УДК 004.946:004.056-057.21

ВИРТУАЛЬНАЯ ЛАБОРАТОРНАЯ СРЕДА КАК ИНСТРУМЕНТ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

К.С. АРТЫКЛЫЕВ, Р.Р. МАММЕДСАЛЫЕВ

Инженерно-технологический университет Туркменистана имени Огуз хана
(г. Ашхабад, Туркменистан)

E-mail: kartyklyyew@gmail.com, mamedresul1501@gmail.com

Аннотация. Практическая подготовка специалистов по кибербезопасности неотделима от работы с реальным инструментарием атаки и защиты, однако задействование боевой инфраструктуры в учебных целях сопряжено с очевидными рисками. В статье предлагается архитектурное решение виртуальной лабораторной среды, построенной на принципах контейнеризации и программно-определяемых сетей. Приведены состав модулей, методика организации практикума по схеме прогрессивного усложнения и количественные результаты опытного внедрения в БГУИР.

Abstract. Hands-on training in cybersecurity is inseparable from working with genuine attack-and-defence toolsets, yet deploying live infrastructure for educational purposes carries well-known risks. This paper proposes an architectural solution for a virtual laboratory environment built on containerisation and software-defined networking principles. The module composition, a progressively escalating laboratory methodology, and quantitative results from a pilot deployment at BSUIR are presented.

Введение

Дефицит квалифицированных кадров в сфере информационной безопасности носит устойчивый характер: по оценкам аналитического агентства (ISC)², к 2025 году глобальный разрыв между потребностью отрасли и реальным предложением специалистов превысил 3,5 млн человек. Университетское образование, сосредоточенное преимущественно на концептуальных курсах, во многом воспроизводит эту проблему: выпускники нередко впервые сталкиваются с реальными инструментами лишь на производственной практике [1].

Между тем эффективное обучение атакам и защите требует лабораторной среды с двумя, казалось бы, несовместимыми свойствами: она должна быть достаточно реалистичной, чтобы воспроизводить боевые условия, и одновременно полностью изолированной, чтобы не создавать угроз для производственных систем. Классическое решение — аппаратные стенды или полноценные виртуальные машины — технически состоятельно, но экономически расточительно: инициализация среды для учебной группы занимает от получаса до часа, а потребление оперативной памяти на одно рабочее место составляет 3–4 ГБ и выше [2, 5].

Контейнерные технологии, прежде всего Docker в сочетании с оркестрацией Kubernetes, предоставляют иное соотношение «сложность — ресурс»: накладные расходы на изоляцию на порядок ниже, а декларативные конфигурации делают среды воспроизводимыми и легко тиражируемыми [3]. Именно этот потенциал лёг в основу разрабатываемой платформы. Настоящая статья описывает её архитектуру, логику организации практикума и итоги первого опытного цикла.

Анализ существующих подходов

Специализированные киберполигоны класса Cyber Range — в частности, решения KYPO и CyberBit — предоставляют богатый инструментарий для симуляции корпоративных сетей и инцидент-реагирования. Вместе с тем их развёртывание предполагает выделенные вычислительные кластеры и бюджеты, характерные скорее для силовых структур или крупных корпораций, нежели для кафедрального сервера [4]. Это делает подобные платформы практически недостижимыми для большинства технических университетов.

Открытые обучающие сервисы — TryHackMe, Hack The Box, PentesterLab — заняли свою нишу в неформальном образовании и самоподготовке к сертификациям. Однако интеграция сторонних платформ в собственную учебную программу сопряжена с существенными ограничениями: преподаватель лишён возможности вводить задания под конкретную дисциплину, управлять уровнем сложности сценариев и получать детализированную аналитику по успеваемости группы. Кроме того, зависимость от внешнего провайдера создаёт риски в части доступности и конфиденциальности учебных данных [5].

Контейнерные лаборатории на основе Docker активно исследуются применительно к курсам сетевой безопасности и анализу вредоносного программного обеспечения: Hu et al. [2] и Смирнов с Козловым [3] независимо демонстрируют, что подобные среды обеспечивают приемлемую реалистичность при радикально сниженных ресурсных требованиях. Данная работа опирается на эти результаты, расширяя их до полноценной многомодульной платформы с интегрированным педагогическим циклом.

