УДК 004.056

СОВРЕМЕННЫЕ ПОДХОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

MODERN APPROACHES TO ENSURING INFORMATION SECURITY OF WEB APPLICATIONS

Д. А. Гордеев

D. A. Gordeev

Аннотация. В условиях постоянного развития технологий и расширения функциональности веб-приложений, актуальность вопросов информационной безопасности в современном информационном обществе становится все более значимой. В работе рассмотрены основные этапы развития веб-приложений и эволюция их уязвимостей. Проанализированы методы обеспечения безопасности веб-приложений, включая традиционные средства защиты, такие как брандмауэры и системы обнаружения/предотвращения вторжений. Выявлены ограничения данных методов в обнаружении новых, неизвестных угроз, и представлены современные подходы к обеспечению информационной безопасности. Определена важность использования оптимальной стратегии, включающей комбинацию различных методов обеспечения безопасности веб-приложений. В результате исследования подчеркнуто, что эффективная стратегия безопасности должна учитывать конкретные потребности и задачи каждого приложения, а также постоянно обновляться для адаптации к новым угрозам.

Abstract. In the context of constant technological development and the expanding functionality of web applications, the relevance of issues related to information security in modern society is becoming increasingly significant. This work examines the key stages of web application development and the evolution of their vulnerabilities. Methods of ensuring the security of web applications are analyzed, including traditional defense mechanisms such as firewalls and intrusion detection/prevention

systems. The limitations of these methods in detecting new, unknown threats are identified, and modern approaches to ensuring information security are presented. The importance of using an optimal strategy, incorporating a combination of different security methods for web applications, is emphasized. The research highlights that an effective security strategy should take into account the specific needs and tasks of each application and should be constantly updated to adapt to new threats.

Ключевые слова: Информационная безопасность, кибербезопасность, угрозы и уязвимости, безопасность веб-приложений.

Key words: Information security, cybersecurity, threats and vulnerabilities, web application security.

Веб-приложения на сегодняшний день являются неотъемлемой частью информационного общества, предоставляя возможность поиска, хранения, передачи и обработки информации. Информационная безопасность веб-приложений особенно актуальна в результате непрерывно растущей сложности и разнообразия кибератак, направленных на получение несанкционированного доступа к конфиденциальным данным и нарушение нормального функционирования систем. Подобные атаки не только угрожают финансовой стабильности организаций, но и затрагивают приватность и доверие конечных пользователей, а развитие технологий, таких как облачные вычисления, микросервисная архитектура, машинное обучение, делает сетевую инфраструктуру более сложной и уязвимой [1]. Поэтому существует необходимость в постоянном анализе и понимании эволюции угроз информационной безопасности, изучении и адаптации передовых методов шифрования, механизмов обнаружения аномалий и анализе потенциальных уязвимостей в веб-приложениях, постоянном обновлении баз знаний в области кибербезопасности [2].

Цель статьи заключается в обзоре современных подходов к организации информационной безопасности веб-приложений. Для достижения цели необходимо провести анализ эволюции ключевых угроз и уязвимостей веб-

приложений, рассмотреть традиционные и современные методы предотвращения угроз информационной безопасности, а также определить оптимальную стратегию применения этих методов при проектировании веб-приложений.

Рассмотрим основные этапы развития веб-приложений и эволюцию их уязвимостей [1-4]:

– Зарождение и эпоха статических страниц: В начале развития интернет-пространства веб-приложения представляли в основном статические HTML-страницы. В это время основное внимание уделялось предоставлению информации, и понятие безопасности веб-приложений еще не было таким актуальным. Тем не менее уже проявлялись некоторые уязвимости, такие как сессионные атаки и отсутствие контроля доступа.

– Динамические веб-сайты и появление уязвимостей: С развитием серверных технологий, таких как PHP, ASP и JSP, веб-приложения стали более интерактивными и динамичными, что, в свою очередь, привело к появлению новых уязвимостей, таких как кросс-сайтовая подделка запросов (CSRF) и SQL-инъекции. Данные уязвимости стали представлять серьезные угрозы безопасности для веб-приложений.

– Появление AJAX и увеличение сложности уязвимостей: Внедрение технологии AJAX (Asynchronous JavaScript and XML) позволило создавать более интерактивные и отзывчивые веб-приложения. Однако, это также увеличило сложность атак и предоставило новые векторы развития уязвимостей. Возникли такие угрозы информационной безопасности как кросс-сайтовая атака (XSS) и утечки данных через асинхронные запросы.

– Развитие одностраничных приложений (SPA) и их программных интерфейсов (API): С появлением одностраничных приложений и расширенного использования API, веб-приложения стали более сложными и динамичными. Это также сопровождалось новыми угрозами, включая атаки на клиентскую сторону, недостаточную защиту API, и уязвимости в библиотеках и фреймворках.

