В диссертационный совет Д 002.073.02

при ФИЦ ИУ РАН

ОТЗЫВ

на автореферат диссертации Милославской Н.Г. «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях»

на соискание учёной степени доктора технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность

Актуальность диссертационной работы определяется необходимостью решения проблемы создания систем упреждения угроз и инцидентов ИБ для обеспечения высокого уровня ИБ ИТКС организаций. Одним из возможных решений на научной основе является построение специализированных центров – ЦИУСБ, предназначенных для упреждающего управления сетевой безопасностью, что является весьма перспективным. .

Целью диссертационной работы Милославской Н.Г. было создание научно обоснованной методологии и принципов построения специализированного структурного элемента ИТКС – типового ЦИУСБ в составе СОИБ ИТКС, призванного осуществлять упреждающее управление сетевой безопасностью при передаче данных в ИТКС на всех стадиях ее жизненного цикла. За счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных эта цель была достигнута автором.

Основными научными результатами исследования являются.

1 Обобщенная модель процессов функционирования типового ЦИУСБ, которая может быть использована не только применительно к ЦИУСБ, но и к ИТКС

2. Для типового ЦИУСБ разработана архитектура хранения и обработки в режиме жесткого и мягкого реального времени больших и быстрых относящихся к ИБ ИТКС данных, основанная на использовании озер данных и ориентированная на применение в ЦИУСБ предложенного в рамках исследования процесса ИБ-аналитики и синтеза новых знаний об информационной защищенности ИТКС ОРГАНИЗАЦИИ для ее упреждающей защиты.

3. Расширенный метод составления карт процессов позволил формализовать основные процессы управления инцидентами ИБ ИТКС.

4. Обоснована необходимость создания *SIEM*-системы нового поколения для использования в типовом ЦИУСБ с применением технологий блокчейна со сверткой.

в составе *SIEM*-системы 3.0 разработано средство блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ.

К достоинствам работы следует отнести: анализ значительного объёма научной и технической литературы, использование результатов проведенного исследования при их внедрении в крупных российских банках и компаниях, в учебном процессе образовательных учреждений. Результаты работы представляют практическую ценность для обеспечения безопасности информации в ИТКС государственных органов, корпораций и отдельных организаций. В частности, в составе *SIEM*-системы 3.0 разработано средство блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ.

Результаты работы представлены в 21 научной статье, из них 16 в журналах, входящих в Перечень рецензируемых научных журналов, рекомендованных ВАК РФ для публикации основных научных результатов диссертаций на соискание ученых степеней, и 5 в иностранных журналах. Кроме того, имеется значительно кол-во публикаций в виде докладов на различных международных конференциях, индексируемых Scopus и Web of Science, а

также учебных пособий. Качество опубликованных работ подтверждается индексами Хирша Милославской Н.Г. в базах данных Scopus и Web of Science, h=7 и h=4 соответственно.

По автореферату имеются замечания.

1. На рис. 1 представлена логическая структура ИТКС ОРГАНИЗАЦИИ, которая должна объединять все подсистемы в единую систему. Однако элементы этой структуры представлены как независимые, разрозненные и не представляющие собой систему с совокупность подсистем.
2. К сожалению, подобный недостаток имеется и на рис. 2. На нем представлена система классификации сетевых атак. Но не показаны связи элементов, что не подтверждает их взаимосвязей. А именно на «их глубокой взаимосвязи» настаивать автор.
3. Имеются в автореферате и не свойственные техническому стилю изложения выражения: «наиболее результативно», «четкие границы», «наиболее», «наименее», «существенно» и т.д. Подобные выражения предполагают наличие критериев «четкости границ», «наибольшей результативности» и т.д. Но таких критериев в работе не обнаружено.
4. На мой взгляд, не достаточно конкретно изложены собственно методология и принципы. Возможно, это связано с малым объемом автореферата. Но представляется вполне уместным разместить и разъяснить именно их в автореферате.

Диссертационная работа Н.Г. Милославской является завершённой научно-квалификационной работой, выполненной ею самостоятельно, вносит значительный вклад в решение научной проблемы создания систем упреждения угроз и инцидентов ИБ для обеспечения высокого уровня ИБ ИТКС организаций, соответствует требованиям Положения ВАК России к докторским диссертациям, а её автор, Милославская Наталья Георгиевна, заслуживает присуждения ей учёной степени доктора технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Президент Томского государственного университета
систем управления и радиоэлектроники,
директор Института системной интеграции и безопасности,
профессор, доктор технических наук, 05.13.01 «Системный анализ, управление и обработка информации», тел.: +7 (3822) 90-71-55, e-mail: president@tusur.ru

Александр Александрович Шелупанов

«28» января 2021 г.

Подпись Александра Александровича Шелупанова удостоверяю.

Ученый секретарь совета Е.В. Прокопчук

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ФГБОУ ВО «ТУСУР»), 634050, г. Томск, пр. Ленина, д. 40, +7 (3822) 510530, e-mail: office@tusur.ru