ОТЗЫВ

на автореферат диссертации соискателя ученой степени доктора технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность

Милославской Натальи Георгиевны

на тему: «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях»

Федеральный закон РФ от 26.07.2017 № 187-ФЗ определяет информационно-телекоммуникационные сети (ИТКС) субъектов критической информационной инфраструктуры (КИИ) наравне с другими объектами КИИ – информационными системами и автоматизированными системами управления. Статья 10 закона гласит, что «в целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование». Основными задачами таких систем безопасности являются предотвращение неправомерного доступа и действий с информацией, обрабатываемой значимым объектом КИИ, недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта КИИ, восстановление функционирования значимого объекта КИИ после подобных воздействий и непрерывное взаимодействие с ГосСОПКА РФ.

На создание научной основы для решения именно этих актуальных задач и направлено диссертационное исследование Милославской Н.Г., что успешно подтверждено получением новых научных результатов, а именно:

- научно обоснованная методология и принципы построения типового специализированного структурного элемента ИТКС – центра упреждающего управления сетевой безопасностью (названного ЦИУСБ) с применением интеллектуальных подходов обработки больших

относящихся к ИБ данных;

- научно обоснованная структуризация сложноорганизованных, иерархически взаимосвязанных понятий теории информационной безопасности (ИБ) в виде таксономии;
- принципы, базовые архитектурные решения построения и бизнес-логика функционирования ЦИУСБ, необходимые для эффективного управления инцидентами ИБ в ИТКС;
- формализованные взаимосвязанные процессы управления инцидентами ИБ ИТКС;
- защищенное средство блокирования попыток компрометации свидетельств инцидентов ИБ в ИТКС в составе SIEM-системы 3.0 как ядра ЦИУСБ.

Соискатель при получении данных результатов использовала как традиционные подходы, основанные на теории систем, теории управления, теории ИБ, и актуальную нормативную и правовую базу, так и новые лучшие практики обеспечения ИБ и технологии типа блокчейна и озера данных.

Высокая практическая ценность работы заключается в широком спектре решенных задач и полученных помимо основных не менее значимых результатов (например, классификатор рисков, собираемая для сбора доказательств компьютерной атаки постоянная и временная информация и многое другое) и их внедрении в системы обеспечения ИБ Банк России Службы ИБ Газпромбанка, ВТБ. Очень важным представляется внедрение в Федеральное УМО в системе высшего образования по укрупненной группе специальностей направления подготовки «Информационная безопасность» и НИЯУ МИФИ для подготовки кадров для ЦИУСБ, что подтверждается соответствующим актами о внедрении/использовании.

Апробация диссертантом результатов исследования выполнена на требуемом уровне – как можно судить по списку работ, приведенных в автореферате диссертации, публикации и доклады автора на международных и российских конференциях отражают их должным образом.

Выводы по автореферату:

Диссертационная работа Милославской Натальи Георгиевны выполнена на высоком научно-методической уровне, обладает существенной научной новизной и практической ценностью, соответствует специальности 05.13.19 и требованиям п. 9 Положения ВАК РФ к диссертациям на соискание ученой степени доктора технических наук, а автор исследования Милославская Н.Г. достойна присуждения ей ученой степени доктора

технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Профессор кафедры вычислительной техники и защиты информации,
Профессор, д.т.н., 01.01.11 – Системный анализ и автоматическое управление
Тел. (347)273-06-72, email: vasilyev@ugatu.ac.ru

Васильев Владимир Иванович

«25» 12 2020 г.

Зав. кафедрой вычислительной техники и защиты информации,
Профессор, д.ф.-м.н., 05.13.01 – Системный анализ, управление и обработка информации (в промышленности)
Тел. (347)273-06-72, email: vtizi@ugatu.su

Картак Вадим Михайлович

«25» 12 2020 г.

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), 450008, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12, +7(347)273-06-72, vtizi@ugatu.su

Подпись Васильева В.И., Картака В.М.
Удостоверяю «25» 12 2020 г.
Начальник отдела документационного обеспечения и архива Гильманова Л.Н.