УДК 004.056

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ВЕБ-СЕРВИСОВ НА НАЧАЛЬНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА СТАРТАПА

Шнайдер К.С.[1] (студент)
Научный руководитель – доктор технических наук, доцент Митрохин М.А.[1]
1 – Пензенский государственный университет
e-mail: Knhn0@yandex.ru

Введение. В условиях активного развития цифровых технологий веб-сервисы являются важнейшим компонентом современных информационных систем. Стартап-проекты ориентированы на быстрое создание и внедрение программных решений. На начальных этапах разработки основной задачей является реализация функциональности и обеспечение работоспособности минимально жизнеспособного продукта. При этом вопросам информационной безопасности зачастую уделяется недостаточное внимание, что приводит к повышенному риску реализации угроз и эксплуатации уязвимостей.

Основная часть. В рамках исследования будут рассмотрены минимальные рабочие прототипы, разработанные в рамках реализации стартап-проектов. Предметом исследования выступают угрозы информационной безопасности веб-сервисов и способы их предотвращения с использованием доступных защитных механизмов.

Согласно современным исследованиям и рекомендациям в области безопасности веб-приложений, значительная часть успешных атак связана с наличием типовых уязвимостей, описанных в проекте OWASP Top 10 [1]. К ним относятся нарушения контроля доступа, уязвимости аутентификации, инъекционные атаки, межсайтовое выполнение сценариев и ошибки конфигурации безопасности. Данные уязвимости возникают из-за недостаточной проверки входных данных, некорректной реализации механизмов авторизации, а также использования небезопасных программных компонентов.

Особенностью стартап-проектов является ограниченность ресурсов и высокая скорость разработки. Эти факторы достаточно сильно затрудняют внедрение комплексных систем защиты. В связи с этим особое значение приобретают базовые меры защиты. В рамках стартап-проекта они позволяют снизить риски без существенного увеличения затрат. К таким мерам относятся использование защищенного протокола передачи данных HTTPS, применение надежных механизмов аутентификации и авторизации, валидация входных данных, использование современных фреймворков с встроенными средствами защиты, а также регулярное обновление программных компонентов [2, 3].

Важным элементом обеспечения безопасности является соблюдение принципа минимальных привилегий и ограничение доступа пользователей к критическим ресурсам системы. Реализация указанных мер позволяет существенно повысить устойчивость веб-сервиса к типовым атакам и снизить вероятность компрометации данных.

Выводы. Обеспечение информационной безопасности должно рассматриваться как важная часть процесса разработки веб-сервиса с самых ранних этапов его жизненного цикла. Применение базовых защитных механизмов позволяет значительно повысить уровень защищенности системы и снизить риски реализации угроз.

Список использованных источников:

1. OWASP Foundation. OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks [Электронный ресурс]. URL: https://owasp.org/www-project-top-ten/ (дата обращения: 06.02.2026).
2. NIST. Secure Software Development Framework (SSDF). — NIST SP 800-218, 2022.
3. Зенков А. В. Информационная безопасность и защита информации. — М.: Юрайт, 2024.
4. Щербак А. В. Информационная безопасность. — М.: Юрайт, 2024.