МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники»

ОТЗЫВ

на автореферат диссертации Милославской Натальи Георгиевны «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях», представленной на соискание ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Корпоративные информационно-телекоммуникационные сети (ИТКС) становятся сегодня важнейшим инструментом управления бизнесом. Но при повышенном внимании к обеспечению безопасности информационных ресурсов ИТКС и развитии нормативной и правовой базы, повышающей требования к защите информации в них, продолжается существенный рост ущерба, причиняемого владельцам и пользователям информации, о чем свидетельствует мировая статистика.

В целях управления средствами защиты информации (СЗИ) в ИТКС и мониторинга их состояния в режиме реального времени создаются центры управления сетевой безопасности (ЦУСБ).

Учитывая масштаб и сложность современных ИТКС, а также с учетом возрастания реальных угроз сетевой безопасности, научная проблема, заключающаяся в разработке методологии и принципов построения ЦУСБ ИТКС, осуществляющих управление безопасностью ИТКС с учетом прогнозирования развития событий в области ИБ, решаемая в рамках диссертационного исследования, является несомненно актуальной.

В основу исследования положены общая методология построения систем, общая теория систем, теория открытых систем, теория управления, теория связи, передачи, обработки и хранения информации, теория информационно-телекоммуникационных систем и сетей, теория ИБ, а также ИТ больших данных и блокчейна.

В рамках решения научной проблемы автором получены следующие научные результаты:

1. 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.

2. 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.

3. 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.

4. 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*).

5. 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.

6. 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.

7. 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.

При проведении исследований использовались как общенаучные методы познания (анализ и синтез, сравнение и обобщение, научная абстракция, формальная логика), так и на специальные методы научного познания явлений и процессов: системный, структурный и функциональный анализы, графические, экспертные методы, моделирование и т.д.

Результаты исследования подтверждены формальными выводами основных утверждений, сформулированных в работе, использованием известных проверенных на

практике методов и лучших практик соответствием предложенных усовершенствований общим архитектурным принципам построения систем вычислительных сетей и СОИБ.

Результаты исследований достаточно полно апробированы в научных изданиях и на научных конференциях. Внедрение результатов исследования подтверждается шестью актами о внедрении/использовании, что свидетельствует об их практической значимости.

К достоинствам работы можно отнести исследование различных стратегий и тактик управления информационными ресурсами ИТКС, четкое формулирование текущих задач исследования, строго обоснованную логическую последовательность проведения исследования, а также адекватную оценку соответствия поставленных задач и полученных результатов.

В качестве недостатков можно отметить следующие:

из автореферата не ясно, какими мерами обеспечивается информационная защищенность и функциональная устойчивость сложных систем класса ИТКС в штатном режиме и в условиях угроз ИБ;

из автореферата не ясно, как осуществляется взаимодействие ЦУСБ ИТКС с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

Данные недостатки не имеет определяющего значения при оценке новизны, теоретической и практической ценности результатов выполненного соискателем исследования.

Таким образом, диссертационная работа Милославской Н.Г. представляет собой завершенное научное исследование, содержащее решение существенной проблемы создания научно-методических основ обеспечения сетевой безопасности информационных ресурсов ИТКС субъектов КИИ РФ в условиях существования угроз ИБ. По своей новизне, уровню научной проработки и практической значимости работа соответствует требованиям Постановления Правительства РФ от 24.09.2013 № 842 «О порядке присуждения ученых степеней», а ее автор, Милославская Наталья Георгиевна, заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Проректор по научной работе НИУ МИЭТ
доктор технических наук, профессор
(специальность: 05.27.06 Технология и оборудование для производства полупроводников, материалов и приборов электронной техники)

Гаврилов Сергей Александрович

Заведующий кафедрой «Информационная безопасность» НИУ МИЭТ
доктор технических наук, профессор
(специальность 20.01.12 – Радиоэлектронная борьба, способы и средства)
Анатолий Анатольевич Хорев

Сведения об организации:
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники» (МИЭТ), 124498, г. Москва, г. Зеленоград, пл. Шокина, д. 1, Телефон: +7 (499) 740-92-13, электронная почта: horev@miee.ru