Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, доцента Козачка Александра Васильевича на диссертационную работу 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

Актуальность создания киберполигонов в сфере информационной безопасности определена Федеральным проектом «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», в рамках которой предусмотрено выполнение работ по созданию киберполигона для обучения и тренировки учащихся, специалистов и экспертов разного профиля, руководителей в области информационной безопасности (ИБ) и информационных технологий современным практикам обеспечения безопасности. Одной из задач учебно-научного компьютерного полигона является создание условий для проведения научных исследований в сфере обеспечения ИБ, в том числе для тестирования как защищенности ИТС в целом, так и отдельных средств защиты информации, среди которых выделяются технические, программные, программно-аппаратные и иные средства, обеспечивающие обнаружение, предупреждение и ликвидацию последствий компьютерных атак, а также реагирования на компьютерные инциденты.

Известные компьютерные полигоны, а также методики тестирования сетевых средств защиты информации (ССЗИ), используемые при проведении сертификационных испытаний и мероприятий по анализу уязвимостей, не позволяют в полной мере моделировать в процессе тестирования условия, существующие при проведении современных комплексных воздействий (комплексных атак), что снижает достоверность результатов мероприятий по анализу уязвимостей информационных систем в целом. Возникает потребность в методиках и практических инструментах тестирования ССЗИ, которые позволят моделировать комплексные атакующие воздействия и условия их проведения в реальных ИТС.

Наблюдается объективное противоречие между потребностями по комплексному тестированию ССЗИ с учетом непрерывного развития информационных технологий и современных ИТС и существующим научно-методическим и математическим обеспечением систем и комплексов, реализующих тестирование ССЗИ,

неудовлетворяющим указанным потребностям. Следствием неразрешенности этого противоречия является объективная необходимость теоретического обобщения и развития методов математического моделирования интерактивной сетевой среды, алгоритмов и программного обеспечения, интегрируемых в компьютерные полигоны, предназначенные для тестирования ССЗИ с учетом вариативности среды и комплексности атакующего воздействия.

В этой связи 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.

Научная новизна полученных результатов

Наиболее существенные научные результаты диссертационной работы и их научная новизна состоят 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. Предложенное решение в виде нового научно-методического инструментария, представляющего собой комплекс методов, моделей, алгоритмов, программного обеспечения и экспериментальных стендов синтеза тестовых массивов данных в составе учебно-научного компьютерного полигона в сфере ИБ, позволяет достичь поставленной цели — повышения показателей защищенности ИТС за счет предупреждения компьютерных атак путем раннего выявления уязвимостей ССЗИ посредством их тестирования, что вносит значительный вклад в повышение защищенности ИТС. Результаты имеют межотраслевой характер, использованы как на предприятиях и организациях, в том числе для тестирования ССЗИ, так и в образовательных учреждениях министерства науки и высшего образования Российской Федерации. Предложенный научно-методический инструментарий практико-ориентирован, универсален, опирается на современные методы математического моделирования систем и сигналов, с некоторой степенью адаптации пригоден для тестирования ССЗИ любого типа.

Обоснованность и достоверность научных положений,
сформулированных в диссертации

Обоснованность и достоверность научных результатов проведенных исследований подтверждается их апробацией на конференциях, публикациях в изданиях,

рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации, 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, рекомендованных ВАК и Аттестационным советом УрФУ, включая 4 статьи в изданиях, входящих в международные цитатно-аналитические базы; получены 4 свидетельства о государственной регистрации программы для ЭВМ.

Практическая значимость результатов диссертации

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 ИТС.

Полученные научные результаты используются в ООО «Уральский центр систем безопасности», в Уральском федеральном университете имени первого Президента России Б.Н. Ельцина, в Екатеринбургском научно-техническом центре ФГУП «НПП Гамма» (Екатеринбург, Россия).

Оценка содержания диссертации и её оформления

Диссертационная работа содержит 298 страниц текста, 72 рисунка и 9 таблиц, состоит из введения, четырех глав, заключения, списка сокращений, списка литературы из 258 наименований.

В первой главе представлено аналитическое исследование, в качестве модели угроз даны понятие и расширенная систематика комплексных сетевых компьютерных атак, которые рассматриваются как совокупная последовательность элементарных атакующих воздействий. Введены объекты тестирования — ССЗИ (СОА, ТКО, САЗ и ИАСБ) в качестве элементов обеспечения безопасности ИТС. Приведены основные свойства каждого типа ССЗИ, характеристики, подлежащие тестированию, и параметры синтеза соответствующих массивов данных. Представлен обзор известных технологий, методов и средств тестирования ССЗИ на примере СОА и ТКО. Рассмотрены и классифицированы

известные реализации синтеза фонового сетевого трафика, показаны их достоинства и недостатки. На основании результатов анализа состояния предметной области сформулированы цель и задачи исследования.

Во второй главе диссертации описана разработанная методология синтеза интерактивной среды для компьютерных полигонов в сфере ИБ, представлен разработанный научно-методический инструментарий проектирования компьютерных полигонов в сфере ИБ на базе интерактивной сетевой среды, позволяющий осуществлять автоматизацию процессов синтеза массивов данных для анализа защищенности ССЗИ с учетом вариативности сетевой среды и комплексности атакующего воздействия, с целью своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на инциденты ИБ на объектах ИТС и ИС.

В третьей главе диссертации представлены комплексы моделей, методик, алгоритмов и программного обеспечения и учебно-экспериментальных стендов синтеза тестовых массивов данных, предназначенные для тестирования ССЗИ.

В четвертой главе приведено описание структуры разработанного учебно-научного компьютерного полигона по расследованию инцидентов ИБ, который представляет собой комплекс моделей, алгоритмов, программного обеспечения и экспериментальных стендов синтеза тестовых массивов данных, основанный на разработанном методе имитационного моделирования интерактивной сетевой среды для тестирования ССЗИ.

Диссертация имеет четкую структуру, грамотно оформлена, соответствует паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Автореферат с достаточной полнотой отражает содержание диссертации.

Замечания и вопросы по работе

Вместе с этим следует отметить некоторые замечания и вопросы по содержанию диссертации и автореферата:

1. В диссертации не в полной мере приведены сведения о проведении количественно-качественной оценки представленного комплекса, также подробно не описаны аналоги похожих программно-аппаратных комплексов.

2. Не в полной мере доказана обоснованность представленного метода синтеза массивов данных, что может привести к некорректности при их использовании.

3. Представленные в диссертации цель работы, «теоретическая» цель и научная проблема с учетом схожести терминов «разработка» и «создание» научно-методического инструментария во многом совпадают, что, на взгляд оппонента, выглядит недостаточно корректно.

4. В диссертации недостаточно внимания уделено вопросу проверки адекватности предложенных автором математических моделей.

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

Заключение по работе

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. Автор диссертации Синадский Николай Игоревич заслуживает присуждения учёной степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
Сотрудник Академии ФСО России
доктор технических наук, доцент

Козачок Александр Васильевич

5 декабря 2022 г.

Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации»
Тел.: +7 (4862) 54-99-16
e-mail: a.kozachok@academ.msk.rsnet.ru
Адрес: 302015, г. Орел, ул. Приборостроительная, 35

Подпись сотрудника Академии ФСО России доктора технических наук, доцента Козачка Александра Васильевича ЗАВЕРЯЮ.

Руководитель кадрового аппарата Академии ФСО России

А.Б. Семибратов