МИНОБРНАУКИ РОССИИ
федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский политехнический
университет Петра Великого»
(ФГАОУ ВО «СПбПУ»)

ИНН 7804040077, ОГРН 1027802505279,
ОКПО 02068574

Политехническая ул., 29, Санкт-Петербург, 195251
тел.: +7(812)297 2095, факс: +7(812)552 6080
office@spbstu.ru

**«УТВЕРЖДАЮ»**

Проректор по научной работе

ФГАОУ ВО «СПбПУ»,

д.т.н., профессор

_____ Сергеев В.В.

«___» _____ 2020 г.

# О Т З Ы В

ведущей организации на диссертационную работу **Милославской Натальи Георгиевны** **«Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях»,**

представленную на соискание ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

**1. Актуальность темы выполненной работы.**

В условиях возрастающей сложности ИТКС, транзитивной связи между всеми участниками информационных взаимодействий, широкой направленности и разнообразия компьютерных атак важнейшую роль играет создание комплексной системы обеспечения сетевой безопасности ИТКС, включая ее непрерывное функционирование. В настоящее время возможности современных центров мониторинга безопасности традиционно ограничены именно процессом мониторинга инцидентов информационной безопасности (ИБ), а не полноценного упреждающего управления ими, т.е. обеспечения защищенности. Для разрешения этого противоречия в работе предпринята попытка формирования научной методологии определения функциональной структуры и организации Центра управления ИБ, который представил бы интеллектуальную систему.

**2. Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации.**

В диссертационной работе предложена научно обоснованная методология и принципы построения типового центра интеллектуального управления сетевой безопасностью (ЦИУСБ), его функциональной и организационной архитектуры, включая обеспечение

собственной ИБ ЦИУСБ. Отличительной особенностью такого подхода, определяющей перечень рассматриваемых научных проблем, является следующее:

1. Центр управления безопасности рассматривается как методологически (функционально, коммуникационно, логически) взаимосвязанная конвергентная структура, объединяющая мониторинг событий безопасности, подсистему принятия решений о допустимом риске, блок реагирования на инциденты, адаптивное управление которой реализует непрерывное обеспечение требуемого уровня безопасности.
2. Достижение поставленной цели базируется на высокой степени интеллектуализации в части обработки данных о событиях безопасности, применении проактивных методов реагирования и «сквозного» проектирования единой системы управления, что и составляет основную часть работы.

Различные компоненты такого подхода рассматривались в ряде работ (например, проактивная защита, выявление трендов и т.д.), однако, несомненным достоинством и новизной является интеграция проблем формирования требований, формирования структуры с учетом динамического управления задачами обеспечения требуемой безопасности в условиях непрерывного потока угроз.

Особенно следует отметить, что при построении целевой функции разрабатываемого центра, предлагается отказаться от традиционных нормативных и плохо контролируемых оценок (класс, уровни защищенности) а перейти к обобщенной оценке в виде функциональной устойчивости, т.е. непрерывности процесса сохранения работоспособности при сохранении потока внешних атак.

Такой подход соответствует передовым тенденциям и обеспечивает опережающую тактику защиты, ориентированную на предупреждение атак на ранней стадии, что полностью соответствует Госпрограмме «Сопка».

При формировании методологии построения ЦУСБ автор намеренно отказывается от рассмотрения конкретных методов и средств мониторинга обнаружения угроз, систем SIEM и т.д., а сосредотачивает усилия на рассмотрении общесистемных вопросов обеспечения полноты контроля состояния, достоверности принимаемых решений и обоснованности требований к системам интеллектуализации управления.

Такая неожиданная позиция автора (на первый взгляд, дающая основания упрекнуть в отсутствии связи с практикой) может быть оценена как достоинство подхода, заключающегося в учете основного требования – разрабатываемая методология должна быть инвариантна к используемым средствам мониторинга, констатирует полноту постав-

ленных требований, а их комплексность должна компенсировать отдельные недостатки частного инструментария и методов обработки.

Доказательством применимости такого подхода является достаточный перечень примеров практических рекомендаций, сформулированных при применении данного подхода в числе которых Банк России, Служба ИБ Газпрома, и ряд других, что подтверждается соответствующими актами.

