

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

В условиях цифровой трансформации вопросы, связанные с исследованием различных аспектов информационной безопасности, имеют важнейшее значение и с теоретической и практической точек зрения. Работа соискателя посвящена созданию киберполигонов в сфере информационной безопасности (далее — ИБ) и имеет двойное предназначение: во-первых, развивает теоретические положения чрезвычайно востребованного в современных условиях направления научных исследований в сфере ИБ моделирование сетевых средств защиты информации (далее — ССЗИ), во-вторых, предлагаемая методика может быть использована при обучении специалистов различного уровня. В работе сделан акцент на методиках и инструментальных средствах тестирования ССЗИ, которые позволят моделировать комплексные атакующие воздействия и условия их проведения в рамках реальных компьютерных сетей. При этом возникает естественная потребность в разработке и внедрении научной надстройки таких методик – методологии имитационного моделирования интерактивной сетевой среды с целью своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на инциденты ИБ. Поэтому актуальность научной проблемы не вызывает сомнения.

Судя по тексту автореферата наиболее существенным научным результатом диссертационной работы, его научная новизна состоит в решении проблемы, имеющей важное значение для народного хозяйства и заключающейся в создании научно-методического инструментария управления интерактивной сетевой средой учебно-научных компьютерных полигонов, позволяющего автоматизировать процессы синтеза тестовых массивов данных для тестирования ССЗИ с учетом многообразия сетевой среды и комплексного характера атакующего воздействия. Практическая значимость результатов диссертации заключается в том, что новое техническое решение – создание учебно-научных компьютерных полигонов позволяет не только автоматизировать процессы тестирования ССЗИ при имитации атакующего воздействия, имеющего комплексный характер, но и позволяет организовать практико-ориентированное обучение специалистов по обнаружению, предупреждению и ликвидации последствий компьютерных атак, а также по реагированию на инциденты ИБ в рамках всех требований федеральных государственных стандартов, что вносит значительный вклад в повышение безопасности компьютерных сетей.

На наш взгляд, работу значимо выделяют синтез эволюционно-генетического аппарата с методами и моделями, используемыми в машинном обучении и интеллектуальном анализе данных: цепи Маркова, нечетко-множественный подход и др.

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 автореферате при описании имитационно-статистического метода синтеза

массивов условно-реальных данных, моделирующих процесса взаимодействия пользователей ИТС не приводится информации об анализе соответствия сгенерированных данных реальным.

2. Из текста автореферата не ясно, кто и как интерпретирует результаты проведения кибератак на сетевую инфраструктуру, другими словами, имеет ли киберполигон интеллектуальную составляющую, позволяющую принимать те или иные решения?

Сделанные замечания имеют дискуссионный характер и 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.

1

09.11.2022

Назаров Дмитрий Михайлович
доктор экономических наук, доцент (докторская диссертация защищена по научной специальности 08.00.13 – Математические и инструментальные методы экономики)
заведующий кафедрой информационной безопасности
ФГБОУ ВО «Уральский государственный экономический университет»
Тел.: +73432831056
e-mail: dmi@usue.ru

Адрес организации: 620144, г. Екатеринбург, ул. 8 Марта/Народной Воли, д. 62/45;
официальный сайт: <https://www.usue.ru>; телефон: +7 (343) 283-11-07.

Подпись Назарова Дмитрия Михайловича заверяю

Директор Института цифровых технологий
управления и информационной безопасности
ФГБОУ ВО «Уральский государственный
экономический университет»



А.Ю. Коковихин