Министерство образования Республики Беларусь

Учреждение образования
Белорусский государственный университет информатики и радиоэлектроники

УДК 004.779-049.5

Хомярчук
Михаил Викторович

Проектирование и разработка обучающей системы управления безопасностью веб-приложений для защиты от веб-уязвимостей

АВТОРЕФЕРАТ
на соискание степени магистра

по специальности 7-06-0612-02 – Информатика и технологии программирования

Научный руководитель
Чернявский Ю.А.
к.т.н., доцент

Минск 2026

КРАТКОЕ ВВЕДЕНИЕ

В условиях стремительного развития веб-технологий и повсеместного внедрения веб-приложений в различные сферы деятельности вопросы информационной безопасности приобретают особую актуальность. Современные веб-приложения используются в электронной коммерции, банковском секторе, образовании, государственных информационных системах и других критически важных областях, что делает их привлекательной целью для злоумышленников. Несмотря на наличие стандартов, рекомендаций и инструментов защиты, веб-уязвимости по-прежнему остаются одной из основных причин инцидентов информационной безопасности.

Одной из ключевых проблем в данной области является недостаточная практическая подготовка разработчиков к вопросам веб-безопасности. Во многих образовательных программах и корпоративных курсах обучение носит преимущественно теоретический характер и не обеспечивает формирования устойчивых навыков выявления и устранения уязвимостей в реальных условиях разработки. Особенно остро данная проблема проявляется в контексте front-end разработки, где значительная часть логики приложения переносится на клиентскую сторону, а вопросы безопасности нередко воспринимаются как второстепенные.

Существующие практико-ориентированные платформы для обучения веб-безопасности, такие как намеренно уязвимые приложения и лабораторные среды, обладают рядом ограничений, включая высокий порог входа, сложность развёртывания и ориентацию на узкую аудиторию специалистов по тестированию безопасности. Это снижает их доступность для разработчиков, стремящихся получить базовые и прикладные знания в области безопасной веб-разработки.

В связи с этим актуальной является задача разработки обучающей системы, ориентированной на практическое освоение веб-уязвимостей, обладающей низким порогом входа, наглядным пользовательским интерфейсом и интерактивным форматом обучения. Такая система должна обеспечивать поэтапное изучение уязвимостей, предоставлять немедленную визуальную обратную связь и способствовать формированию причинно-следственных связей между действиями разработчика и возникающими рисками безопасности.

Целью данной магистерской диссертации является проектирование и разработка интерактивной обучающей системы управления безопасностью веб-приложений, направленной на формирование практических навыков выявления и устранения веб-уязвимостей у front-end разработчиков. Для достижения поставленной цели в работе проведён анализ основных классов веб-

уязвимостей, рассмотрены существующие подходы к обучению веб-безопасности, сформированы требования к обучающей системе, спроектирована её архитектура и реализована обучающая платформа HackShield Academy.

Практическая значимость работы заключается в возможности использования разработанной системы в образовательном процессе, а также в рамках самостоятельного обучения разработчиков основам безопасной веб-разработки. Предложенный подход ориентирован на сочетание теоретических знаний и практического опыта, что позволяет повысить эффективность обучения и способствует формированию устойчивых навыков в области веб-безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является проектирование и разработка обучающей системы управления безопасностью веб-приложений, ориентированной на практическое освоение веб-уязвимостей и формирование навыков их предотвращения.

Для достижения поставленной цели в работе решены следующие задачи:

– проведён анализ основных классов веб-уязвимостей и особенностей их возникновения в современных веб-приложениях;

– исследованы существующие подходы и обучающие платформы в области веб-безопасности, выявлены их достоинства и ограничения;

– сформированы требования к обучающей системе с учётом специфики целевой аудитории;

– спроектирована архитектура обучающей системы и определён используемый программный стек;

– реализована интерактивная обучающая платформа с поддержкой уровней обучения, системы формирования прогресса пользователя и административного функционала;

– проведена апробация разработанной системы и оценена её практическая применимость.

Объектом исследования являются процессы обучения веб-безопасности в контексте современной веб-разработки.

Предметом исследования являются методы, средства и программные решения, обеспечивающие практико-ориентированное обучение выявлению и предотвращению веб-уязвимостей.

Методы исследования

В процессе выполнения работы использованы методы анализа и обобщения научно-технической литературы, сравнительный анализ существующих обучающих платформ, методы системного проектирования программного обеспечения, а также практические методы разработки и тестирования веб-приложений.

Личный вклад соискателя

Результаты, приведённые в диссертации, получены соискателем лично. Вклад научного руководителя Ю. А. Чернявского заключается в формулировке целей и задач исследования.

