ОТЗЫВ

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

Развитие глобального информационного общества и цифровизация всех сфер человеческой деятельности должны поддерживаться созданием информационного пространства, удовлетворяющего строгим требованиям обеспечения его информационной безопасности (ИБ). Информационное пространство Российской Федерации (РФ) включает объекты критической информационной инфраструктуры (КИИ), для которых обеспечение устойчивого функционирования, целостности и ИБ передаваемой по ним информации, бесперебойное предоставление сервисов являются важнейшими приоритетами. В Федеральном законе РФ № 187-ФЗ объектами КИИ названы информационно-телекоммуникационные сети (ИТКС) субъектов КИИ. В этом связи тема диссертации Милославской Н.Г. «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях» и выделенная научная проблема представляются весьма актуальными.

Для достижения поставленной цели автором определены структурно-логическая схема и задачи исследования, в ходе решения которых получены новые научные результаты:

- обоснование включение в ИТКС ЦИУСБ – нового структурного элемента – специализированного центра, предназначенного для упреждающего управления сетевой безопасностью ИТКС;
- научно обоснованная методология и принципы построения типового ЦИУСБ, отличающегося от его предшественников применением интеллектуальных подходов обработки больших данных, относящихся к ИБ ИТКС, и концепции озер данных;
- научно обоснованная структуризация сложноорганизованных, иерархически взаимосвязанных понятий ИБ (уязвимости, угрозы ИБ, сетевые атаки, инциденты ИБ) в виде единой таксономии;

- принципы, базовые архитектуры построения и бизнес-логика функционирования ЦИУСБ для объектов КИИ;
- формализованные взаимосвязанные процессы управления инцидентами ИБ для ИТКС;
- средство защиты свидетельств инцидентов ИБ в ИТКС в составе SIEM-системы 3.0, основанное на технологии блокчейна.

Кроме этого заслуживающими внимания результатами являются временная шкала эволюции технологий и средств обеспечения сетевой безопасности и глоссарий взаимосогласованных терминов предметной области обеспечения сетевой безопасности, расширяющий терминологию ГОСТ Р ИСО/МЭК 27033-1-2011. Для практического применения полезны и такие результаты исследования, как обзор основных возможностей ИБ-аналитики при решении задач управления инцидентами ИБ ИТКС, реестр (классификатор) рисков ИБ, примеры постоянной и временной информации, подлежащей сбору при расследовании инцидентов ИБ в ИТКС, меры и средства обеспечения ИБ, распределенные по зонам безопасности ЦИУСБ.

Практическая ценность работы подтверждается успешными внедрениями в Банке России (акты головного исполнителя работ – российской компании «ЕС-лизинг» и ООО «ЛИНС-М»), Ситуационном центре Службы ИБ Газпромбанка, Банке ВТБ (акт головного исполнителя работ – ООО «ЛИНС-М»), компании Qualys, НИЯУ МИФИ, Федеральном УМО в системе высшего образования по укрупненной группе специальностей направления подготовки «Информационная безопасность».

В основных публикациях автора по теме диссертационного исследования, насколько можно судить по приведенному в конце автореферата сокращенному списку, полно отражают полученные результаты исследования. Их апробация на международных и российских конференциях и семинарах показывает их состоятельность.

По автореферату диссертации можно сделать несколько замечаний:

1. Вид реестра рисков ИБ в тексте автореферата не представлен, что затрудняет его оценку.
2. Средство защиты свидетельств инцидентов ИБ как часть SIEM-системы, разработанное с использованием технологии блокчейна, описано слишком кратко, что также не позволяет в полной мере оценить его функционал и реализацию.
3. В тексте присутствует ряд стилистических погрешностей.

Однако вышеприведенные замечания не умоляют несомненных

достоинств представленной работы, ее научную новизну и практическую ценность.

Заключение:

Диссертационная работа Милославской Н.Г. выполнена на высоком научном и методическом уровне, обладает существенной научной новизной и практической ценностью и соответствует специальности 05.13.19 – методы и системы защиты информации, информационная безопасность. Автор исследования – Милославская Наталья Георгиевна – заслуживает присуждения ей ученой степени доктора технических наук по специальности 05.13.19.

Отзыв подготовил: Рацеев Сергей Михайлович

Профессор кафедры информационной безопасности и теории управления

д.ф.-м.н., 01.01.06 математическая логика, алгебра и теория чисел

Тел. 8(8422) 37-24-73 (доб. 4), email: ratseevsm@mail.ru

_____ С. М. Рацеев

«25» января 2021 г.

Подпись Рацеева С. М.
ЗАВЕРЯЮ
Менеджер по персоналу Смирнова С. М.

Сведения об организации:

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ульяновский государственный университет» (УлГУ), 432017, г. Ульяновск, ул. Льва Толстого, д. 42, +7 8422 41-20-88, contact@ulsu.ru.