Таким образом, основная научная проблема, решаемая в диссертационном исследовании, может быть сформулирована следующим образом:

В работе предложена методология создания центров управления сетевой безопасностью (ЦУСБ), обеспечивающих сохранение функциональной устойчивости на основе адаптивного опережающего управления сетевой безопасностью с использованием интеллектуальных подходов к обработке больших данных при управлении инцидентами ИБ.

Методология определяет функциональный состав ЦУСБ, требований к используемым методам, включая модули процессов управления, обеспечивающих реконфигурацию настроек средств защиты и создание непрерывного процесса поддержания функциональной устойчивости ИТКС в условиях динамических изменений внешней среды. Следует отметить решение ряда частных научных задач, среди которых важнейшими являются:

- разработка таксономии понятий, определяющих систематизацию сущностей, базовые понятия определения уровня защищенности на основе оценки функциональной устойчивости, описания ИТКС, в том числе с использованием понятия модели зрелости, впервые примененном при оценке ИБ.

- разработка состава и систематизация процесса функционирования ЦУСБ, его бизнес-логики и организация обратной связи процесса управления.

- методика блокирования попыток компрометации попыток массива накопленных данных инцидентов с использованием аналогий методов блокчейн в качестве ядра типовой SIEM системы.

Совокупность методологических положений, функциональных требований, принципов построения ЦУСБ, направленных на реализацию перспективных подходов обеспечения защищенности как задач опережающего управления структурой и параметрами ИТКС для поддержания непрерывной функциональной устойчивости в условиях непрерывного потока киберугроз может быть оценена как решение важной задачи совершенствования методов обеспечения информационной безопасности, имеющей значение для народного хозяйства.

**3. Обоснованность и достоверность заключительных выводов и рекомендаций, сформулированных в диссертации.**

Достоверность выводов и рекомендации, представленной работы состоят в корректном применении методов искусственного интеллекта (поведенческий, корреляционный, структурный анализ, технологии Big Data) при формировании методологии создания ЦУСБ, современных технологий теорий управления, а также соответствуют известным положениям теории обеспечения ИБ и обширному фактическому материалу. Результаты практического применения положений методологии в практике управления ИБ в ряде предприятий и организаций, что подтверждено документально.

**4. Значимость для науки и практики полученных результатов.**

Совокупность перечисленных результатов и теоретических положений, сформулированных в ходе проведения научного исследования, можно квалифицировать как значительное научное достижение в области обоснованности требований к системам обеспечения сетевой безопасности, что развивает теоретические положения кибербезопасности сетевых систем. В работе решена крупная научно-техническая проблема, имеющая большое народно-хозяйственное значение и заключающаяся в научно обоснованном выборе конкретных методов, принципов, способов и средств построения ЦИУСБ для достижения требуемого уровня информационной защищенности ИТКС.

Научную значимость прежде всего составляют принципы методологии построения типового ЦИУСБ с применением интеллектуальных подходов (включая корреляционный, контекстный, поведенческий и структурный анализ методов), обработки относящихся к ИБ больших данных для упреждающего управления сетевой безопасностью ИТКС, структуризация понятий информационной защищенности ИТКС, концепция поддержания функциональной устойчивости на основе адаптивной реконфигурации структуры сети.

Результаты диссертационной работы использованы при разработке системы обеспечения ИБ (СОИБ) для Банка России (акт головного исполнителя работ – российской компании «ЕС-лизинг»), при создании решений для ЦИУСБ организаций в регионах Восточной Европы, Кавказа и Центральной Азии (акт головного исполнителя работ – компании Qualys), при модернизации Ситуационного центра Службы ИБ Газпромбанка, при реализации типового ЦИУСБ в НИЯУ МИФИ.

**5. Конкретные рекомендации по использованию результатов и выводов диссертационной работы.**

Результаты и выводы диссертации могут быть использованы в организациях (предприятиях, учреждениях), связанных с обеспечением безопасности важных объектов и ре-

сурсов, и в научно-исследовательских учреждениях, ведущих исследования в области обеспечения безопасности информационных систем, в частности, в следующих организациях:

- на предприятиях и в организациях высокотехнологичных отраслей промышленности: в Госкорпорации «Росатом», АО «Российские космические системы», СНПО «Элерон», ЗАО «Голлард», банковских структурах;
- в высших учебных заведениях Министерства науки и высшего образования РФ, ведущих исследования по проблемам информационной безопасности: МГУ им. М.В.Ломоносова, СПбПУ Петра Великого, МИЭМ им. А.Н.Тихонова, ВГТУ, ЮФУ.

