ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора военных наук, профессора Лося Владимира Павловича 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». Задача киберполигонов – создание условий для обучения специалистов в области информационной безопасности (далее — ИБ), а также для проведения научных исследований в сфере обеспечения ИБ, в том числе для тестирования сетевых средств защиты информации (далее — ССЗИ).

При этом наблюдается объективное противоречие между потребностями по комплексному тестированию ССЗИ и существующим научно-методическим и математическим обеспечением систем и комплексов, реализующих тестирование ССЗИ. 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 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.

Научная новизна полученных результатов

Наиболее существенные научные результаты диссертационной работы и их научная новизна состоят в решении научной проблемы по созданию 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. 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, 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, определенных ВАК РФ 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, приведены основные свойства каждого типа ССЗИ (СОА, ТКО, САЗ и ИАСБ), 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 главе раскрываются структура и основные компоненты комплексного метода синтеза интерактивной среды, который предусматривает воздействие на тестируемый образец ССЗИ комбинации двух видов массивов данных: фонового и атакующего

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, хорошо 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 работе указано, что известные полигоны « … не позволяют в полной мере моделировать в процессе тестирования условия, существующие при проведении современных комплексных воздействий (комплексных атак)». Из чего соискатель делает вывод о том, что « … возникает потребность в методиках и практических инструментах тестирования ССЗИ … ». Данное утверждение представляется недостаточно обоснованным, поскольку критика применяемых при тестировании ССЗИ методик и инструментов не приведена.

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

3. Для оценки адекватности синтезируемого фонового трафика в работе используется показатель правдоподобия Херста. Не совсем понятно, что с точки зрения «природы» фонового трафика описывает указанный показатель? Достаточно ли проведения анализа только показателя правдоподобия, чтобы утверждать об адекватности синтезируемого трафика реальному.

4. В разделе «заключение» утверждается, что «Предложенное решение … позволяет достичь поставленной цели — повышения показателей защищенности ИТС за счет предупреждения компьютерных атак путем раннего выявления уязвимостей ССЗИ посредством их тестирования». При этом не конкретизируется, показатели какого (каких) процесса обеспечения безопасности объектов ИТС были улучшены, в результате каких экспериментов эти данные были подтверждены.

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:

Доктор военных наук, профессор
директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности
Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет»

Тел.: +7 (495) 246-05-55 доб. 231
e-mail: tyshuk@mirea.ru
Адрес: 119571, г. Москва, проспект Вернадского, д. 86

Лось Владимир Павлович