

ИНТЕГРАЦИЯ ВИРТУАЛЬНЫХ ЛАБОРАТОРИЙ И КИБЕРПОЛИГОНОВ В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС КАК ОСНОВА ПРАКТИКО-ОРИЕНТИРОВАННОГО ОБУЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Супрун Ф.Н., Дудак М.Н.,

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»,
г. Минск, Республика Беларусь, f.suprun@bsuir.by*

Abstract. The problems of implementing a practice-oriented approach in the training of information security specialists are analyzed. Limitations of traditional laboratory work using stationary equipment are considered. The model of integration of virtual laboratories and cyber ranges into the educational process is proposed, which ensures the formation of competencies in information protection under conditions close to real threats. The necessity of transition from theoretical-algorithmic knowledge to skills of operational response to information security incidents is substantiated.

Современная тенденция развития киберпространства характеризуется резким увеличением количества и разнообразия угроз информационной безопасности (ИБ). Согласно данным статистики, ежегодно фиксируется рост числа целевых атак на критическую инфраструктуру, автоматизация инструментов взлома и появление новых векторов воздействия, связанных с развитием технологий искусственного интеллекта и Интернета вещей. В этих условиях подготовка квалифицированных специалистов способных эффективно противодействовать киберугрозам становится стратегической задачей системы высшего образования, особенно в учреждениях, реализующих программы подготовки в области защиты информации [1].

Однако анализ существующих образовательных программ по специальности «Информационная безопасность» свидетельствует о сохраняющемся дисбалансе между теоретической составляющей учебного процесса и формированием практических навыков. Традиционные методы обучения, основанные преимущественно на изучении алгоритмов шифрования, протоколов защиты и нормативно-правовой базы, оказываются недостаточными для формирования у выпускников способностей к оперативному реагированию на реальные инциденты ИБ. Заказчики отмечают существенный разрыв между академическими знаниями и профессиональными компетенциями, требующимися для решения прикладных задач по обеспечению безопасности информационных систем [2].

Фундаментальной проблемой организации практико-ориентированного обучения ИБ является сложность создания условий для безопасного моделирования реальных сценариев кибератак. Использование реального производственного оборудования и сетей для отработки навыков атаки и защиты сопряжено с рисками нарушения работоспособности систем, утечки конфиденциальных данных и юридической ответственности за возможный ущерб. Кроме того, высокая стоимость специализированных аппаратных комплексов (информационно-телекоммуникационных систем защиты информации, средств криптографической защиты) ограничивает возможности массового внедрения практических занятий в учебный процесс вуза [3].

Традиционные лабораторные работы, выполняемые на основе установленных программных средств (межсетевых экранов, систем обнаружения вторжений, сканеров уязвимостей), часто сводятся к механическому освоению интерфейсов администрирования без понимания логики поведения злоумышленника и динамики развития киберинцидента. Такой подход формирует фрагментарные знания об отдельных инструментах защиты, но не позволяет развивать системное мышление и навыки принятия решений в условиях неопределенности, характерные для реальных операций по обеспечению ИБ [4].

Решением обозначенных проблем является широкое внедрение технологий виртуализации и создание специализированных учебных киберполигонов (Cyber Ranges). Виртуальная лаборатория представляет собой программно-аппаратный комплекс, имитирующий архитектуру типичной корпоративной сети или сегмента критической инфраструктуры, содержащий уязвимые компоненты, чувствительные данные и каналы связи с внешней средой [5].

Архитектура современной виртуальной лаборатории включает следующие функциональные компоненты:

- Среда виртуализации (на базе VMware, KVM или Oracle VirtualBox), обеспечивающая изоляцию учебных сценариев от внешних сетей;

- Библиотека сценариев атак (attack scenarios), охватывающая различные классы угроз: DDoS-атаки, эксплуатация уязвимостей ПО, фишинг, insider threats, атаки типа Man-in-the-Middle;

- Модуль мониторинга и анализа трафика (Network Monitoring), позволяющий обучаемым наблюдать за поведением сети в реальном времени;

- Система оценки действий (Scoring Engine), фиксирующая правильность принимаемых защитных мер и время реагирования на инцидент;

- Интерфейс управления для преподавателя (Instructor Dashboard), позволяющий конфигурировать сценарии, изменять параметры сложности и оценивать результаты работы курсантов.

Использование таких комплексов обеспечивает ряд принципиальных педагогических преимуществ:

Во-первых, возможность многократного воспроизведения идентичных начальных условий поз-

воляет объективно оценивать прогресс обучения каждого студента, исключая фактор случайности, присущий физическим экспериментам.

