ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, доцента

Сычева Артема Михайловича

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. Диссертационная работа Милославской Натальи Георгиевны направлена на разработку научно-методического базиса, а именно методологии и принципов построения специализированного центра, обеспечивающего информационную защищенность передаваемых по информационно-телекоммуникационных сетям (ИТКС) субъектов критической информационной инфрастуктуры (КИИ) РФ на всех стадиях жизненного цикла ИТКС в условиях угроз информационной безопасности (ИБ) в едином информационном пространстве (ЕИП) субъета КИИ и при возникновении отказов в работе, требующих реструктуризации системотехнической составляющей ИТКС, за счет создания в ее составе типового Центра интеллектуального управления сетевой безопасностью (ЦИУСБ), являющего основой системы обеспечения ИБ (СОИБ) ИТКС. Общая направленность темы диссертации определяется актуальностью выбранной проблематики и задач исследования, ее объекта и предмета.

Достоверность и новизна результатов диссертации.

Достоверность теоретических и прикладных результатов работы обеспечивается строгим следованием общенаучным методам и основным положениям и системе понятий российских ГОСТов и международных

стандартов, корректностью и формально-логическими доказательствами формулируемых утверждений и рекомендаций и условий их применимости, показом получаемых конкурентных преимуществ по сравнению с существующими в настоящее время решениями, критическим анализом представленного в открытых источниках фактического материала, а также успешным внедрением полученных результатов в крупных отечественных и зарубежных корпорациях и организациях.

В диссертации на основе применения системного анализа и синтеза и современных интеллектуальных подходов при решении поставленной научной проблемы получены *новые выносимые на защиту результаты*:

- научно обоснованная методология и принципы построения типового ЦИУСБ, его функциональной и организационной архитектуры, включая обеспечение собственной ИБ ЦИУСБ, разработанные на основе выявления недостатков существующих центров;
- таксономия, обеспечивающая систематизацию и классификацию сущностей, базовых понятий ИБ, таких как «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», позволяющая регламентировать процесс определения уровня информационной защищенности ИТКС, описания функциональной деятельности ОРГАНИЗАЦИИ, требующей обеспечения информационной защищенности ИТКС, и для разработки документационного обеспечения ее ИБ на всех стадиях жизненного цикла ИТКС;
- детальное и формализованное описание основных взаимосвязанных процессов управления инцидентами ИБ, требующих первоочередной реализации в ЦИУСБ ОРГАНИЗАЦИИ, с применением расширенного метода составления карт процессов, который позволяет оптимизировать существующие процессы путем отслеживания избыточных действий и выявления рисков их успешной реализации;
- бизнес-логика функционирования типового ЦИУСБ, расширенная функциональными группами модулей, отвечающими за обратную связь процессов управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ, включая

оперативное изменение конфигурационных настроек СЗИ в динамически изменяющейся среде функционирования ИТКС и взаимодействие с источниками информации о тенденциях в области сетевой безопасности (Threat Intelligence);

- защищенное по своему дизайну на основе технологий блокчейна средство блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ в составе рекомендуемой в качестве ядра типового ЦИУСБ SIEM-системы 3.0, предназначенное для обеспечения целостности этого массива;
- уточненная и существенно расширенная по сравнению с используемой временная шкала появления технологий и средств обеспечения сетевой безопасности, что позволяет наглядно отслеживать эволюцию существующих и своевременно фиксировать появление новых технологий и средств;
- глоссарий предметной области обеспечения сетевой безопасности на основе типового ЦИУСБ, отвечающий существующей нормативной и правовой базам и включающий 205 терминов и расширяющий терминологию действующего ГОСТ Р ИСО/МЭК 27033-1-2011.

Научная новизна результатов и положений диссертации, полученных лично автором, заключается в научно и методологически обоснованном выборе методов, принципов, способов и средств построения типового ЦИУСБ в составе ИТКС, его функциональной и организационной архитектуры, а также программно-аппаратных и кадровых решений, внедрение которых вносит значительный вклад в повышение информационной защищенности и операционной надежности субъектов КИИ РФ в условиях угроз ИБ для развития страны и научной области обеспечения сетевой безопасности.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации. Диссертант провела большую работу по исследованию, анализу и творческому осмыслению фундаментальных и прикладных научно-методических работ по проблематике

диссертации и использовала большое число трудов отечественных и зарубежных авторов, нормативные и правовые документы. Это позволило сделать автору научно-обоснованные выводы и осуществить разработку практически значимых рекомендаций. Обоснованность полученных результатов также доказывается структурой и логикой их изложения. Сформулированные в диссертации выводы и рекомендации, представленные на защиту основные научные результаты полностью соответствуют поставленной цели.

Ценность для науки и практики результатов работы.

