ОТЗЫВ

на автореферат диссертационной работы Милославской Натальи Георгиевны на тему «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»

Диссертационная работа Милославской Н.Г. посвящена решению одной из актуальных проблем сферы информационной безопасности – разработке методологии построения центров управления сетевой безопасностью информационно-телекоммуникационных сетей. Развертывание подобных центров направлено на обеспечение устойчивого функционирования информационно-телекоммуникационных сетей, а также информационных систем, взаимодействие которых такие сети обеспечивают в условиях, проводимых на них различных кибератак.

Иерархическая архитектура типового центра управления сетевой безопасностью, предложенная соискателем, представляет собой пять взаимосвязанных уровней, функционирование которых направлено на структурирование поступающей информации о функционировании информационно-телекоммуникационных сетей с ее последующим ее анализом для обнаружения угроз и инцидентов информационной безопасности.

Отличительной особенностью центра является его ядро, которое базируется на SIEM системе 3.0. Для контроля целостности данных в ней предложено использовать технологию блокчейн. Обеспечение информационной безопасности центра управления сетевой безопасностью базируется на принципе сегментирования (зонирования) и реализуется за счет применения межсетевых экранов, обеспечивающих разграничение доступа к различным элементам архитектуры центра.

Анализ представленных результатов работы позволяет констатировать, что поставленная цель достигнута. В итоге исследования получен ряд результатов, характеризующихся научной новизной и практической значимостью.

В качестве замечаний по автореферату можно выделить следующее:

1. Пункты «Теоретическая и практическая значимость» и «Новизна полученных результатов» очень схожи по изложению.

2. Требует пояснения, за счет каких программно-технических решений обеспечивается функциональная устойчивость центра управления сетевой безопасностью.

3. Присутствуют неудачные выражения: «озеро данных» (стр. 33), «быстрое обнаружение» (стр. 37).

Приведенные замечания не снижают научной и практической значимости диссертационной работы.

В заключение необходимо отметить, что диссертационная работа Милославской Н.Г. является научно-квалификационной работой, выполненной на высоком методическом уровне, и отвечает требованиям, предъявляемым ВАК России к диссертациям на соискание учёной степени доктора наук. Соискатель – Милославская Наталья Георгиевна – заслуживает присуждения учёной степени

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

Отзыв подготовил:
Борботько Тимофей Валентинович
заведующий кафедрой защиты информации,
учреждения образования «Белорусский государственный
университет информатики и радиоэлектроники»,
профессор, д.т.н., 05.13.19 - «Методы и системы защиты информации, информационная безопасность»
Тел. +375172932308, email: secure@bsuir.by

_____ Борботько Тимофей Валентинович

«6» января 2021 г.

Подпись Борботько Тимофея Валентиновича удостоверяю

ПОДПИСЬ УДОСТОВЕРЯЮ
Начальник центра кадровой работы
Митрофанова Е.С
(подпись, ФИО)
06.01. 2021 г.

Сведения об организации:
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», 220013, Республика Беларусь, г. Минск, ул. П.Бровки, 6,
Тел. + 375 (17) 379 32 35, email: kanc@bsuir.by