О Т З Ы В

на автореферат диссертации 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

Актуальность проблем обеспечения сетевой безопасности для современных компьютерных сетей обусловлена бурным развитием общедоступных сетевых технологий обосновывается в семействе стандартов ISO/IEC 27033 и ее гармонизированных версиях ГОСТ Р ИСО/МЭК 27033. В части средств обеспечения безопасности компьютерных сетей в них рассматриваются только такие средства, как шлюзы безопасности, виртуальные частные сети и т.д., но в них не упоминаются центры управления сетевой безопасностью. В этой связи диссертационное исследование Милославской Н. Г., объектом которого являются информационно-телекоммуникационные сети (ИТКС) субъектов критической информационной инфраструктуры (КИИ) Российской Федерации (РФ) с точки зрения необходимости защиты их информационных ресурсов на всех стадиях их жизненного цикла, устраняет существующий пробел и является, несомненно, актуальным.

В начале работы, после формулирования научной проблемы и определения области и границ исследования, были выбраны пути решения пяти поставленных задач. Пять глав диссертации последовательно и в логической взаимосвязи излагают полученные диссертантом результаты. Четкое формулирование требований и выбранные методы исследования позволили всестороннее и комплексно достичь цели исследования, которая заключалась в разработке научно обоснованной методологии и принципов построения специализированного структурного элемента информационно- телекоммуникационных сетей (ИТКС) – типового центра интеллектуального управления сетевой безопасностью (ЦИУСБ) в составе общей системы обеспечения информационной безопасности (СОИБ) единого информационного пространства субъекта КИИ, позволяющего за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ интеллектуальных подходов обработки больших, относящихся к ИБ ИТКС данных, более эффективно управлять сетевой безопасностью. К достоинствам работы можно отнести комплексный подход к решению задач ИБ сетевой инфраструктуры, а также отдельные результаты, представляющие как научное, так и практическое значение. Это, например, применение блокчейн-технологии для защиты инкапсулированной в ЦИУСБ базы данных, создание таксономии для базовых понятий в области ИБ, и глоссария в области обеспечения сетевой безопасности. Судя по автореферату, соискатель отлично владеет нормативно-правовой базой в области ИБ, и хорошо разбирается как в традиционных, так и в новейших подходах к обеспечению информационной безопасности и функциональной устойчивости ИТКС.

Все основные результаты диссертации опубликованы в рецензируемых изданиях, входящих в перечень ВАК, а также в ряде зарубежных работ, входящих в базы научного цитирования Web of science и Scopus. Заслуживает внимания и большое число учебно-методического материала с участием автора, опубликованного с грифом УМО. Структура, содержание и объем автореферата соответствуют требованиям, установленным «Положением о присуждении ученых степеней».

По автореферату имеются следующие замечания к его содержанию, не влияющие на общую положительную оценку диссертации:

1. Показанная на рис. 2 системная классификация сетевых атак на ИТКС представлена в виде разрозненных подграфов и не имеет вид ни дерева, ни семантической сети. На стр. 19 отмечается, что в работе оцениваются лишь угрозы, актуальные для ИТКС, а не ее клиентов, но в классификации присутствует персонал, который никак компонентом ИТКС не является. Не раскрыты на рисунке и такие классификационные признаки, как цели, методы и средства реализации атаки, используемые атакой уязвимости.
2. Не все вопросы изложены в автореферате достаточно полно. Так, после прочтения автореферата осталось не до конца понятным, в чем же состоит интеллектуальность ЦИУСБ: это интеллект обслуживающих его сотрудников или же это какие-то системы искусственного интеллекта? Нет информации и по организации защиты данных с применением блокчейн технологии, которая, как известно, предполагает наличие компьютерной сети для распределенного хранения цепочек транзакций, тогда как само понятие ЦИУСБ предполагает, что данные хранятся локально. Не нашлось места в автореферате и для описания структуры, архитектуры и состава ЦИУСБ в целом. Из трех спроектированных архитектур (функциональной, обработки относящихся к ИБ ИТКС данных и обеспечения собственной ИБ) на рис. 8 и 9 показаны лишь две. Конкретные результаты работы, изложенные в шестом разделе диссертации, почему-то в автореферате тоже не освещены, хотя объем автореферата вполне позволял бы это сделать.
3. Текст автореферата плохо вычитан и имеет ряд других изъянов. Так, в нем имеются неверные склонения падежей (например, «повышения качество» на стр.4, «обоснованная структуризации понятий» на стр. 11, «предложен виды…» на стр.13, «для немедленного выявление» на стр.26, «рассмотрены вопросов» на стр35 и др.), несогласованные предложения (последнее предложение на стр.10, предложение п.4 на стр.12 и п.1. на стр.13), стилистические неточности (последний абзац на стр.4 трудно читаем, предмет исследования не может быть построением чего-либо (стр.6), дважды непонятна фраза на стр.10 «Защищенное по своему дизайну на основе технологий блокчейна средство…», т.к. непонятно, как можно защитить по дизайну и какое отношение к нему имеет блокчейн-технология). Есть и просто ошибки («Исследование опиралось как общенаучные методы…» (пропущен предлог «на») на стр. 10, «Статистика … за 2020 г. от показывает» на стр. 3 внизу). Ничем не оправдано и написание слова «организация» в верхнем регистре по всему тексту автореферата. А обилие аббревиатур (СОИБ, СУИБ, ЕИП, ЦИУСБ, ИТКС, ИИ, ПУИИБ, ЦМБ, ЖРС, МЭ, СОВ/СПВ, ЦИБ, СОЦ), некоторые из которых используются в ином смысле (например, ИИ – это чаще искусственный интеллект, чем информационная инфраструктура) усложняет чтение. Из-за таких изъянов только на стр.14 в п. 9 практической значимости стало немного понятно, что же такое ЦИУСБ: структурное подразделение организации, или комплекс программных или программно-аппаратных средств. Впрочем, и тут есть двусмысленности: если ЦИУСБ — это структурное подразделение и содержит штат сотрудников, то как он может быть интеллектуальным?

Как уже было отмечено, данные замечания не являются критическими, не оказывают влияния на положительную оценку диссертации и не снижают общей ценности работы, которая представляет несомненный научный интерес и имеет большое практи

ческое значение для специалистов, занимающихся исследованиями в области разработки систем обеспечения сетевой безопасности.

Содержание автореферата, а также представленные в научных публикациях сведения позволяют утверждать, что диссертация является завершенной научно-квалификационной работой, в целом выполненной на высоком научном уровне, соответствует упомянутым в автореферате пунктам паспорта научной специальности, полностью удовлетворяет другим требованиям к докторским диссертациям, изложенным в п.14 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 (ред. от 01.10.2018, с изм. от 26.05.2020), и ее автор достойна присуждения ей учёной степени доктора технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Якунин Алексей Григорьевич,
заведующий кафедрой «Информатика,
вычислительная техника и информационная безопасность», профессор, д.т.н.,
научная специальность - 05.13.05 –
Элементы и устройства вычислительной
техники и систем управления.
Тел. +7(3852) 290-786,
e-mail: almpas@list.ru

Якунин Алексей Григорьевич

« 27 » января 2021 г.

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Алтайский государственный технический университет имени И.И. Ползунова» (АлтГТУ им. И.И.Ползунова), 656038, г. Барнаул, проспект Ленина, д. 46,
тел. +7 (385-2) 29-07-06, altgtu@list.ru

подпись Якунина А.Г.
заверяю:
зам нач-ка упр. Т.В. Кравцова