DOI 10.37882/2223-2966.2025.07.22

СОВРЕМЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ И КОМПЛЕКСНЫЙ ПОДХОД К ИСПОЛЬЗОВАНИЮ МЕТОДОВ ДЛЯ ИХ ПРЕДОТВРАЩЕНИЯ

MODERN WEB APPLICATION SECURITY THREATS AND A COMPREHENSIVE APPROACH TO USING METHODS TO PREVENT THEM

M. Malyavin

Summary. With the rapid growth in the number of web applications and integration into key professional and everyday areas of human activity, ensuring their security is becoming a priority. Modern threats such as SQL injection, cross-site scripting, denial of service attacks and zero-day vulnerability exploitation pose serious risks to private users and organizations. The purpose of this article is to analyze current cyber threats, identify their features and consider an integrated approach to the use of protection methods. The study summarizes modern attack prevention strategies, including the use of web firewalls, authentication and authorization mechanisms, anomaly monitoring, and the use of machine learning technologies to identify threats. The author confirms the necessity and importance of an integrated (combined) approach to ensure multi-level protection of modern web applications. The results of the work will allow us to form a holistic view of the necessary measures to ensure the security of web applications. The presented materials can be useful to cybersecurity specialists, software developers, and web system administrators, as well as used in the future to develop effective protection strategies.

Keywords: Web application, web development, security, information security, protection, attack, cyber threat.

Малявин Максим Юрьевич
Аспирант, Московский информационно-технологический университет, Московский архитектурно-строительный институт МАСИ
max-malyavin@bk.ru

Аннотация. В условиях стремительного роста количества веб-приложений и интеграции в ключевые как профессиональные, так и бытовые сферы деятельности человека, становится приоритетной задачей обеспечение их безопасности. Современные угрозы, такие как SQL-инъекции, межсайтовый скриптинг, атаки типа «отказ в обслуживании» и эксплуатация уязвимостей нулевого дня, создают серьезные риски для частных пользователей и организаций. Целью настоящей статьи является выполнение анализа актуальных киберугроз, выявление их особенностей и рассмотрение комплексного подхода к использованию методов защиты. В ходе исследования обобщены современные стратегии предотвращения атак, включая применение веб-фаерволов, механизмов аутентификации и авторизации, мониторинга аномалий и использования технологий машинного обучения для выявления угроз. Автором подтверждается необходимость и значимость комплексного (комбинированного) подхода для обеспечения многоуровневой защиты современных веб-приложений. Результаты работы позволят сформировать целостное представление о необходимых мерах по обеспечению безопасности веб-приложений. Представленные материалы могут быть полезны специалистам в области кибербезопасности, разработчикам программного обеспечения и администраторам веб-систем, а также использоваться в дальнейшем при разработке эффективных стратегий защиты.

Ключевые слова: Веб-приложение, веб-разработка, безопасность, информационная безопасность, защита, атака, киберугроза.

Введение

Безопасность веб-приложений является одной из ключевых задач в области кибербезопасности, поскольку их уязвимости могут привести к утечке данных, финансовым потерям и компрометации систем. В последние годы наблюдается рост атак на веб-приложения, что требует совершенствования существующих методов защиты. По результатам анализа В. Бесединой (аналитика Positive Technologies), в третьем квартале 2024 года количество инцидентов увеличилось на 15 % по сравнению с аналогичным периодом 2023 года и лишь незначительно уменьшилось (на 4 %) по сравнению с предыдущим кварталом [1]. Вредоносное ПО остается основным инструментом злоумышленников, применяясь в 65 % успешных атак на организации и в 72 % атак на частных лиц. Дополнительно, специалисты компании BI.Zone выяснили, что 25 % веб-уязвимостей, обнаруживаемых ежемесячно, могут представлять высокие риски для кибербезопасности организаций [2]. Это подчеркивает критическую важность своевременного выявления и устранения уязвимостей, а также внедрения комплексных мер защиты.

Ключевой проблемой на современном этапе исследований является недостаточный уровень защиты веб-приложений, обусловленный как ростом сложности атак, так и несовершенством применяемых мер безопасности. В связи с этим материалы настоящей статьи посвящены анализу актуальных угроз и формированию комплекса решений, которые на 2025 год способны обеспечить достаточный уровень защиты веб-приложений,

минимизируя риски кибератак. Автором предполагается, что применение комплексного подхода, включающего как традиционные методы защиты, так и новейшие технологии, такие как машинное обучение и искусственный интеллект для обнаружения аномалий, а также автоматизированные системы для мониторинга безопасности в реальном времени, позволит значительно повысить уровень защиты веб-приложений. В статье также рассматриваются методы предотвращения уязвимостей, связанные с неправильной настройкой безопасности, а также угрозы, возникающие из-за недостаточной защиты пользовательских данных и слабых мест в кодировании. Проводимый анализ направлен на формирование практических рекомендаций для улучшения кибербезопасности, что поможет разработчикам, специалистам по безопасности и организациям повысить надежность своих веб-приложений и снизить риски в условиях постоянно меняющихся угроз.