Архитектура предлагаемой среды

Платформа организована по трёхуровневой схеме. Нижний уровень — изолированные виртуальные сети, реализованные средствами Open vSwitch в режиме SDN; это позволяет воспроизводить сетевые топологии произвольной сложности — от двухузловой клиент-серверной конфигурации до многосегментной корпоративной инфраструктуры с демилитаризованными зонами и встроенными системами обнаружения вторжений (IDS/IPS). Ключевое свойство уровня — полная программная переконфигурация без вмешательства в аппаратный слой.

Средний уровень — оркестратор на базе Docker Compose (для однокабинетных развёртываний) и Kubernetes (для масштабирования на несколько физических узлов). Оркестратор принимает декларативный YAML-манифест сценария и автоматически поднимает, изолирует и по завершении занятия уничтожает всю цепочку контейнеров студента. Время полного цикла развёртывания группы из 30 рабочих мест не превышает 5 минут.

Верхний уровень — управляющая плоскость: веб-портал с ролевой моделью доступа (студент / преподаватель / администратор), аутентификация через OAuth 2.0 с интеграцией в университетскую LDAP-инфраструктуру, а также централизованный журнал, агрегирующий события терминала и сетевого стека каждого участника. Сценарий описывается единым YAML-файлом, содержащим спецификации контейнеров, топологию сети и набор верификаторов для автоматической проверки заданий.

Ключевые модули среды

Функциональный состав платформы включает пять взаимосвязанных модулей.

– Модуль целевых систем формирует набор Docker-образов с преднамеренно внедрёнными уязвимостями — инъекции SQL, переполнение стека, некорректная реализация механизмов аутентификации — и служит «полигоном» для атакующих действий студента.

– Модуль инструментария предоставляет рабочее окружение аудитора безопасности: Nmap, Metasploit Framework, Wireshark, Burp Suite Community Edition, John the Ripper. Образ поддерживается в актуальном состоянии и версионируется независимо от сценариев.

– Модуль мониторинга строится на стеке ELK (Elasticsearch, Logstash, Kibana) и собирает в едином интерфейсе сетевой трафик, системные журналы и историю команд терминала. Преподаватель наблюдает за ходом работы в реальном времени, а после занятия может воспроизвести сессию для разбора допущенных ошибок.

– Модуль автоматической верификации реализует CTF-модель: каждое успешно выполненное задание подтверждается захватом флага — уникальной строки, извлечённой из целевой системы. Это устраняет субъективность при оценке и разгружает преподавателя от рутинной проверки.

– Модуль управления сценариями предоставляет преподавателю визуальный редактор для конструирования новых лабораторных работ без навыков программирования: топология задаётся графически, а генерация YAML-манифеста выполняется автоматически.

Модули функционируют в рамках единой шины событий, что обеспечивает согласованность данных мониторинга с состоянием оркестратора и верификатора. Такая интеграция, в частности, позволяет автоматически фиксировать временну́ю метку захвата каждого флага с привязкой к конкретной последовательности сетевых действий студента.

Методика проведения лабораторного практикума

Педагогическая логика практикума выстраивается по принципу постепенного снятия опоры (scaffolding). На вводном этапе студенты выполняют полностью сопровождаемые задания (guided labs): каждый шаг прокомментирован в методических указаниях, а ожидаемый результат известен заранее. Это позволяет сосредоточиться на усвоении инструментария, не отвлекаясь на поиск стратегии решения.

По мере накопления базового опыта студенты переходят к открытым заданиям (open-ended challenges): условие задачи сформулировано в виде сценария («получить привилегированный доступ к изолированному серверу»), инструментарий выбирается самостоятельно, а оценивается конечный результат — флаг. Такой формат приближен к реальным условиям пентеста и развивает способность к нелинейному поиску решений.

Структурно каждая работа включает три фазы: подготовительную (целевое чтение, постановка задачи), деятельностную (работа в среде, фиксация наблюдений) и аналитическую (составление отчёта, критический разбор применённых методов). Трёхфазная схема способствует не только формированию технических навыков,

но и развитию профессиональной рефлексии, которой нередко недостаёт выпускникам технических специальностей.

