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 компьютерных полигонов, адекватно моделирующих функционирование современных сетевых средств защиты информации (далее — ССЗИ) и позволяющих без ущерба информационной безопасности осуществлять анализ технологий реализации распределенных комплексных сетевых атак, разработку и тестирование механизмов защиты от них, несомненно является актуальным и востребованным направлением научных исследований. Не менее важна здесь подготовка квалифицированных в данной предметной области специалистов, которая может быть существенно улучшена, если она будет осуществляться на базе развитых компьютерных полигонов.

При этом возникает потребность в методах, моделях, алгоритмах и реализующих их инструментальных средствах синтеза максимально приближенной к реальности интерактивной сетевой среды для дальнейшего тестирования ССЗИ, выявления в них уязвимостей. Следовательно, разработка и апробация 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 информационной безопасности является актуальной научной проблемой. Наиболее существенным научным результатом диссертационной работы, его научная новизна состоит в решении указанной 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 применение разработанной методологии на базе учебно-научных компьютерных полигонов позволяет автоматизировать процессы синтеза тестовых массивов данных и сетевого трафика для выявления уязвимостей при тестирования ССЗИ с учетом вариативности внешней сетевой среды и комплексности атакующего воздействия, что дает возможность организовать практико-ориентированное обучение специалистов по

обнаружению, предупреждению и ликвидации последствий компьютерных атак, а также по реагированию на инциденты информационной безопасности.

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 по содержанию автореферата:

1. В автореферате не приведено результатов сравнения разработанных в ходе диссертационного исследования методов, моделей, методик, алгоритмов с существующими аналогами (например, генераторами трафика), для строгого обоснования их преимуществ. Например, не ясно, чем предлагаемые методы и технологии поиска новых уязвимостей ССЗИ, заключающихся в сбоях при определенных сочетаниях параметров внешней среды, отличаются или превосходят известные технологии фаззинг-тестирования.

2. При имитационном моделировании ССЗИ на основе изложенной в автореферате методологии (входящих в нее методах, моделях, методиках, алгоритмах, реализующих их инструментальных средствах) не говорится о использовании современных технологий виртуализации, позволяющих повысить достоверность такого моделирования, осуществлять мониторинг безопасности ССЗИ не только с применением «внешних» сенсоров систем обнаружения атак (СОА), а из используемых для виртуализации хостовых систем.

3. Хотя в автореферате указывается, что атаки анализируются «с точки зрения нарушения конфиденциальности, целостности и доступности информации», по сути везде рассматривается только угроза доступности информации («отказа в обслуживании»).

Сделанные замечания в целом 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.

Девянин Петр Николаевич

член-корреспондент Академии криптографии России,
д.т.н., профессор
научный руководитель ООО «РусБИТех-Астра»
Тел.: +7 (916) 154-19-48
e-mail: pdevyanin@astralinux.ru
Адрес организации: 117105, г. Москва,
Варшавское ш., д. 26

09.11.2022

(подпись) (дата)

Подпись Девянина П.Н. заверяю
заместитель генерального директора ООО «РусБИТех-Астра»
Соснин Ю.В.

09.11.2022

(подпись) (дата)