– Облачные технологии и мобильные веб-приложения: С ростом популярности облачных вычислений и мобильных веб-приложений, угрозы безопасности стали более разнообразными. Возникли новые проблемы, такие как недостаточная защита хранилищ данных в облаке, атаки на мобильные устройства, и угрозы, связанные с разделением мобильных приложений и браузера.

Существующие методы обеспечения информационной безопасности веб-приложений представляют собой разнообразный инструментарий, каждый из которых обладает своими преимуществами и ограничениями.

Традиционные методы защиты, такие как брандмауэры и системы обнаружения/предотвращения вторжений (Firewalls, IDS/IPS), обеспечивают базовый уровень безопасности, фильтруя трафик и предотвращая широкий спектр известных атак. Однако они оставляют веб-приложения уязвимыми перед новыми, неизвестными угрозами, так как их подход ограничен в обнаружении подобных атак. Они также могут создавать ложные срабатывания, что требует дополнительного времени и ресурсов для анализа [5].

Файрвол веб-приложений (Web Application Firewall, WAF) является специализированным средством защиты, способным эффективно блокировать атаки на уровне приложения. К таким атакам можно отнести SQL-инъекции или межсайтовый скриптинг (Cross-Site Scripting, XSS). Однако эффективность зависит от тщательной конфигурации, постоянного обновления правил и фильтров, что может влиять на производительность приложения [6].

Тестирование на проникновение обеспечивает анализ стойкости системы к различным видам атак, выявляя уязвимые места, которые могли бы быть упущены другими методами. Задача тестирования заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования аудитор выполняет роль злоумышленника, мотивированного на нарушение информационной безопасности заказчика [7]. Ограничения заключаются в том, что тестирование

проводится периодически, охватывает конкретные тестовые сценарии и может не полностью отражать реальные условия эксплуатации, что делает приложение уязвимым в промежутках между тестированиями.

Применение протоколов передачи данных в сети обеспечивает безопасную связь между веб-браузером пользователя и веб-сервером. На сегодняшний день широко используется протокол HTTPS, который применяет шифрование для обеспечения конфиденциальности и целостности передаваемой информации [8]. В основе HTTPS лежит процесс шифрования, который обеспечивает защищенную передачу данных путем кодирования информации так, что она становится непонятной для третьих лиц, не обладающих соответствующим ключом. Этот метод предотвращает возможность перехвата и прослушивания чувствительных данных, таких как логины и пароли. Внедрение протокола HTTPS способствует повышению уровня безопасности в сети, создавая доверие пользователей к веб-ресурсам и обеспечивая конфиденциальность передаваемой информации [9].

С развитием анализа больших данных, искусственного интеллекта и машинного обучения открылись новые возможности в обнаружении аномалий и выявлении новых видов атак, даже если ранее они не были известны [6]. Их способность адаптироваться к изменяющимся условиям и угрозам делает их эффективными в борьбе с постоянно эволюционирующими угрозами. Для успешного применения этих технологий необходимы значительные вычислительные ресурсы, экспертные знания правильной настройки и постоянное обновление моделей [10]. Важно отметить, что системы машинного обучения могут подвергаться атакам, направленным на обман, что создает дополнительные риски. Для устойчивости к таким угрозам требуется постоянное совершенствование методов защиты. Также стоит учесть, что безопасность систем искусственного интеллекта и машинного обучения – это комплексная задача, требующая внимания к техническим, организационным и правовым аспектам [11].

Также одним из методов обеспечения безопасности является применение технологии блокчейн. Представляет инновационный метод обеспечения безопасности данных, основанный на создании непрерывной цепи блоков. Эта цепь представляет последовательность данных, каждый блок которой содержит информацию о предыдущем блоке, а также хеши, обеспечивающие целостность блокчейна. Такая структура делает блокчейн особенно устойчивым к взлому, обеспечивает прозрачность и надежность данных. Поскольку каждый блок в цепи связан с предыдущим, любые попытки вмешательства или изменения данных в одном блоке приведут к изменению всех последующих блоков, что сразу же становится заметным. Это обеспечивает невозможность манипулирования информацией без обнаружения. Кроме того, блокчейн применяется в системах управления доступом, где требуется высокая степень безопасности и надежности авторизации. Благодаря принципам блокчейна, такие системы могут гарантировать, что только уполномоченные пользователи имеют доступ к определенным ресурсам или информации. Вся история доступа сохраняется в блокчейне, что делает возможным более детальное отслеживание активности пользователей и обеспечивает аудит доступа [12].

С появлением перспективы активного развития квантовых вычислений, квантовая криптография стала неотъемлемым направлением в области информационной безопасности. Этот подход фокусируется на создании криптографических методов, которые остаются устойчивыми и эффективными в условиях атак, основанных на принципах квантовой физики. В отличие от классической криптографии, которая использует сложные математические задачи для создания надежных шифров, квантовая криптография основана на принципах квантовой физики. Она использует квантовые состояния, например, фотоны, для обеспечения безопасной передачи ключей шифрования. Это основное преимущество квантовой криптографии – она предоставляет механизмы обмена ключами, которые могут быть надежно защищены от атак, даже при использовании квантовых компьютеров [13].

