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 заключаетсяв 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. На странице 23 говорится о том, что «синтез тестовых массивов данных осуществляется на основе статистических характеристик реальных ИТС», хранящихся в виде набора матриц. Является ли это распределение многомерным? Учитывались ли корреляции признаков, связаны ли распределения, или значение по каждому распределению выбирается независимо? Например, одинакова ли вероятность выбрать малую задержку (первое распределение) между пакетами для пакетов большой и малой длины (второе распределение)?

2. Чем обоснован выбор относительно малоизвестного алгоритма сдвига среднего для решения задачи кластерного анализа результатов работы генетического алгоритма при тестировании защищенности телекоммуникационного оборудования от атак типа «отказ в обслуживании»?

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.

Доцент базовой кафедры № 252 – информационной безопасности
Института кибернетики МИРЭА – Российского технологического университета
кандидат технических наук, доцент

Тимаков Алексей Анатольевич
"14" ноября 2022 года

Подпись Тимакова Алексея Анатольевича удостоверяю:
Начальник отдела Управления делами Сазонова
Федеральное государственное бюджетное образовательное учреждение высшего образования "МИРЭА - Российский технологический университет" (РТУ МИРЭА)
Адрес: 119454, город Москва, проспект Вернадского, дом 78
Сайт: https://www.mirea.ru/
Телефон: +7 (499) 215-65-65
Электронная почта: rector@mirea.ru