретическая разработка методологии упреждающего управления сетевой безопасностью ИТКС на основе ЦИУСБ с применением интеллектуальных подходов, включая принципы, процессы, функциональные постановки задач, технические, технологические и иные решения;

– **разработана** оригинальная систематизация понятий информационной защищенности ИТКС и **создана** терминологическая база для определения среды

функционирования ЦИУСБ с конкретизацией требований по обеспечению его ИБ;

– **обоснована** необходимость создания в составе ядра ЦИУСБ SIEM-системы третьего поколения (3.0) с применением технологий блокчейна средства блокирования попыток компрометации накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС, для которого **сформулирована** задача «свертки» блокчейна;

– достоверность и результативность проведенных научных исследований **подтверждена** практическими внедрениями их результатов.

Теоретическая значимость исследования обоснована тем, что:

– на основе проведенного научного анализа продемонстрирована эволюция технологий и средств обеспечения сетевой безопасности и обоснована необходимость построения ЦИУСБ, а также **разработаны** методология и принципы построения типового ЦИУСБ организации как объединения Центра интеллектуальной безопасности (ЦИБ) и Сетевого операционного центра (СОЦ), что вносит значительный теоретический вклад в обеспечение сетевой безопасности ИТКС КИИ при интенсификации использования информационно-коммуникационных технологий;

– **разработана** методика и проведена систематизация сложноорганизованных базовых понятий ИБ, что вносит существенный вклад в развитие теории ИБ;

– **разработаны** обобщенная модель процессов функционирования ЦИУСБ для реагирования в режиме реального времени на инциденты ИБ в ИТКС, расширенная табличным описанием метода составления карт процессов, что позволило **формализовать** взаимосвязанные процессы управления инцидентами ИБ (ПУИИБ) ИТКС, типовые архитектуры хранения больших данных, относящихся к ИБ ИТКС, и их многопотоковой обработки из гетерогенных источников;

– **продемонстрирована** преемственность полученных результатов по отношению к известным и их значимость для эволюции средств обеспечения ИБ.

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

– **разработана и описана** методология как упорядоченная пошаговая «инструкция» построения ЦИУСБ и реализации в нем ПУИИБ на объектах КИИ;

– **определены и детализированы** средства обеспечения ИБ инфраструктуры ЦИУСБ с указанием их расположения в зонах безопасности ЦИУСБ и виды

информации об ИБ ИТКС, подлежащей визуализации для управления сетевой безопасностью в целом по ИТКС и по отдельным событиям ИБ;

– **разработана** терминологическая база, позволяющая давать точное описание составных элементов и свойств ЦИУСБ, включая понятия информационной защищенности и функциональной устойчивости ЦИУСБ в штатном режиме и в условиях угроз ИБ;

– **разработаны** готовые к использованию базовый набор показателей системы оценки уровня функциональной устойчивости и основные мероприятия процесса управления функциональной устойчивостью ЦИУСБ, реестр рисков ИБ ИТКС, типовая структура частной Политики ИБ ЦИУСБ, вербальные описания типовых признаков удаленных сетевых атак на ИТКС для разработки индикаторов атак, а также определена подлежащая сбору постоянная и временная информация, необходимая для расследовании инцидентов ИБ в ИТКС;

– **определена** штатная структура ЦИУСБ с функциональными обязанностями конкретных участков и квалификационными требованиями исполнителей;

– результаты диссертации **использованы** при разработке уникальной в России и мире образовательной программы подготовки магистров под названием «Обеспечение непрерывности и информационной безопасности бизнеса» в рамках направления подготовки 10.04.01 «Информационная безопасность»;

– практическая значимость результатов исследования **подтверждена** шестью актами о внедрении.

Оценка достоверности результатов исследования выявила, что:

– исследование **основывалось** как на фундаментальных общенаучных (формальная логика, сравнение и обобщение, анализ и синтез, научная абстракция), так и специальных методах научного познания явлений и процессов (системный, структурный и функциональный анализы, экспертные методы, моделирование), а также на анализе и обобщении накопленного опыта при соблюдении принципов преемственности с предшествующими работами;

– при проведении исследований **использовались** российские и международные стандарты, а полученные результаты **согласуются** с основными положениями теории систем, теории управления и теории ИБ и **подтверждены** формаль-

ными выводами основных утверждений, сформулированных в работе;

– вывод о целесообразности объединения центров интеллектуальной безопасности и сетевых операционных центров в единый ЦИУСБ **основывался** на результатах анализа практики их функционирования и целесообразности совместного использования единых инструментальных средств при сокращении суммарного объема организационного обеспечения, а построение ЦИУСБ выполнено с использованием проверенных на практике подходов, включая многопотоковый метод сбора данных от источников и интеллектуальные методы их анализа;

– установлено, что направленность исследований находится в русле международных исследований в области совершенствования средств обеспечения СБ;

– достоверность и реализуемость результатов исследования **подтверждены** широкой апробацией в открытой печати и на международных и национальных научных конференциях, а также практикой их внедрения в крупных организациях и образовательных учреждениях России.

Основные результаты, представленные в диссертационной работе, получены соискателем лично. В опубликованных совместных работах постановка и исследование задач осуществлялись совместными усилиями соавторов при непосредственном участии соискателя.

На заседании 03 марта 2021 года диссертационный совет принял решение присудить Милославской Наталье Георгиевна ученую степень доктора технических наук.

При проведении тайного голосования диссертационный совет в количестве 22 человек, из них 6 докторов наук по профилю защищаемой диссертации, участвовавших в заседании, из 32 человек, входящих в состав совета, проголосовали: за 22, против 0, недействительных бюллетеней 0.

Председатель
диссертационного совета Д 002.073.02
академик И.А. Соколов

Ученый секретарь
диссертационного совета Д 002.073.02
к.ф.-м.н. Р.В. Разумчик

«03» марта 2021 г.