Ценность работы для науки заключается в методологии и принципах построения типового ЦИУСБ, разработанных для упреждающего управления сетевой безопасностью ИТКС на основе интеллектуальных подходов к обработке больших относящихся к ИБ данных (корреляционного, контекстного, поведенческого и структурного анализа), систематизации и классификации основных понятий ИБ ИТКС в виде единой таксономии, формализации и наглядном представлении взаимосвязанных процессов управления инцидентами ИБ для ИТКС. Перечисленные результаты являются необходимыми исходными данными для проведения НИОКР по созданию ЦИУСБ в конкретной организации – субъекте КИИ, использующем ИТКС.

Разработанные научные результаты использованы в Банке России (акт головного исполнителя работ – российской компании «ЕС-лизинг»), компании Qualys в регионах Восточной Европы, Кавказа и Центральной Азии, Ситуационном центре Службы ИБ Газпромбанка, НИЯУ МИФИ, ООО «ЛИНС-М» и Федеральном Учебно-методическом объединении в системе высшего образования по укрупненной группе специальностей направления подготовки «Информационная безопасность», что подтверждается соответствующими актами о внедрении/использовании.

Подтверждение опубликования основных результатов диссертации в научной печати. Полученные в диссертации новые научные результаты *опубликованы* в 56 научных работах автора, учтенных в тексте диссертации, и

еще 2 работах, вышедших после ее передачи в Диссертационный совет, в числе которых 21 статья в рецензируемых научных изданиях, рекомендуемых ВАК России, и журналах, индексируемые в базах SCOPUS и WebofSciemce, неоднократно докладывались и получили одобрение на конференциях международного, всероссийского и регионального уровней, а также представлялись на научных семинарах в Национальном исследовательском ядерном университете «МИФИ». В конце автореферата добавлены еще две важных публикации, вышедших из печати после его сдачи в Диссертационный совет, а именно, монография и учебное пособие с грифом для направления подготовки «Информационная безопасность» по теме диссертации.

Соответствие содержания автореферата основным положениям диссертации. Текст диссертации представлен на 461 странице машинописного текста; включая введение, шесть глав, в каждой из которых решена своя задача исследования, заключение с основными результатами работы, список литературы из 307 источников, глоссарий из 205 терминов и шесть приложений, соотвествующих шести внедрениям результатов работы. Материалы диссертации хорошо проиллюстрированы 20 таблицами и 57 рисунками. Автореферат полностью отражает основное содержание диссертации и соответствует ей, раскрывая направление исследований, актуальность и содержание разрабатываемой *научной проблемы*, состоящей в формировании научной основы обеспечения информационной защищенности и функциональной устойчивости сложных систем класса ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ.

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

Замечания по работе. По работе можно отметить следующие *замечания*:

- практическая значимость полученных результатов исследования

подтверждена несколькими актами о внедрении, но при их описании не в полной мере отражена специфика для финансовой индустрии;

- замечание терминологического характера, вызванное еще не в полной мере устоявшимся понятийным аппаратом – поскольку в финансовой отрасле России общепринят перевод англоязычного словосочетания «operational resilience» как «операционная надежность», можно было бы рекомендовать автору пользоваться именно им, но она в самом начале предпочла термин «функциональная устойчивость», что может быть принято, поскольку в Национальной программе «Цифровая экономика Российской Федерации» используется именно он (наряду с «устойчивостью функционирования»).

При этом выделенные замечания не ставят под сомнение высокий научно-квалификационный уровень диссертационной работы.

Заключение по работе:

Диссертационная работа Милославской Натальи Георгиевны представляет собой законченную научно-квалификационную работу, в которой на основе выполненных автором исследований *разработаны методология и принципы построения специализированного структурного элемента ИТКС – типового ЦИУСБ в составе СОИБ ИТКС для упреждающего управления сетевой безопасностью при передаче данных в ИТКС на всех стадиях ее жизненного цикла за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных, что можно квалифицировать как новое крупное научное достижение*, 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:

Сычев Артем Михайлович
Банк России, первый зам. директора Департамента информационной безопасности, доктор технических наук, 05.13.19 – методы и системы защиты информации, информационная безопасность,
доцент,
Тел. +7(495)987-71-20, email: sichev@mail.ru

_____Сычев Артем Михайлович

«19» _____01___2021 г.

Подпись Сычева Артема Михайловича удостоверяю.

Центральный банк Российской Федерации (Банк России)
Департамент кадровой политики
ВЕРНО
ведущий эксперт
Департамента кадровой политики
_____ А.В. Кузнецов

Сведения об организации:

Центральный Банк Российской федерации (Банк России)
107016, г. Москва, ул. Неглинная, д. 12
8 (800) 300-30-00, media@cbr.ru