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

Концептуализация и 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 и практических исследований в сфере ИБ. При этом возникает потребность в методиках и практических инструментах тестирования ССЗИ, которые позволят моделировать комплексные компьютерные атаки и анализировать предпосылки к их возникновению 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 существенный научный результат диссертационной работы и ее 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, позволяющих 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, что в свою очередь обеспечивает возможность организации практико-ориентированного обучения специалистов по обнаружению, предупреждению и ликвидации последствий

компьютерных атак, а также по реагированию на инциденты ИБ, что в совокупности 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. В качестве рассматриваемого в работе результата приводится систематика компьютерных атак, вместе с тем в работе не указано, каким образом разработанная систематика соотносится с другими, аналогичными систематиками (н.р. с матрицей MITRE ATT@CK).

2. Представленный в автореферате метод синтеза атакующего воздействия и ситуационных задач предназначен для имитации реализации комплексной компьютерной атаки, построенной на базе алгоритмов сетей Петри, с учетом характеристик моделируемой информационно-телекоммуникационной системы, однако в качестве временных интервалов между элементарными тестирующими воздействиями выбираются случайные значения. Из текста автореферата непонятны подходы к определению необходимых характеристик плотности распределения ряда указанных значений и собственно характер функции плотности распределения, учитывающих характер комплексных компьютерных атак, их распределенность во времени и низкую стохастическую предсказуемость.

3. Состав средств защиты информации, используемых в сегментах описанного в автореферате киберполигона, требует уточнения, а также необходима детализация, каким требованиям должны удовлетворять упомянутые средства для обеспечения интеграции в данный киберполигон новых или тестируемых средств защиты информации.

Сделанные замечания имеют дискуссионный характер и безусловно не могут рассматриваться, как снижающие научную и практическую ценность рецензируемой по автореферату работы.

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.

Богданов Валентин Викторович:

Кандидат технических наук
Генеральный директор
ООО «УЦСБ»
Тел.: +7(343)379-98-34
e-mail: vbogdanov@ussc.ru
Адрес организации: 620100, Екатеринбург, Ткачей 6

_____ _____
(подпись) (дата)

Подпись _____ заверяю

ДАВЫДОВА А.В.
НАЧАЛЬНИК ОТДЕЛА ПЕРСОНАЛА