

ИНСТРУМЕНТАРИЙ ДЛЯ МОДЕЛИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННОЙ СРЕДЕ ВУЗА

А.М. Тюнина¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье рассматривается проблема моделирования угроз информационной безопасности в распределенной ИТ-среде вуза. Предлагаются конструктор сценариев инцидентов и генератор тестов, позволяющие формировать и воспроизводить различные векторы атак с учетом специфики образовательной инфраструктуры. Описываются модульная архитектура программного комплекса, методы генерации тестов и результаты апробации в условиях реального вуза.

Ключевые слова: моделирование угроз, информационная безопасность, конструктор сценариев, генератор тестов, распределенная ИТ-среда, вуз.

TOOLS FOR MODELING INFORMATION SECURITY THREATS IN A DISTRIBUTED UNIVERSITY ENVIRONMENT

A.M. Tyunina¹

¹Voronezh State University of Forestry and Technologies named after
G.F. Morozov

Abstract. The article discusses the problem of modeling information security threats in a distributed IT environment of a university. An incident scenario constructor and a test generator are proposed, which make it possible to generate and reproduce various attack vectors, taking into account the specifics of the educational infrastructure. The modular architecture of the software package, methods of test generation and the results of approbation in a real university are described.

Keywords: threat modeling, information security, scenario designer, test generator, distributed IT environment, university.

Современные вузы представляют собой сложные распределенные информационные системы, объединяющие территориально удаленные корпуса, разнородное оборудование и множество категорий пользователей. Статистика фиксирует устойчивый рост числа кибератак на образовательные учреждения, что обусловлено как значительными объемами персональных данных, так и спецификой академической среды - открытостью, сезонными колебаниями активности, использованием личных устройств. Существующие подходы к оценке защищенности, основанные на периодических аудитах, дают точечную картину, быстро теряющую актуальность. Цель работы - разработка конструктора сценариев инцидентов и генератора тестов для моделирования угроз в распределенной ИТ-среде вуза.

Информационная инфраструктура вуза обладает рядом специфических характеристик: территориальная распределенность, разнородность оборудования и ПО, множественность категорий пользователей (студенты, преподаватели, административный персонал, технические специалисты), исторически сложившаяся сегментация сети, сезонные факторы активности, наличие открытых сервисов и использование личных устройств (BYOD). Эти особенности требуют специализированного инструментария моделирования угроз. [1,2]

Комплекс строится по модульному принципу и включает:

- модуль управления сценариями (визуальное конструирование, библиотека сценариев);
- модуль генерации тестов (преобразование сценариев в воздействия);
- модуль интеграции с системами мониторинга (SIEM, IDS/IPS, DLP);
- модуль сбора результатов и формирования отчетности;
- модуль администрирования (управление доступом, настройка параметров).

Апробация проводилась в техническом вузе с распределенной инфраструктурой (6 корпусов, 12000 студентов, 1500 сотрудников). Сформировано 10 сценариев различных категорий. Результаты выявили: наличие сервисов с устаревшим ПО; 15% сотрудников открывают вложения от неизвестных отправителей; избыточные права доступа у ряда сотрудников; недостаточную изоляцию гостевого Wi-Fi. Апробация подтвердила работоспособность инструментария и его практическую значимость. [5,6]

Таблица 1. Основные модули программного комплекса и их функции

Модуль	Основные функции
Управления сценариями	Визуальное конструирование, редактирование, хранение сценариев
Генерации тестов	Преобразование сценариев в тестовые воздействия
Интеграции с СЗИ	Взаимодействие с SIEM, IDS/IPS, DLP
Сбора результатов	Аккумуляция данных тестирования, формирование отчетов
Администрирования	Управление доступом, настройка параметров

Разработаны конструктор сценариев инцидентов и генератор тестов для моделирования угроз в распределенной ИТ-среде вуза. Предложенная концепция базируется на модульном подходе к формированию сценариев. Апробация подтвердила способность инструментария выявлять уязвимости, неочевидные при традиционных подходах. Практическая значимость заключается в возможности регулярной оценки защищенности, выявления недостатков сегментации сети и проверки готовности персонала.

Список литературы

1. Сумин, В. И. Использование ситуационного моделирования в разработке систем принятия решений для сложных организационных систем / В. И. Сумин, А. С. Кравченко, А. В. Толкачев // Моделирование систем и процессов. – 2024. – Т. 17, № 3. – С. 71-79. – DOI 10.12737/2219-0767-2024-69-77. – EDN FBVHJO.
2. Петрова, Е. В. Моделирование процесса обнаружения угроз в распределенной информационной системе / Е. В. Петрова // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 061-063. – EDN PUOHUD.
3. Миняев, А. А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах / А. А. Миняев // Научные технологии в космических исследованиях Земли. – 2021. – Т. 13, № 2. – С. 52-65. – DOI 10.36724/2409-5419-2021-13-2-52-65. – EDN OJBVGU.
4. Ланкин, О. В. Моделирование систем защиты информации на основе временных аналитических баз данных / О. В. Ланкин, И. И. Застрожных, А. Д. Попов // Вестник Воронежского института МВД России. – 2025. – № 4. – С. 84-93. – EDN UVGUDO.

5. Баранов, В. В. Комплексная модель функционирования распределенных информационных систем в условиях деструктивного воздействия / В. В. Баранов // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2022. – № 5. – С. 51-67. – EDN USWVKZ.

6. Вульфин, А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных / А. М. Вульфин // Системная инженерия и информационные технологии. – 2023. – Т. 5, № 4(13). – С. 50-76. – DOI 10.54708/2658-5014-SIIT-2023-no3-p50. – EDN FJPFKC.

References

1. Sumin, V. I. The use of situational modeling in the development of decision-making systems for complex organizational systems / V. I. Sumin, A. S. Kravchenko, A.V. Tolkachev // Modeling of systems and processes. - 2024. – Vol. 17, No. 3. – pp. 71-79. – DOI 10.12737/2219-0767-2024-69-77. – EDN FBBHJO.

2. Petrova, E. V. Modeling of the threat detection process in a distributed information system / E. V. Petrova // Bulletin of the Voronezh Institute of High Technologies. – 2009. – No. 5. – pp. 061-063. – EDN PUOHUD.

3. Minyaev, A. A. Modeling information security threats in geographically distributed information systems / A. A. Minyaev // High-tech technologies in space exploration of the Earth. – 2021. – Vol. 13, No. 2. – pp. 52-65. – DOI 10.36724/2409-5419-2021-13-2-52-65. – EDN OJBGTGU.

4. Lankin, O. V. Modeling of information security systems based on temporary analytical databases / O. V. Lankin, I. I. Zastrozhnov, A.D. Popov // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. – 2025. – No. 4. – pp. 84-93. – EDN UVGUDO.

5. Baranov, V. V. Complex model of functioning of distributed information systems in conditions of destructive influence / V. V. Baranov // Electronic network political journal "Scientific works of KubSTU". – 2022. – No. 5. – pp. 51-67. – EDN USWVKZ.

6. Vulfin, A.M. Models and methods of integrated assessment of security risks of critical information infrastructure facilities based on data mining / A.M. Vulfin // System engineering and information technology. – 2023. – Vol. 5, No. 4(13). – pp. 50-76. – DOI 10.54708/2658-5014-SIIT-2023-no3-p50. – EDN FJPFKC.