**6. Полнота опубликования основных положений и результатов диссертации.**

Основные результаты работы с достаточной степенью полноты опубликованы в научной печати. Автором единолично и в соавторстве опубликовано 56 печатных работ по теме диссертации, в том числе: в трех монографиях, восьми пособий, 16 научных статей в журналах из Перечня ВАК РФ, пять статей в иностранных журналах, 24 полнотекстовых доклада на 11 международных конференциях, 28 публикаций проиндексированы в Scopus и WebofScience.

**7. Соответствие диссертации специальности и отрасли наук, по которым она представлена к защите.**

Тема диссертационной работы соответствует паспорту специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность – и отрасли наук (технические), по которым представлена к защите в части пп. 3 (Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.), 4 (Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.), 6 (Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.), 14 (Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.), 15 (Модели и методы управления информационной безопасностью.) паспорта специальности.

**8. Замечания по работе.**

1. Работа существенно выиграла бы, если бы в гл. 5 для типовой структуры ЦУСБ был приведен пример функционального состава и технических характеристик модулей ЦУСБ конкретной ИТКС.

2. Существенным отличием и значимым результатом является использование в качестве цели управления функциональной устойчивости. Однако, в работе не приведены в явном виде определения и структура показателей оценки этого понятия применительно к решаемой задаче.

3. Предлагаемый подход направлен на развитие существующих систем на основе опережающего управления (стр. 256 работы и ТС 5), однако, не полностью раскрыты методы экстраполяции, набор прогнозируемых параметров и оценка периода экстраполяции. Неясно осуществляется ли это в режиме экстраполяции или требует настройки ИТКС.

4. На стр. 215 работы используется характеристика «эффективность управления ИБ», однако, не раскрыты его определение и методы оценки.

5. Каково назначение используемой модели зрелости (стр. 252) и существуют ли метрики оценки этого свойства?

6. В работе не рассмотрена возможность связи управления безопасностью с используемыми методами и технологиями обнаружения и идентификации сетевых атак. Решающими здесь являются время обнаружения и динамика реконфигурации и допустимая потеря функциональности. Как это учитывается в требованиях при выборе и согласовании подсистемы?

**9. Общая оценка работы.**

Указанные замечания не приуменьшают научной ценности проведённого лично автором исследования и существа основных положений, выносимых на защиту. В целом диссертация является законченной научно-квалификационной работой, имеющей несомненную научную и практическую значимость в решении задач обоснованности формирования требований к системам обеспечения и управления сетевой безопасностью. Полученные результаты обладают актуальностью, научной новизной и практической ценностью. Работа оформлена в соответствии с требованиями «Положения о порядке присуждения учёных степеней» к диссертациям на соискание учёной степени доктора наук. Автореферат диссертации полно и достоверно передаёт её основное содержание.

**Заключение по работе.**

Таким образом, диссертационная работа оформлена в соответствии с ГОСТ Р 7.0.11-2011 и удовлетворяет требованиям пп. 11, 13, 14 и 18 «Положения о присуждении ученых степеней» от 24 сентября 2013 г. № 842, в части требований, предъявля-

емых к диссертациям на соискание ученой степени доктора технических наук, а её автор – Милославская Наталья Георгиевна – заслуживает присуждения ей ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв обсуждён на заседании Ученого совета Института кибербезопасности и защиты информации СПбПУ. Протокол №04-20 от «25» декабря 2020 г.

Профессор Института кибербезопасности и защиты информации СПбПУ,
профессор, доктор технических наук, 05.13.19 – Методы и системы защиты информации, информационная безопасность
195251, г. Санкт-Петербург, Политехническая ул., д. 29, ауд. 173
Тел. +7 (812) 552-76-32, электронная почта: kafedra@ibks.spbstu.ru

Зегжда Петр Дмитриевич

«28» декабря 2020 г.

Сведения о ведущей организации:
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (СПбПУ), 195251, г. Санкт-Петербург, Политехническая ул., д. 29, office@spbstu.ru, 8 (812) 552-60-80