ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
доктора технических наук, доктора юридических наук, профессора
Стрельцова Анатолия Александровича
на диссертацию Милославской Натальи Георгиевны
на тему: «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях», представленную на соискание
учёной степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы. Актуальность изучения закономерностей развития систем обеспечения информационной безопасности информационно-коммуникационных систем и сетей во многом обусловлена особенностями современного этапа развития общества, которое переживает этап «цифровой трансформации». Перед обществом стоит проблема не просто противодействовать угрозам критической информационной безопасности и, в частности, защищенности информации и устойчивости функционирования сетей телекоммуникаций и связи. Необходимо найти достойный ответ на серьезный вызов способности общества преодолевать «проклятие размерности» при решении проблемы обеспечения безопасности их использования и устойчивого функционирования как средств автоматизации информационной деятельности человека, общества и государства.

С одной стороны, критическая информационная инфраструктура (КИИ) теперь включает информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, которые де-факто стала необходимым условием жизнедеятельности всех субъектов общественной жизни. Уровень развития КИИ и используемых в ней ИКТ оказывает существенное влияние на реализацию конституционных прав и свобод человека и гражданина, на экономическую и социальную конкурентоспособность общества, на политическую культуру, на обороноспособность страны и безопасность государства.

С другой стороны, серьезным препятствием для и дальнейшего расширения использования ИКТ и повышения эффективности применения объектов КИИ в интересах общественного развития становится их уязвимость по отношению к злонамеренному внедрению вредоносного программного обеспечения и данных.

Серьезность вызова, с которым столкнулось общество в области использования ИКТ и функционирования КИИ, подтверждается продолжающимся, несмотря на принимаемые политические, правовые и иные меры как у нас в стране, так и за рубежом, ростом количества и увеличением опасности компьютерных преступлений. Злонамеренное и враждебное использование ИКТ против объектов КИИ для достижения военно-политических целей становится фактором провоцирования роста международной напряженности. Более того, фактически сложилась ситуация, в которой апробированные сред-

ства противодействия угрозам международной безопасности не демонстрируют прежнюю эффективность.

В этих условиях одним из перспективных направлений решения проблемы представляется развитие системы нормативного технического регулирования отношений в этой области создания систем управления безопасностью КИИ и, в частности, регулирования отношений, связанных с построением центров интеллектуального управления сетевой безопасностью (ЦИУСБ) для информационно-телекоммуникационных сетей (ИТКС) субъектов КИИ.

С этой точки зрения актуальность диссертационного исследования Н.Г. Милославской, посвященной разработке методологии и принципов построения специализированного структурного элемента ИТКС – типового ЦИУСБ в составе системы обеспечения информационной безопасности (СОИБ) ИТКС, трудно переоценить, т.к. эти методология и принципы закладывают научную основу подготовки соответствующих документов нормативного технического регулирования в области создания Центров управления сетевой безопасностью ИТКС.

Краткое содержание работы. Работа состоит из введения, 6 глав основного материала, заключения и приложений.

Во введении обоснована актуальность диссертационного исследования, определены его цель и задачи, а также выделены научная новизна и теоретическая и практическая значимость.

В первой главе проведен анализ текущего состояния обеспечения ИБ современных ИТКС, а также сформулирована общая постановка проблемы формирования научных основ обеспечения информационной защищенности и функциональной устойчивости ИТКС на основе создания центра управления сетевой безопасностью.

Вторая глава описывает разработанные автором основы теории классификации и систематизации (таксономии) основных элементов описания взаимодействия ИТКС со средой ее функционирования, характеризуемого, с одной стороны, уязвимостями составляющих сети, а с другой – угрозами нарушения безопасности функционирования и устойчивости функционирования, проявляющимися в виде сетевых атак и порождающих инциденты ИБ в ИТКС.

Третья глава посвящена исследованию процессов обеспечения информационной и сетевой безопасности ИТКС и разработке подходок к формализации процесса управления инцидентами ИБ, включая описание их и реагирование на такие инциденты.

В четвертой главе проведен анализ существующих походов к организации управления сетевой безопасностью ИТКС на основе использования систем сбора, архивирования, агрегирования и поиска корреляции данных в системных журналах мониторинга функционирования объектов сети. С учетом проведенного анализа разработан подход к созданию нормативной модели функционирования Центра интеллектуального управления сетевой безопасностью ИТКС.

Пятая глава содержит основные положения по описанию облика типового Центра интеллектуального управления сетевой безопасность ИТКС, включая вопросы целепола-

гания и структурирования управления сетевой безопасностью, визуализации используемой для управления информации и ее анализа, моделирования процесса обеспечения информационной безопасности, построения и оценки уровня функциональной устойчивости процесса управления, взаимодействия с ГосСОПКА.