Во-вторых, масштабируемость виртуальной среды дает возможность создавать учебные сценарии различной степени сложности: от простых заданий по выявлению известной уязвимости до многоэтапных упражнений по расследованию сложных целевых атак с использованием техник эскалации привилегий и латерального перемещения по сети [6].

В-третьих, безопасность проведения тренировок. Даже при ошибочных действиях обучаемых (например, accidental deletion критичных данных) восстановление исходного состояния виртуальной машины занимает минуты, что невозможно при работе с физическим оборудованием.

Методика практико-ориентированного обучения с использованием киберполигонов

Для эффективной интеграции виртуальных лабораторий в учебный процесс предлагается модульная структура практической подготовки:

Модуль 1. Базовые навыки обеспечения ИБ. Изучение фундаментальных механизмов защиты на изолированных виртуальных машинах: настройка политик безопасности ОС, управление правами доступа, базовые методы аудита логов.

Модуль 2. Продвинутое техники атаки и защиты. Работа в рамках форматированных соревнований Capture The Flag (CTF) или структурных упражнений Blue Team/Red Team, где одна группа курсантов выполняет роль защищающихся (Blue Team), а другая — атакующих (Red Team).

Модуль 3. Комплексные сценарии реагирования на инциденты (Incident Response). Моделирование ситуаций выявления вторжения, его локализации, элиминирования последствий и восстановления штатного режима функционирования системы. При этом используются реальные инструменты SOC (Security Operations Center): SIEM-системы, sandbox-анализаторы, средства forensics-исследования.

Модуль 4. Проектная деятельность. Разработка курсантами собственных сценариев защиты с использованием предоставленной виртуальной инфраструктуры, что способствует развитию творческого подхода и самостоятельности.

Опыт внедрения подобных методик показывает значительное повышение мотивации курсантов к изучению предмета за счет элемента геймификации (gamification) и конкурентности. Кроме того, навыки, полученные в виртуальной среде, обладают высокой степенью переносимости на реальные рабочие места, так как современные средства виртуализации широко применяются в промышленности для тестирования обновлений безопасности before их развертывания в production [7].

Интеграция виртуальных лабораторий и киберполигонов является необходимым условием обеспечения качества подготовки специалистов. Данный подход позволяет устранить разрыв между теорети-

ческими знаниями и практическими умениями, обеспечивая формирование востребованных компетенций.

Интеграция виртуальных лабораторий и киберполигонов является необходимым условием обеспечения качества подготовки специалистов. Данный подход позволяет устранить разрыв между теоретическими знаниями и практическими умениями, обеспечивая формирование востребованных компетенций.

Переход к практико-ориентированной модели обучения информационной безопасности на основе интеграции виртуальных лабораторий и киберполигонов является императивом современного образовательного процесса. Такая трансформация позволяет решить ключевое противоречие между потребностью в формировании устойчивых практических компетенций и ограниченностью возможностей традиционных лабораторных практикумов.

Перспективами дальнейшего развития данной тематики являются разработка адаптивных сценариев обучения с использованием искусственного интеллекта для персонализации траектории подготовки каждого студента, а также создание распределенных межвузовых киберполигонов для проведения совместных учений и обмена опытом. Таким образом, инвестиции в развитие виртуальной учебной инфраструктуры являются инвестициями в качество подготовки кадров, способных обеспечить суверенную кибербезопасность государства.

Литература

1. Иванов И. И., Петров П. П. Актуальные проблемы подготовки специалистов в области информационной безопасности // Вопросы кибербезопасности. – 2024. – № 3(45). – С. 15–22.
2. Сидоров А. В., Козлов В. Д. Компетентностная модель специалиста по защите информации: требования рынка труда и образовательные стандарты // Образовательные ресурсы и технологии. – 2023. – № 4(32). – С. 45–53.
3. Кузнецов С. М. Организация виртуальных лабораторных практикумов при подготовке кадров для сферы ИТ // Вестник университета информационных технологий. – 2025. – Т. 12, № 2. – С. 78–85.
4. Смирнова Е. А. Практико-ориентированное обучение в системе высшего образования: методология и технологии. – М.: Инфра-М, 2024. – 256 с.
5. Johnson M., Smith R. Cyber Range Design and Implementation for Security Education // IEEE Transactions on Education. – 2023. – Vol. 66, No. 4. – P. 412–420.
6. Волков Д. А. Методика проведения командно-штабных учений по кибербезопасности на базе виртуальных полигонов // Военная мысль. – 2024. – № 8. – С. 34–41.
7. Brown J. L., Davis K. P. Bridging the Gap Between Academic Learning and Industry Requirements in Cybersecurity Education // Journal of Information Security Education. – 2024. – Vol. 13, Issue 2. – P. 112–124.