ОТЗЫВ

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

Усилия международного сообщества, направленные на развитие глобального информационного общества должны сопровождаться согласованными действиями по созданию безопасного информационного пространства. Российская Федерация (РФ), в свою очередь, в Федеральном проекте «Информационная безопасность» формулирует направления обеспечения информационной безопасности (ИБ) в отношении объектов ее критической информационной инфраструктуры (КИИ), включая обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи РФ и обеспечение безопасности передаваемой по ней информации, а также обрабатываемой в информационных системах на территории РФ. Федеральным законом РФ № 187-ФЗ к объектам КИИ отнесены, в том числе, информационно-телекоммуникационные сети (ИТКС) субъектов КИИ. Таким образом, решение вопросов создания и эксплуатации защищенных ИТКС сегодня требует разработки адекватных методов и подходов. В этом свете тематика диссертации Милославской Н.Г. и сформулированная научная проблема чрезвычайно актуальны.

Автором проведена декомпозиция решаемой проблемы на ряд частных научных задач исследования, в ходе решения которых получены следующие основные новые научные результаты:

- обоснование включение в ИТКС нового специализированного структурного элемента – центра (названного ЦИУСБ), предназначенного для упреждающего управления сетевой безопасностью ИТКС;
- научно обоснованная методология и принципы построения типового ЦИУСБ с применением интеллектуальных подходов обработки больших относящихся к ИБ данных;
- научно обоснованная структуризация сложноорганизованных, иерархически взаимосвязанных понятий информационной защищенности ИТКС в виде единой таксономии;
- принципы и базовые архитектурные решения построения

перспективных ЦИУСБ для объектов КИИ и необходимая для их функционирования при управлении инцидентами ИБ в ИТКС бизнес-логика;

- защищенное средство блокирования попыток компрометации свидетельств инцидентов ИБ в ИТКС в составе SIEM-системы 3.0;
- формализованные взаимосвязанные процессы управления инцидентами ИБ ИТКС.

Кроме этого, при получении результатов исследования применены такие новые технологии и концепции, как блокчейн и озера данных. Также уточнена и существенно расширена по сравнению с известной временная шкала эволюции технологий и средств обеспечения сетевой безопасности и разработан глоссарий взаимосогласованных терминов предметной области обеспечения сетевой безопасности, отвечающий существующей нормативной и правовой базам и расширяющий терминологию ГОСТ Р ИСО/МЭК 27033-1-2011.

Практическая ценность работы заключается в масштабности рассматриваемой темы и полученных результатов, успешно внедренных в такие организации как Банк России (акты головного исполнителя работ – российской компании «ЕС-лизинг» и ООО «ЛИНС-М»), Ситуационный центр Службы ИБ Газпромбанка, Банк ВТБ (акт головного исполнителя работ – ООО «ЛИНС-М»), компания Qualys, НИЯУ МИФИ, Федеральное УМО в системе высшего образования по укрупненной группе специальностей направления подготовки «Информационная безопасность», что подтверждено соответствующим актами.

Публикации автора достаточно полно отражают результаты исследования. Их апробация диссертантом на международных и российских конференциях проведена должным образом.

По автореферату диссертации имеются следующие замечания:

1. В практической значимости работы упомянута разработка реестра (классификатора) рисков ИБ. К сожалению, сам вид реестра в тексте автореферата не представлен, что не позволяет оценить его.
2. В тексте присутствуют опечатки: на стр. 13 «предложен виды реестра» и на стр. 7 «информационную защищенности».

Заключение:

Вышеприведенные замечания не уменьшают в целом актуальность, научную новизну и практическую ценность научной квалификационной работы. Работа выполнена на высоком научном уровне и соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Автор диссертационной работы – Милославская Н.Г. заслуживает присуждения ей ученой степени доктора технических наук по специальности 05.13.19.

Остапенко Александр Григорьевич
Заведующий кафедрой систем информационной безопасности
Воронежского государственного технического университета
Профессор, д.т.н.,
шифр специальности: 05.09.05 Теоретическая электротехник
Тел. +7(473) 252-34-20, email: alexostap123@gmail.com

_____ Александр Григорьевич Остапенко

«21» декабря 2020 г.

Подпись Остапенко Александра Григорьевича удостоверяю.

Проректор по научной работе Коновалов Д.А.

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный технический университет» (ФГБОУ ВО «ВГТУ»), 394006, г. Воронеж, ул. 20-летия Октября, д. 84. Телефон: +7(473) 271-53-15. Электронная почта: priem@vgasu.vrn.ru