Результаты и обсуждение

На фоне быстрого развития технологий в 2025 году угроза безопасности веб-приложений продолжает оставаться одной из наиболее актуальных проблем в области киберзащиты. Как отмечают Ю. Быкова и А.В. Звягинцева, в первую очередь, это связано с ростом числа

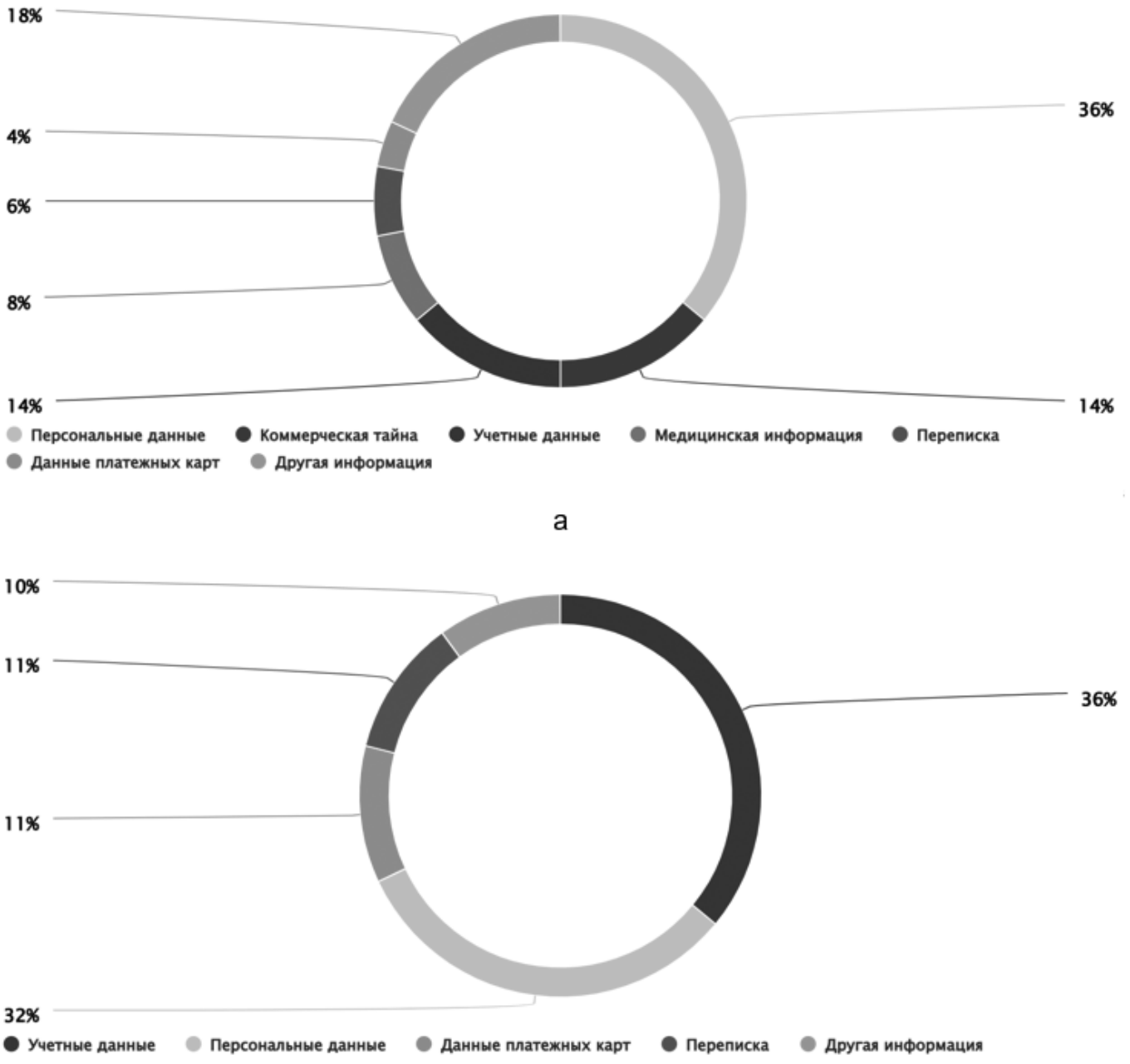

Рис. 1. Типы украденных данных: а — в атаках на организации; б — в атаках на частных лиц