Шестая глава содержит описания внедрений полученных диссертантом результатов в различных организациях – субъектах КИИ: в Ситуационном центре Газпромбанка; в Банке России; в компании Qualys, являющейся поставщиком облачных решений для обеспечения информационной безопасности; в Институте кибернетических интеллектуальных систем Национального исследовательского ядерного университета МИФИ; в компании «ЛИНС-М», являющееся системным интегратором в области информационной безопасности. Представлена также информация о внедрении результатов исследования в системе высшего образования по группе специальностей «Информационная безопасность».

В заключении обобщены теоретические и практические результаты работы, а также намечены возможные направления продолжения исследования.

В приложениях приводятся шесть актов о внедрении и использовании результатов диссертационной работы.

Достоверность и новизна результатов диссертации. *Научная новизна* результатов и положений диссертации, полученных лично автором, заключается в том, что автором получены научные результатов, совокупность которых может рассматриваться как методология построения специализированного структурного элемента ИТКС – типового Центра интеллектуального управления информационной безопасностью в составе системы обеспечения информационной безопасности ИТКС, основанная на рациональном выборе конкретных методов, принципов, способов и средств построения типового Центра, и на научно обоснованных технических, технологических и организационных решениях, внедрение которых вносит значительный вклад в развитие страны и научной области обеспечения сетевой безопасности.

Достоверность теоретических и прикладных результатов работы обеспечивается корректностью систематизации частных научных задач, решаемых в рамках научной проблемы, а также постановок и обоснованием условий решения частных научных задач, доказательствами формулируемых в работе утверждений, а также апробацией результатов при практическом внедрении полученных результатов по обеспечению сетевой безопасности ИТКС ряда организаций – субъектов КИИ.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации. Исследование опиралось как общенаучные и специальные методы познания и базировалось на общей методологии построения систем, общей теории систем, теории открытых систем, теории управления, теории связи, передачи, обработки и хранения информации, теории информационно-телекоммуникационных систем и сетей, теории ИБ, ИТ больших данных, блокчейна, а также российских ГОСТах и международных стандартах, апробацией научных результатов в печати и на научных конференциях. Результаты исследования подтверждены корректными выводами основных утверждений, сформулированных в работе, использованием известных проверенных на практике методов и лучших практик, соответствием предложенных усовершенствований общим архи-

тектурным принципам построения ИТКС, а также результатами их практического внедрения.

Ценность для науки и практики результатов работы. В диссертации сформулированы ***выносимые на защиту*** положения, создающие научную основу для развития системы нормативного технического регулирования отношений в области обеспечения информационной безопасности ИТКС и, в частности, следующие:

1) научно обоснованная методология и принципы построения типового ЦИУСБ, выбора его функциональной и организационной архитектуры, включая обеспечение его собственной ИБ;

2) основы теории классификации и систематизации (таксономии) основных элементов описания взаимодействия ИТКС со средой ее функционирования, включая базовые смысловые понятия ИБ (а именно – «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»), которая может быть использована для описания функционирования ИТКС субъекта КИИ при разработке документационного обеспечения ИБ и определения уровня ИБ ИТКС;

3) формализованное описание взаимосвязанных процессов управления инцидентами ИБ в ЦИУСБ с применением расширенного метода составления карт процессов;

4) бизнес-логика функционирования типового ЦИУСБ, расширенная обратной связью процессов управления сетевой безопасностью ИТКС, включая оперативное изменение конфигурационных настроек СЗИ в среде функционирования ИТКС и взаимодействие с источниками информации о тенденциях в области сетевой безопасности;

5) метод блокирования попыток компрометации массива накапливаемых данных об инцидентах ИБ в ИТКС в составе ядра SIEM-системы для типового ЦИУСБ;

6) расширенная временная шкала появления технологий и средств обеспечения сетевой безопасности, демонстрирующая эволюцию существующих и позволяющая фиксировать появление новых технологий и средств;

7) терминологический словарь (глоссарий) обеспечения сетевой безопасности, отвечающий существующей нормативной и правовой базам и расширяющий терминологию действующего ГОСТ Р ИСО/МЭК 27033-1-2011.

Теоретическая значимость работы состоит в том, что сформулированные в ней положения развивают теорию обеспечения ИБ современных ИТКС, создавая основу для использования потенциала нормативного технического регулирования отношений в области создания Центров интеллектуального управления информационной безопасностью, синтеза рационального технического и организационного обеспечения этих Центров.

