

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

Актуальность темы диссертационного исследования Синадского Николая Игоревича не вызывает сомнений, в условиях диверсификации экономической системы Российской Федерации на отраслевых предприятиях в промышленном и топливно-энергетическом секторах активно ведется работа по импортозамещению автоматизированных систем управления технологическими процессами (АСУ ТП), многие из которых в соответствии с Федеральным законом от 26 июля 2017 г. № 187 - ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» отнесены к объектам критической информационной инфраструктуры страны.

В рамках реализации Приказа Федеральной службы по техническому и экспортному контролю России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», необходимостью бесшовной интеграции информационно-управляющих систем существует потребность в разработке научно обоснованной методологии имитационного моделирования и оценке рисков при модернизации и дооснащение подсистем защиты информации АСУ ТП от угроз информационной безопасности (ИБ).

Создание киберполигонов в сфере информационной безопасности, предназначенных как для тестирования сетевых средств защиты информации (далее — ССЗИ), так и для проведения обучения специалистов — это активно развивающееся и чрезвычайно востребованное в современных условиях направление научных исследований в сфере ИБ.

Одной из отличительных особенностей компьютерных полигонов является использование полунатурного моделирования, когда часть систем моделируется с помощью математических (программных) моделей, а часть киберфизических систем (АСУ ТП) с помощью реального оборудования.

При этом возникает потребность в методиках и практических инструментах тестирования ССЗИ, которые позволят моделировать комплексные атакующие воздействия и условия их проведения 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 существенным научным результатом диссертационной работы Синадского Николая Игоревича, ее научная новизна состоит 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.

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 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. По нашему мнению, в автореферате недостаточно внимания уделено вопросу проверки адекватности предложенных автором математических моделей.
2. 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.

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.

Ведущий специалист по информационной безопасности
службы корпоративной безопасности
АО «Ачимгаз»
кандидат технических наук, доцент
тел.: +7(3494) 91-23-00 (доб. 549)
e-mail: e.dudorov@achimgaz.ru

Дудоров Евгений Николаевич

Начальник отдела управления персоналом
АО «Ачимгаз»

Першин Олег Александрович

22 ноября 2022 года

Подпись Дудорова Е.Н. заверяю.

629309, Ямало-Ненецкий автономный округ, г. Новый Уренгой, мкр. Славянский, д. 10
тел.: 8(3494) 91-23-07
e-mail: kancelyaria@achimgaz.ru