и сложности кибератак, направленных на нарушение функционирования веб-приложений и утечку конфиденциальной информации [3]. Одной из главных угроз остаются атаки с использованием вредоносного ПО, которое используется злоумышленниками для организации киберпреступлений. Согласно данным из обзора крупнейших киберинцидентов 2024 года, в 65 % успешных атак на организации и в 72 % — на частные лица использовалось вредоносное ПО. Так, например, в одном из крупных инцидентов 2024 года злоумышленники применили вирус-вымогатель, что привело к компрометации корпоративных данных и крупным финансовым потерям. По данным отчета аналитика компании Cloud Networks А. Савиной за первый квартал 2024 года хакеры атаковали более 19 млн российских пользователей Android-смартфонов с помощью изначально занесённых на устройства вирусов [4].

Атаки на веб-приложения с целью утечки конфиденциальной информации все также продолжают быть широко распространенными на момент 2025 года. По данным отчета аналитиков компании Positive technologies, в этих атаках злоумышленники чаще всего ориентировались на похищение персональных данных (36 %), учетных данных (36 %) и коммерческой тайны (14 %). Эти данные подтверждают, что персональные данные и учетные данные являются приоритетными целями для хакеров, что усиливает необходимость разработки и применения надежных механизмов защиты веб-приложений [5]. Рис. 1 иллюстрирует эти данные и показывает основные направления атак. Также на основе анализа материалов М.А. Лапиной, А.Р. Багаутдиновой и Н. Загнетовой, становится очевидным, что текущие методы защиты не всегда способны эффективно справляться с новыми угрозами, такими как атаки на уровне приложений, использующие уязвимости в API, и атаки на базы данных [6].

Как результат, на основе анализа актуальных угроз безопасности веб-приложений можно утверждать о высоком уровне их актуальности в 2025 году. Наблюдаемое увеличение количества инцидентов и использование все более сложных методов атак ставит перед исследователями и разработчиками веб-приложений задачу создания комплексных решений, способных эффективно противодействовать этим угрозам. В частности, необходимо сосредоточиться на разработке систем защиты, включающих современные технологии, такие как искусственный интеллект, машинное обучение и расширенные системы мониторинга в реальном времени. В связи с этим, как подчеркивает М.В. Шатурный, обеспечение комплексного подхода к защите веб-приложений станет необходимым шагом на пути повышения уровня киберзащиты и защиты конфиденциальной информации в условиях современных угроз [7]. На основе анализа актуальных материалов и киберинцидентов 2024 года автором настоящей статьи разработана следующая табл. 1, отражающая актуальные угрозы безопасности веб-приложений. Данная таблица позволяет выделить основные угрозы, с которыми сталкиваются веб-приложения в 2025 году, а также дает представление о распространенности и возможных последствиях каждой угрозы в современном сегменте веб-приложений.

Таблица 1.

Актуальные угрозы безопасности веб-приложений в 2025 году

№	Угроза	Описание	% случаев воздействия
1	Утечка персональных данных	Включает кражу личных данных пользователей, таких как ФИО, адреса, телефонные номера, email и номера банковских карт.	36 % (по данным BI.Zone)
2	Атаки с использованием вредоносного ПО	Вредоносное ПО используется для взлома и повреждения системы, часто с целью получения конфиденциальной информации.	65 % (по данным Positive Technologies)
3	SQL-инъекции	Атаки через уязвимости в базе данных веб-приложений, что позволяет злоумышленникам манипулировать запросами к базе данных.	22 % (по оценке автора статьи)
4	Кросс-сайтовый скриптинг (XSS)	Уязвимости, позволяющие внедрять вредоносный JavaScript код на страницы веб-приложений, что может привести к утечке данных.	18 % (по оценке автора статьи)
5	Атаки через уязвимости в API	Злоумышленники используют недостатки в API для получения доступа к данным и управления системой.	25 % (по данным Positive Technologies)
6	Атаки на сессии и куки	Хищение сессионных данных или фальсификация куков для получения несанкционированного доступа к учетным записям.	15 % (по данным Cloud Networks)

На основе анализа актуальных угроз безопасности веб-приложений, представленных ранее в работе, следует сделать следующие выводы, которые подтверждают необходимость применения комплексного подхода к обеспечению безопасности веб-приложений. Так, современные угрозы, такие как утечка персональных данных, атаки с использованием вредоносного ПО, SQL-инъекции и XSS-уязвимости, показывают, что традиционные методы защиты оказываются недостаточными для

эффективной защиты от множества атакующих факторов. Учитывая быстрое развитие технологий, появление новых уязвимостей и инновационных методов атаки, требуется создание многоуровневой системы защиты, которая обеспечит целостность и безопасность данных на всех уровнях взаимодействия с веб-приложениями. Как отмечают М.В. Зейкан, Е.В. Вершинин и В.О. Фёдоров, комплексность защиты веб-приложений состоит в интеграции методов и технологий, которые в совокупности создают многослойную архитектуру безопасности [8]. Такой подход позволяет эффективно противодействовать широкому спектру угроз, минимизируя риски взлома или утечки данных. Наиболее важными элементами комплексной защиты являются комбинация различных методов аутентификации и авторизации, защита соединений, защита данных при передаче и защита API.

