

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 сценарии 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. Адекватность тестовых данных, объединяющих фоновый трафик и атакующие воздействия, соискатель предлагает осуществлять путем анализа значения показателя правдоподобия Херста. Насколько оправдано его применение именно для объединенного трафика? Не наблюдается ли при слиянии частных трафиков «синергетического» эффекта, меняющего важные характеристики интегрального трафика?

2. В автореферате при описании имитационно-статистического метода синтеза массивов условно-реальных данных, моделирующих процесса взаимодействия пользователей ИТС не приводится информации об анализе соответствия сгенерированных данных реальным.

Указанные 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.

Воронцов Юрий Витальевич:

Кандидат технических наук
Начальник специального научно-технического отдела
Акционерное общество «Уральский электрохимический комбинат»
Тел.:8(34370) 9-24-24
e-mail: condor@ueip.ru
624130, г. Новоуральск, ул. Дзержинского, 2

Подпись



заверяю

(подпись)

(дата)

09.11.2022