Разработанные ***научные результаты использованы*** при разработке СОИБ для Банка России (акт головного исполнителя работ – российской компании «ЕС-лизинг»), создании решений для ЦИУСБ организаций в регионах Восточной Европы, Кавказа и Центральной Азии (акт компании Qualys), модернизации Ситуационного центра Службы ИБ Газпромбанка и реализации типового ЦИУСБ в НИЯУ МИФИ, в практике деятельности ООО «ЛИНС-М» при разработке средств ИБ для Банка России и стандарта обеспечения ИБ для Банка ВТБ, а также при разработке и внедрении нормативных правовых и учебно-методических документов в Федеральном Учебно-методическом объединении в

системе высшего образования по укрупненной группе специальностей направления подготовки «Информационная безопасность», что подтверждается соответствующими актами реализации результатов диссертации.

Подтверждение опубликования основных результатов диссертации в научной печати. Полученные в диссертации новые научные результаты опубликованы в 56 научных и учебно-методических работах автора, в числе которых 21 статья в ведущих рецензируемых научных изданиях, рекомендуемых ВАК России для публикации основных результатов диссертаций на соискание учёной степени доктора наук, таких как «Безопасность информационных технологий» и «Системы высокой доступности», и 11 учебников и учебно-методических пособий с грифами Министерства образования и науки РФ, УМО по образованию в области ИБ и УМО «Ядерная физика и технологии», неоднократно докладывались и получили одобрение на конференциях международного, всероссийского и регионального уровней, а также на научных семинарах в Национальном исследовательском ядерном университете «МИФИ». 28 публикаций по теме диссертации проиндексированы в Scopus и WebofScience. В начале 2021 г. также увидят свет еще два труда – учебное пособие с грифом Федерального УМО по УГСиНП «Информационная безопасность» и единолично написанная монография по теме диссертации. Индекс Хирша Милославской Н.Г. – 4 (WoS), 7 (Scopus).

Соответствие содержания автореферата основным положениям диссертации. Автореферат полностью соответствует диссертации и раскрывает направление исследований, актуальность и содержание разрабатываемой *проблемы формировании научных основ обеспечения информационной защищенности и функциональной устойчивости ИТКС, образуемых совокупностью методологию и принципы построения специализированного структурного элемента ИТКС ОРГАНИЗАЦИИ – Центра интеллектуального управления сетевой безопасностью, призванного осуществлять на основе обработки больших данных упреждающее управление сетевой безопасностью ИТКС на всех стадиях жизненного цикла ее информационных ресурсов за счет прогнозирования развития событий в области ИБ ИТКС*, важность результатов и практические возможности их использования.

Тема диссертации *соответствует* специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Содержание диссертации *соответствует* отрасли «технические науки».

Замечания по работе. В качестве *замечаний* можно отметить следующие:

- предложенная методология не доведена до уровня проекта нормативного документа технического регулирования вопросов обеспечения сетевой безопасности ИТКС на основе создания специализированного Центра интеллектуального управления;

- не приведены результаты применения предложенного диссертантом типового решения на объектах внедрения, подтверждающий повышение защищенности информационных ресурсов ИТКС.

Указанные замечания несколько снижают ценность отдельных положений диссертационного исследования, но не являются определяющими при оценке ее научно-квалификационного уровня в целом.

Заключение по работе:

Диссертационная работа Милославской Натальи Георгиевны представляет собой законченную научно-квалификационную работу, в которой на основе выполненных автором исследований *разработаны научно обоснованные теоретические положения по обеспечению сетевой безопасности ИТКС субъектов КИИ, совокупность которых можно квалифицировать как новое крупное научное достижение*, оформлена согласно ГОСТ Р 7.0.11-2011 и, таким образом, полностью удовлетворяет требованиям пп. 11, 13, 14, 18 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 (ред. от 01.10.2018, с изм. от 26.05.2020), к диссертациям на соискание учёной степени доктора наук, а её автор – Милославская Наталья Георгиевна – заслуживает присуждения ей учёной степени доктора технических наук.

ОФИЦИАЛЬНЫЙ ОППОНЕНТ –

Стрельцов Анатолий Александрович
МГУ имени М.В.Ломоносова,
Заведующий отделом Института проблем информационной безопасности,
член-корреспондент Академии криптографии РФ, заслуженный деятель науки Российской Федерации, профессор,
доктор технических наук, 05.13.19 – Методы и системы защиты информации, информационная безопасность,
доктор юридических наук, 20.02.12 – Военная кибернетика, системный анализ, исследование операций, моделирование боевых действий и систем военного назначения
Тел.: +7-910-4414001, email: aa.streltsov@yandex.ru

_____Стрельцов Анатолий Александрович

« 29 » декабря 2020 г.

М.П.

Подпись Стрельцова Анатолия Александровича удостоверяю.

Ученый секретарь Ученого совета Института проблем информационной безопасности МГУ имени М.В.Ломоносова Шаряпов Ринат Абдулберович

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова» (МГУ имени М.В.Ломоносова), 119991, Российская Федерация, Москва, Ленинские горы, д. 1,
Тел.: +7 (495) 939-10-00, адрес электронной почты: info@rector.msu.ru