ОТЗЫВ

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

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. Следовательно, разработка и внедрение научно обоснованной методологии имитационного моделирования при синтезе интерактивной сетевой среды с целью своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на инциденты ИБ является актуальной научной проблемой.

Наиболее существенным научным результатом диссертационной работы, его научная новизна состоит в решении научной проблемы, имеющей важное значение для народного хозяйства и заключающейся в создании научно-методического инструментария при синтезе интерактивной сетевой среды для учебно-научных компьютерных полигонов, позволяющего автоматизировать процессы синтеза тестовых массивов данных для тестирования ССЗИ с учетом вариативности сетевой среды и комплексности атакующего воздействия.

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 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.

Вместе с этим, следует отметить некоторые замечания и вопросы по содержанию

автореферата:

1. В автореферате сказано, что разработана модель сетевого средства защиты информации (ССЗИ) как объекта тестирования в практической реализации для четырех категорий ССЗИ: систем обнаружения вторжений, телекоммуникационного оборудования, систем анализа защищенности и информационно-аналитических систем безопасности. Учтено ли в моделях ССЗИ применение средств виртуализации?
2. На стр. 5 автореферата указано, что результативность реакции ССЗИ на определенное воздействие зависит от состояния внешней для ССЗИ среды и конфигурирования ССЗИ с учетом характеристик сетевой среды. Каковы возможности внесения изменений в конфигурацию ССЗИ в процессе тестирования?
3. В автореферате не в полной мере приведены сведения о проведении количественно-качественной оценки представленного комплекса, также подробно не описаны аналоги похожих программно-аппаратных комплексов. Каковы перспективы применения представленного полигона для ССЗИ автоматизированных систем управления технологическими процессами?

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.

Заведующий кафедрой защиты информации
Высшей школы электроники и компьютерных наук
ФГАОУ ВО «Южно-Уральский государственный университет
(национальный исследовательский университет)»,
кандидат технических наук, доцент

Тел: +7 (351) 267-93-55
E-mail: sokolovan@susu.ru
Адрес: 454080, г. Челябинск, проспект Ленина, 76

_____ /Соколов Александр Николаевич/

21.11.2022

Подпись Соколова А.Н. удостоверяю
Начальник управления
по работе с кадрами Н.С. Макарова