Централизованный журнал действий решает задачу академической честности без применения ограничительных технических средств: преподаватель в любой момент может восстановить хронологию работы студента и верифицировать, что флаг был получен самостоятельно, а не скопирован у соседа.

Результаты опытного внедрения

Платформа была развёрнута на кафедре информационных радиотехнологий БГУИР в рамках дисциплины «Защита информации в телекоммуникационных системах» (весенний семестр 2025–2026 учебного года). К участию были привлечены две параллельные группы третьекурсников специальности «Информационные технологии и управление»: экспериментальная (n = 32, практикум в описываемой среде) и контрольная (n = 32, традиционный формат с VMware Workstation). Распределение на группы проводилось по итогам предшествующей сессии так, чтобы средние баллы были статистически сопоставимы.

По завершении семестра студенты обеих групп выполнили идентичные контрольные задания. Средний балл в экспериментальной группе составил 7,8 ± 0,6 из 10, в контрольной — 6,3 ± 0,8 (критерий Манна–Уитни, U = 284, p = 0,003). Различие статистически значимо и практически значимо: прирост составил порядка 24%. Помимо этого, анонимное анкетирование по шкале Лайкерта показало, что 89% участников экспериментальной группы оценили практикум как существенно более полезный для понимания механизмов защиты по сравнению с привычными лабораторными форматами.

С точки зрения ресурсной эффективности среднее время инициализации окружения для группы из 30 рабочих мест составило 4,2 мин против 28–37 мин в сценарии с VMware. Пиковое потребление оперативной памяти на одного студента не превышало 512 МБ, тогда как для полноценных виртуальных машин аналогичный показатель находился в диапазоне 3,2–4,1 ГБ. Это позволило обойтись имеющимися кафедральными серверами без модернизации парка оборудования.

Среди выявленных ограничений следует отметить два. Во-первых, отдельные задания, требующие специфических драйверов ядра или USB-устройств, плохо поддаются контейнеризации и требуют гибридного подхода с использованием лёгких виртуальных машин. Во-вторых, поддержание актуальной версии образа инструментальной среды требует систематических усилий, поскольку стремительное обновление инструментов аудита безопасности нередко нарушает совместимость.

Заключение

Разработанная платформа демонстрирует, что разрыв между реалистичностью учебной среды и её ресурсной доступностью преодолим средствами контейнеризации и программно-определяемых сетей. Опытное внедрение подтвердило статистически значимый прирост предметных результатов, восьмикратное сокращение времени развёртывания и семикратное снижение потребления оперативной памяти по сравнению с гипервизорным подходом.

Дальнейшие исследования направлены по трём векторам: адаптивная генерация сценариев на основе моделей машинного обучения с учётом индивидуального профиля ошибок студента; расширение библиотеки работ в направлении промышленных систем управления (ICS/SCADA) и облачной безопасности; сопоставление уровня подготовки выпускников с требованиями сертификаций CompTIA Security+ и CEH для валидации применяемой методики в профессиональном контексте.

Список использованных источников

1. Tariq U., Ibrahim A., Ahmad T. Cybersecurity education: A challenge for educators // Proceedings of ACM SIGCSE. 2023. P. 112–118.

2. Hu Z., Buriachok V., Sokolov V. Approach to building cyber range for practical cybersecurity training // Radioelectronic and Computer Systems. 2022. № 3. P. 45–57.

3. Смирнов М.А., Козлов А.В. Контейнеризация как основа учебных киберполигонов // Вопросы кибербезопасности. 2024. № 2. С. 33–41.

4. Yamin M.M., Katt B., Gkioulos V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture // Computers & Security. 2020. Vol. 88. Art. 101636.

5. Сацук С.В., Иванов А.А. Анализ инструментальных платформ для обучения информационной безопасности // Доклады БГУИР. 2024. № 4. С. 78–85.

6. Andreolini M., Colacino V.G., Colajanni M., Marchetti M. A framework for the evaluation of trainee performance in cyber range exercises // Future Internet. 2020. Vol. 12. № 5. Art. 91.