ОСНОВНОЕ СОДЕРЖАНИЕ

В первой главе магистерской диссертации рассматриваются теоретические аспекты обеспечения безопасности веб-приложений, а также анализируются основные классы веб-уязвимостей, представляющие наибольшую угрозу для современных информационных систем. Особое внимание уделено причинам возникновения уязвимостей, связанным с особенностями архитектуры веб-приложений, обработкой пользовательского ввода и взаимодействием клиентской и серверной частей.

В рамках главы проанализированы наиболее распространённые веб-уязвимости, включая межсайтовое выполнение сценариев (XSS), межсайтовую подделку запросов (CSRF), небезопасные прямые ссылки на объекты (IDOR), серверные подделки запросов (SSRF), а также уязвимости, связанные с некорректной обработкой данных. Рассмотрены типовые сценарии эксплуатации данных уязвимостей и возможные последствия их использования злоумышленниками.

Отдельное внимание уделено анализу статистических данных и отчётов в области информационной безопасности, демонстрирующих устойчивую тенденцию к сохранению и повторяемости типовых веб-уязвимостей в реальных проектах. Что подтверждает необходимость не только теоретического изучения принципов безопасной разработки, но и формирования практических навыков у разработчиков.

Также проведён обзор существующих подходов к обучению веб-безопасности. Проанализированы как теоретические курсы и учебные материалы, так и практико-ориентированные платформы, предлагающие лабораторные задания и симуляции атак. По результатам анализа выявлены основные ограничения существующих решений, связанные с высоким порогом входа, сложностью развёртывания и недостаточной ориентацией на разработчиков, не обладающих специализированной подготовкой в области информационной безопасности.

Вторая глава посвящена проектированию обучающей системы HackShield Academy и описанию концептуальных, архитектурных и педагогических решений, положенных в основу разработанной платформы.

В рамках главы сформированы функциональные и нефункциональные требования к обучающей системе с учётом специфики целевой аудитории — web и front-end разработчиков. При формировании требований особое внимание уделено доступности системы, минимальному порогу входа, возможности поэтапного освоения материала и наличию наглядной обратной связи.

При проектировании обучающей системы был учтён опыт интерактивных образовательных платформ, демонстрирующих эффективность обучения в формате пошаговых заданий с постепенным усложнением. Подобный подход позволяет пользователю без предварительной подготовки приступить к выполнению заданий, постепенно осваивая новые концепции и закрепляя полученные знания на практике. Использование элементов геймификации и квестовой структуры обучения способствует повышению мотивации и вовлечённости обучающихся.

Архитектура обучающей системы спроектирована с использованием современных веб-технологий и предусматривает разделение клиентской и серверной частей. Клиентская часть реализована с использованием фреймворка Next.js, что обеспечивает удобство разработки, расширяемость и возможность дальнейшего развития платформы. Серверная часть реализована в виде отдельного backend-приложения, отвечающего за обработку пользовательских данных, хранение результатов обучения и реализацию административного функционала.

В рамках главы также описана система управления прогрессом пользователей. Особенностью разработанной платформы является возможность использования системы без обязательной регистрации с сохранением прогресса в локальном хранилище браузера. При последующей регистрации пользователя предусмотрен механизм синхронизации локального прогресса с серверной частью системы, что повышает удобство использования и снижает барьер входа для новых пользователей.

Дополнительно рассмотрен административный функционал системы, предназначенный для анализа результатов обучения пользователей и контроля их активности. Наличие административных прав позволяет использовать разработанную платформу в образовательном процессе, в том числе в рамках учебных курсов и практических занятий.

Третья глава магистерской диссертационной работы посвящена практической реализации обучающей системы HackShield Academy, и оценке ее функциональных возможностей.

В рамках главы подробно описан процесс реализации архитектуры обучающей системы с учётом ранее сформулированных требований. Клиентская часть системы реализована в виде веб-приложения с использованием фреймворка Next.js, что обеспечивает высокую производительность, модульность и удобство расширения функционала.

Серверная часть системы реализована в виде отдельного backend-приложения, разработанного с использованием фреймворка NestJS. Backend отвечает за обработку пользовательских запросов, хранение данных о пользователях и результатах прохождения уровней, а также за реализацию механизмов аутентификации и разграничения прав доступа. Для хранения данных используется документоориентированная база данных MongoDB, размещённая в облачной среде, что обеспечивает масштабируемость и надёжность хранения информации.

Особое внимание в третьей главе уделено реализации логики обучающих уровней. Все уровни платформы построены по единому принципу и представляют собой интерактивные задания, моделирующие типовые сценарии возникновения веб-уязвимостей. В целях упрощения восприятия и обеспечения безопасности выполнения заданий используется так называемый «декоративный» уровень моделирования, при котором пользователь получает наглядное представление о механизмах атак и уязвимостей без необходимости развёртывания реальной уязвимой инфраструктуры. Такой подход позволяет сосредоточиться на понимании принципов работы уязвимостей и методах их предотвращения.

