ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора Котенко Игоря Витальевича 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 определяется необходимостью обучения и тренировки специалистов в области информационной безопасности (ИБ), а также создания условий для проведения научных исследований в сфере обеспечения ИБ, в том числе для тестирования сетевых средств защиты информации (ССЗИ), обеспечивающих обнаружение, предупреждение и ликвидацию последствий компьютерных атак, а также реагирование на компьютерные инциденты. При этом возникает потребность в методиках и практических инструментах тестирования ССЗИ, которые позволят моделировать комплексные атакующие воздействия и условия их проведения в реальных компьютерных сетях.

Наблюдается объективное противоречие между потребностями по комплексному тестированию ССЗИ и существующим научно-методическим и математическим обеспечением систем и комплексов, реализующих тестирование ССЗИ, не удовлетворяющим 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.

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 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, 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. Результаты научного исследования 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 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 информационно-телекоммуникационных сетей (ИТС). Полученные научные результаты используются в ООО «Уральский центр систем безопасности», в Уральском федеральном университете имени первого Президента России Б.Н. Ельцина, в Екатеринбургском НТЦ 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 элементов обеспечения безопасности ИТС введены объекты тестирования - системы

обнаружения компьютерных атак (СОА), телекоммуникационное оборудование (ТКО), системы анализа защищенности (САЗ), а также информационно-аналитические системы безопасности (ИАСБ), составляющие ССЗИ. 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. Показано, что для обеспечения безопасности ИТС требуется проведение тестирования ССЗИ, для чего необходимы стенды, в которых на основе имитационного моделирования и синтеза массивов тестовых данных должна быть создана имитационная среда функционирования реальных ИТС.

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.

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. Использование в теме диссертации слово «синтез» предполагает, что в работе четко определены свойства, показатели и требования к исследуемому объекту, однако его свойства четко не определены. Также не определены показатели этих свойств и требования. В результате отсутствует четкая постановка задачи синтеза. Не понятно, на какие показатели накладываются ограничения, а какой показатель (какие показатели) следует оптимизировать (максимизировать или минимизировать). Соответственно, непонятно, к какому классу задач синтеза относится решаемая задача, можно или нельзя применять для ее решения известные методы.

2. В работе в недостаточной степени учитывается фактор Больших Данных. Не понятно, будут ли работать предлагаемые модели и методы в современных условиях, отличающиеся большими размерностями. Как известно, генетические алгоритмы (и не только они) чувствительны к увеличению размерности решаемой задачи. С недостаточной полнотой представлены сведения о времени, которое потребуется для использования предлагаемых методов. А это затрудняет понимание возможности использования предлагаемых решений по построению компьютерных полигонов в сфере информационной безопасности в существующих и перспективных автоматизированных информационных и телекоммуникационных системах.

3. Не достаточно полно представлен анализ степени достижения поставленной в работе прагматической цели, заключающейся в создании условий для повышения показателей защищенности объектов. Не совсем понятно, какие конкретно условия создаются при реализации научных результатов соискателя, каковы показатели защищенности объектов и насколько эти показатели при этом повышаются. Не в полной мере проведена верификация и валидация представленного метода синтеза массивов данных, что может привести к некорректности при их использовании.

4. Не в полной мере приведены сведения о проведении количественно-качественной оценки представленного комплекса, недостаточно подробно представлен анализ существующих киберполигонов, а также не описаны с необходимой детализацией аналоги аналогичных программно-аппаратных комплексов, не указаны требующие устранения недостатки. Поэтому вызывает затруднение оценка полученных результатов в отношении повышения качества работы компьютерных полигонов.

5. Соискатель указывает, что научная новизна работы заключается, в том числе, в создании « … методологии, основанной на ряде разработанных методов, моделей, алгоритмов и аппаратно-программного инструментария автоматизации процессов синтеза массивов данных для тестирования ССЗИ … ». Однако из текста не понятно, какие

численные параметры или качественные характеристики «тестовых массивов данных и сетевого трафика» улучшились благодаря автоматизации процессов их синтеза.

6. Совокупность выражений (1)-(11) в автореферате диссертации представляют собой интерактивную модель *M* сетевой среды функционирования ССЗИ, используемую для синтеза тестового сетевого трафика. Представляется целесообразным соотнести их, например, с рисунком 5, что обеспечило бы наглядность формирования и установки параметров сетевого трафика на всех этапах его синтеза.

Сделанные замечания имеют, в основном, 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 технических наук, профессор
главный научный сотрудник, руководитель лаборатории проблем компьютерной безопасности

Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН)

Тел.: +7 (812) 328 81 82
e-mail: ivkote1@mail.ru
Адрес: 199178, г. Санкт-Петербург, 14 линия В.О., д. 39

Котенко Игорь Витальевич

06 декабря 2022

Подпись д.т.н., профессора Котенко И.В. заверяю

Начальник отдела кадров
Л.В.Токарев
06 12 2022 г.