АКТУАЛЬНОСТЬ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ТРЕНИРОВОК СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ: РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Пучков Е.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Савицкий А.Ю. – кандидат военных наук

Аннотация. В работе обоснована необходимость проведения практических тренировок специалистов по кибербезопасности в Вооруженных Силах Республики Беларусь и представлена архитектура разрабатываемого веб-приложения, обеспечивающего автоматизацию данных тренировок. Создаваемое программное средство позволяет моделировать кибератаки, оценивать действия специалистов, вести учет результатов и формировать отчеты, учитывая специфику военных задач, что не в полной мере реализовано в существующих аналогах.

В условиях возрастания числа киберугроз и перехода военных структур на цифровые технологии особое внимание уделяется подготовке высококвалифицированных специалистов по кибербезопасности. В Вооруженных Силах Республики Беларусь проведение практических тренировок (отработка выявления, анализа и отражения кибератак) является критически важным элементом боевой подготовки. Однако существующие методы тренировок зачастую не автоматизированы, не позволяют оперативно создавать реалистичные сценарии атак. Это приводит к снижению эффективности подготовки и увеличивает время на развертывание тренировочной среды.

Анализ доступных аналогов показал, что они не обеспечивают необходимый уровень безопасности и изоляции, имеют ограниченные возможности по интеграции с существующими информационными системами, не поддерживают специфические для военной сферы сценарии. Кроме того, в большинстве решений отсутствует гибкая система оценки действий обучаемого. В связи с этим разработка собственного специализированного веб-приложения является актуальной и практически значимой задачей.

В ходе выполнения работы проектируется веб-приложение, реализующее следующие основные функции:

– аутентификация и авторизация пользователей с ролями «тренер» (руководитель тренировки), «специалист» (курсант/офицер), «администратор»;

– создание и управление тренировочными сценариями (виртуальные сети с заданными уязвимостями, симуляция атакующих действий);

– автоматизированная проверка выполнения заданий (захват флагов, обнаружение инцидентов, написание отчетов);

– ведение личного кабинета с историей тренировок, результатами и динамикой прогресса;

– генерация отчетов о результатах тренировки в формате PDF с графиками успеваемости;

– безопасное хранение данных в PostgreSQL, контейнеризация с помощью Docker.

Архитектура разрабатываемого программного средства строится с использованием языка Java, фреймворка Spring Boot (Spring Security, Spring Data JPA), системы сборки Maven. Для моделирования тренировочных сред планируется применение технологий виртуализации (Docker, Kubernetes). Такой подход обеспечивает изоляцию процессов, масштабируемость и возможность быстрого развертывания на серверах Министерства обороны.

Разрабатываемое веб-приложение позволит повысить качество практической подготовки специалистов по кибербезопасности за счет регулярных автоматизированных тренировок с реалистичными сценариями, сократить временные затраты на организацию и проведение занятий, обеспечить объективность оценки и детальный анализ действий каждого военнослужащего. Применение собственной разработки гарантирует учет всех требований военного ведомства и возможность доработки функционала в ходе эксплуатации. Дальнейшее развитие системы предполагает интеграцию с существующими системами управления обучением военных учебных заведений, внедрение элементов искусственного интеллекта для адаптивной генерации сценариев под уровень подготовки специалиста, а также создание распределенного полигона для проведения совместных тренировок подразделений кибербезопасности.

Список использованных источников:

1. Spring Boot Documentation [Электронный ресурс]. – Электронные данные. – Режим доступа: https://docs.spring.io/spring-boot/docs/current/reference/html/. – Дата доступа: 28.03.2026.

2. NIST SP 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf. – Дата доступа: 28.03.2026.