В процессе прохождения уровней пользователь выполняет задания, направленные на выявление и устранение уязвимостей, а также отвечает на контрольные вопросы, позволяющие оценить степень усвоения материала. За успешное выполнение заданий начисляются баллы, формирующие общий показатель прогресса пользователя. Наличие системы оценки и визуальной обратной связи способствует повышению мотивации и вовлечённости обучающихся.

Также описана реализация механизма сохранения прогресса пользователей. Платформа предоставляет возможность использования без предварительной регистрации с сохранением результатов в локальном хранилище браузера. При последующей регистрации пользователя реализован механизм синхронизации локального прогресса с серверной частью системы, что позволяет сохранить достигнутые результаты и продолжить обучение без потери данных. Данный подход повышает доступность платформы и снижает барьер входа для новых пользователей.

Отдельное внимание уделено реализации административного интерфейса, предназначенного для анализа результатов обучения пользователей. Административная часть системы позволяет просматривать статистику прохождения уровней, анализировать успешность выполнения заданий и использовать полученные данные в образовательных целях. Наличие подобного функционала делает возможным применение платформы не только для самостоятельного обучения, но и в рамках учебного процесса.

Реализованная система демонстрирует практическую применимость и может быть использована в качестве основы для дальнейшего развития и расширения функциональности.

Научная новизна магистерской диссертационной работы заключается в разработке обучающей системы управления безопасностью веб-приложений,

ориентированной на практико-ориентированное освоение веб-уязвимостей с использованием интерактивного и квестового формата обучения. В отличие от существующих решений, разработанная система ориентирована преимущественно на web- и front-end разработчиков и не требует специализированной подготовки в области информационной безопасности.

В работе предложен подход к обучению веб-безопасности, основанный на моделировании типовых сценариев уязвимостей в упрощённой, контролируемой среде, что позволяет сосредоточить внимание обучающихся на понимании принципов возникновения и предотвращения уязвимостей. Дополнительной особенностью является сочетание анонимного режима использования системы с возможностью последующей синхронизации прогресса пользователя при регистрации, что снижает порог входа и повышает удобство обучения.

Практическая значимость работы

Практическая значимость магистерской диссертационной работы заключается в возможности использования разработанной обучающей системы HackShield Academy для самостоятельного обучения веб-разработчиков основам безопасной разработки веб-приложений. Реализованная платформа может быть использована в качестве дополнительного учебного инструмента при изучении дисциплин, связанных с веб-разработкой и информационной безопасностью.

Функциональные возможности системы, включая систему уровней, контрольные вопросы, визуальную обратную связь и административный интерфейс, позволяют применять разработанную платформу в образовательном процессе для оценки прогресса обучающихся и анализа результатов обучения. Архитектура системы обеспечивает возможность её дальнейшего расширения и адаптации под различные учебные программы и сценарии использования.

Апробация и внедрение результатов работы

Результаты апробации магистерской диссертационной работы проводились в форме функционального тестирования и практической проверки реализованных сценариев обучения, а также могут быть использованы в учебном процессе при подготовке специалистов в области веб-разработки и информационной безопасности. Разработанная обучающая система ориентирована на практическое применение и обладает потенциалом для внедрения в образовательные курсы и практические занятия, а также для использования в рамках самостоятельного обучения разработчиков.

Гибкость архитектуры и модульный подход к реализации позволяют адаптировать систему под различные требования образовательных программ и расширять её функциональные возможности с учётом специфики учебного процесса.

Структура и объём работы

Магистерская диссертационная работа состоит из введения, трёх глав, заключения, списка использованных источников и приложений. Общий объем работы составляет 81 страницу, из которых основного текста – 51 страница, 20 рисунков на 17 страницах, списка использованных источников из 38 наименований на 3 страницах и 3 приложений на 15 страницах.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1- А. М.В. Хомярчук, Современные тенденции и инновации в обеспечении веб-безопасности: вызовы, решения и перспективы/ Ю.А.Чернявский, М.В. Хомярчук, // Актуальные вопросы современной науки и образования: материалы 8-ой международной научно-практической конференции. – Пенза, 2023. – с. 28-33.

2- А. М.В. Хомярчук, Алгоритмы машинного обучения для проактивного мониторинга веб-приложений/ Ю.А.Чернявский, М.В. Хомярчук, // Актуальные вопросы современной науки и образования: материалы 2-ой международной научно-практической конференции. – Пенза, 2025. – с. 21-24.

3- А. М.В. Хомярчук, Влияние новых стандартов (http/3, quic, webassembly) на веб-безопасность/ Ю.А.Чернявский, М.В. Хомярчук, // Актуальные вопросы современной науки и образования: материалы международной научно-практической конференции состоявшейся 10 октября 2025 г. – Пенза, 2023. – с. 42-45.