Каждый метод защиты веб-приложений имеет свои сильные и слабые стороны. Оптимальная стратегия обеспечения безопасности веб-приложений обладает комплексным характером и включает в себя несколько взаимосвязанных методов. В начале процесса разработки веб-приложения необходимо провести анализ угроз и рисков, чтобы точно определить уровень защиты, который требуется в конкретном случае.

Шифрование данных является основным строительным блоком безопасности. Использование протокола HTTPS для защиты передачи данных по сети обеспечивает шифрование посредством криптографических протоколов, предотвращая возможные атаки на конфиденциальность. Для данных, хранящихся на сервере, также важно применять шифрование, чтобы предотвратить несанкционированный доступ.

Аутентификация пользователей следует быть многоуровневой. Использование сильных методов аутентификации, таких как двухфакторная аутентификация, усиливает защиту от несанкционированного доступа [4]. Кроме того, управление доступом должно быть строго регулированным, применяя принцип наименьших привилегий и разделяя права доступа на основе ролей пользователей.

Защита от веб-атак также является важным компонентом обеспечения безопасности. Фильтрация и валидация ввода данных, применение параметризованных запросов к базе данных, а также обеспечение валидации данных на стороне клиента и сервера помогают предотвратить множество возможных уязвимостей веб-приложения.

История развития веб-приложений представляет собой борьбу между инновациями и безопасностью. На каждом этапе прогресса появлялись новые уязвимости, и обеспечение безопасности веб-приложений продолжает оставаться важной и сложной задачей для разработчиков, исследователей и специалистов по кибербезопасности. Ключевым элементом оптимальной стратегии в области информационной безопасности является постоянное

обновление и адаптация. Безопасность веб-приложений не является статическим понятием, и стратегия должна непрерывно совершенствоваться в ответ на новые угрозы и изменения в технологическом ландшафте. Регулярные проверки безопасности, обновления и мониторинг помогут поддерживать высокий уровень защиты веб-приложения в постоянно меняющейся киберсреде.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Дибиров Г.М., Ковцур М.М., Бабков И.Н.* Разработка требований для веб-интерфейсов систем контроля информационной безопасности // XI Конгресс молодых учёных: Сборник научных трудов (г. Санкт-Петербург, 04–08 апреля 2022 г.). СПб., 2022.
2. *Лесько С.А.* Модели и сценарии реализации угроз для интернет-ресурсов // Российский технологический журнал. 2020. № 6(38).
3. *Шинкарев А.А.* Ретроспектива развития веб-технологий в создании корпоративных информационных систем // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2020. № 4.
4. *Нестеренко В.Р., Маслова М.А.* Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними // Научный результат. Информационные технологии. 2021. № 1.
5. *Базарова И.А.* Анализ сравнительных характеристик систем защиты сетей IDS и IPS // Информационные технологии в управлении и экономике. 2021. № 3(24).
6. *Безпалов М.Ю., Ланец С.А.* Современные вызовы и технологические решения информационной безопасности // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. 2022. Т. 1.
7. *Мельникова А.Е., Карманов И.Н.* Разработка методики тестирования на проникновение мобильных и веб-приложений // Интерэкспо Гео-Сибирь. 2019. Т. 9.
8. *Коростень А.О., Аксенов С.С.* Информационная безопасность веб-приложений // Информационная безопасность регионов России (ИБРР-2021):

Материалы XII Санкт-Петербургской межрегиональной конференции (г. Санкт-Петербург, 27–29 ноября 2021 г.). СПб., 2021.
9. *Афанасьева Д.В., Абидарова А.А., Плахина Е.А.* Применение протокола https для повышения информационной безопасности в сети // Известия Тульского государственного университета. Технические науки. 2019. № 9.
10. *Окатов Д.А., Минеева Т.А.* Технологии искусственного интеллекта в информационной безопасности // Тенденции развития науки и образования. 2021. № 74-2.
11. *Камалова Г.Г.* Информационная безопасность и искусственный интеллект: организационно-правовые проблемы // Обеспечение информационной безопасности: вопросы теории и практики: Сборник статей Всероссийской научно-практической конференции, (г. Ижевск, 29 мая 2023 г.). Ижевск, 2023.
12. *Сазанова Е.В.* Технология блокчейн в контексте информационной безопасности // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. 2019. Т. 1.
13. *Шемякина М.А.* Анализ использования квантовых технологий в криптографии // Международный журнал гуманитарных и естественных наук. 2019. № 5-4.

Гордеев Данил Александрович
Аспирант Московского финансово-юридического университета МФЮА
dan.gor220@yandex.ru

Gordeev Danil Alexandrovich
Postgraduate student Moscow University of Finance and Law (MFUA)
dan.gor220@yandex.ru