

ОТЗЫВ

доктора технических наук, доцента Баранковой Инны Ильиничны на автореферат диссертации Синадского Николая Игоревича на тему «Методология синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности», представленной на соискание ученой степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Создание киберполигонов в сфере информационной безопасности (далее — ИБ), предназначенных как для проведения обучения специалистов, так и для тестирования сетевых средств защиты информации (далее — ССЗИ), — это активно развивающееся и чрезвычайно востребованное в современных условиях направление научных исследований в сфере ИБ. При этом возникает потребность в методиках и практических инструментах тестирования ССЗИ, которые позволят моделировать комплексные атакующие воздействия и условия их проведения в условиях реальных компьютерных сетей, поэтому разработка и внедрение научно обоснованной методологии для своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на инциденты ИБ является актуальной научной проблемой.

Научная новизна полученных результатов

Научная новизна диссертационной работы состоит в решении научной проблемы, имеющей важное социально-экономическое значение и заключающейся в создании научно-методического инструментария при синтезе интерактивной сетевой среды для учебно-научных компьютерных полигонов, предназначенных для обнаружения компьютерных атак.

Практическая значимость результатов

Практическая значимость результатов диссертации заключается в том, что новое техническое решение по созданию учебно-научных компьютерных полигонов позволяет автоматизировать процессы синтеза тестовых массивов данных и сетевого трафика для выявления неизвестных уязвимостей при тестирования ССЗИ с учетом вариативности внешней сетевой среды и комплексности атакующего воздействия, позволяет организовать практико-ориентированное обучение специалистов по обнаружению, предупреждению и ликвидации последствий компьютерных атак, а также по реагированию на инциденты ИБ, что вносит значительный вклад в повышение безопасности компьютерных сетей.

Обоснованность и достоверность научных положений

Обоснованность и достоверность научных результатов проведенных исследований подтверждается их апробацией на конференциях, публикациях в изданиях, определенных ВАК РФ, корректностью использованного математического аппарата и теоретических обоснований, а также результатами экспериментов, проведенных в рамках диссертационного исследования.

Основные научные результаты диссертации опубликованы в 18 работах, из них 14 статей, опубликованных в рецензируемых научных изданиях, получены 4 свидетельства о государственной регистрации программы для ЭВМ.

Замечания и вопросы по работе

1. Соискатель указывает, что научная новизна работы заключается в том числе в создании «методологии, основанной на ряде разработанных методов, моделей, алгоритмов и аппаратно-программного инструментария автоматизации процессов синтеза массивов данных для тестирования ССЗИ». Однако из текста автореферата не понятно, какие численные параметры или качественные характеристики «тестовых массивов данных и сетевого трафика» улучшились благодаря автоматизации процессов их синтеза?

2. Из текста автореферата неясно, как проводилась проверка адекватности предложенных автором математических моделей.

3. Для синтеза фонового сетевого трафика соискателем предложена его статистическая модель. При этом не указывается, каким образом и в каком количестве накапливались данные на реальных сетях, чтобы закладываемые при моделировании трафика параметры и характеристики обладали статистической представительностью.

Сделанные замечания имеют дискуссионный характер и не снижают научной ценности рецензируемой по автореферату работы.

Диссертационная работа изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, личному вкладу автора, отражению результатов в публикациях, а также полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ и специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Автор диссертации Синадский Николай Игоревич заслуживает присуждения учёной степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Баранкова Инна Ильинична

Доктор технических наук, доцент

Заведующая кафедрой информатики и информационной безопасности

Федеральное государственное бюджетное образовательное учреждение высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова»

Тел.: +7 (3519) 23-27-51

e-mail: inna_barankova@mail.ru


Адрес: 455000, г. Магнитогорск, пр. Ленина, д.38, УК 1, ауд. 368

Подпись _____ заверяю


(подпись)

06.12.22
(дата)

Личную подпись заверяю
Начальник отдела кадров
ФББОУ ВО «МГТУ» им. Г.И. Носова


«06» 12 2022

М.П.