Одним из основных методов является использование OAuth 2.0 и JWT (JSON Web Tokens), которые обеспечивают надежную аутентификацию и авторизацию пользователей, предотвращая несанкционированный доступ к ресурсам веб-приложения. С.А. Лесько подтверждает, что данные технологии позволяют надежно передавать информацию о пользователе и контролировать доступ к различным сервисам и данным, исключая возможность подмены данных злоумышленниками [9]. Другим важным элементом является использование HTTPS, Content Security Policy (CSP) и CORS для защиты соединений между клиентом и сервером. HTTPS обеспечивает шифрование данных, предотвращая их перехват в процессе передачи. CSP и CORS служат защитой от атак типа XSS, контролируя загрузку внешних ресурсов и ограничивая возможность выполнения опасного кода на стороне клиента. Важным аспектом является защита API, которая включает такие механизмы, как Rate Limiting и DDoS Protection, для предотвращения перегрузки серверов и блокировки атак, направленных на исчерпание ресурсов системы [10]. По оценке автора настоящей статьи, внедрение таких технологий и методов позволяет значительно повысить уровень безопасности веб-приложений, эффективно противодействуя самым актуальным угрозам, с которыми сталкиваются организации и частные лица в 2025 году. В итоге комплексный подход к защите веб-приложений, включающий комбинацию различных методов защиты и построение многоуровневой системы безопасности, является необходимостью для обеспечения надежности и защиты информации в условиях современных киберугроз. Автором предлагается следующая система методов и инструментов для построения комплексной системы защиты современных веб-приложений, которая сочетает в себе лучшие практики и новейшие технологии в области кибербезопасности (рис. 2). Данная система представляет собой многоуровневую архитектуру, включающую несколько ключевых слов и технологий, обеспечивающих защиту от большинства актуальных угроз веб-приложений.

Разработка предложенной системы безопасности веб-приложений требует использования нескольких этапов:

1. Оценка рисков (на начальном этапе важно провести анализ существующих угроз и уязвимостей в веб-приложении. Это позволит определить, какие слои защиты необходимо интегрировать в первую очередь);
2. Интеграция технологий и инструментов (внедрение каждого из предложенных слоев безопасности должно быть последовательным. Важно начать с базовых технологий, таких как HTTPS и OAuth 2.0, а затем добавлять более сложные решения, такие как WAF и API Gateway);
3. Тестирование и оптимизация (после интеграции всех компонентов системы необходимо провести тестирование на уязвимости и производительность, чтобы убедиться в надежности защиты);
4. Мониторинг и обновление (важнейший этап — это постоянное отслеживание актуальности угроз и обновление системы защиты, с учетом новых угроз и изменений в области кибербезопасности).

Предложенная система защиты является универсальной и может быть адаптирована под различные типы веб-приложений в зависимости от их специфики. Например, для финансовых приложений можно усилить защиту с помощью более строгих методов аутентификации и авторизации, таких как биометрия. Для медиа-платформ можно сконцентрироваться на защите контента и предотвращении утечек данных. Архитектура системы имеет модульную природу, что позволяет добавлять или удалять компоненты в зависимости от уровня угроз и требований безопасности. Возможность масштабирования системы также заключается в ее гибкости: по мере роста веб-приложения можно увеличивать количество защитных слоев или добавлять новые технологии, такие как блокчейн для дополнительной защиты данных.

Согласно результатам анализа, представленных в предшествующих материалах, предложенная система может обеспечить защиту от 90–95 % актуальных угроз веб-приложений. Этот процент был получен на основе анализа статистики о распространенности различных атак и уязвимостей, а также эффективности существующих защитных мер. Например, внедрение WAF, HTTPS и OAuth 2.0 позволяет существенно снизить риски, связанные с XSS, SQL-инъекциями и фишингом, которые составляют основную долю атак на веб-приложения. Использование системы мониторинга SIEM и IDS/IPS снижает вероятность успешных атак на уровне сети и приложений. С учетом всех перечисленных технологий и методов защиты, комплексная система, предложенная в настоящей статье, способна существенно повысить уровень безопасности современных веб-приложений, обеспечивая надежную защиту от большинства актуальных угроз.

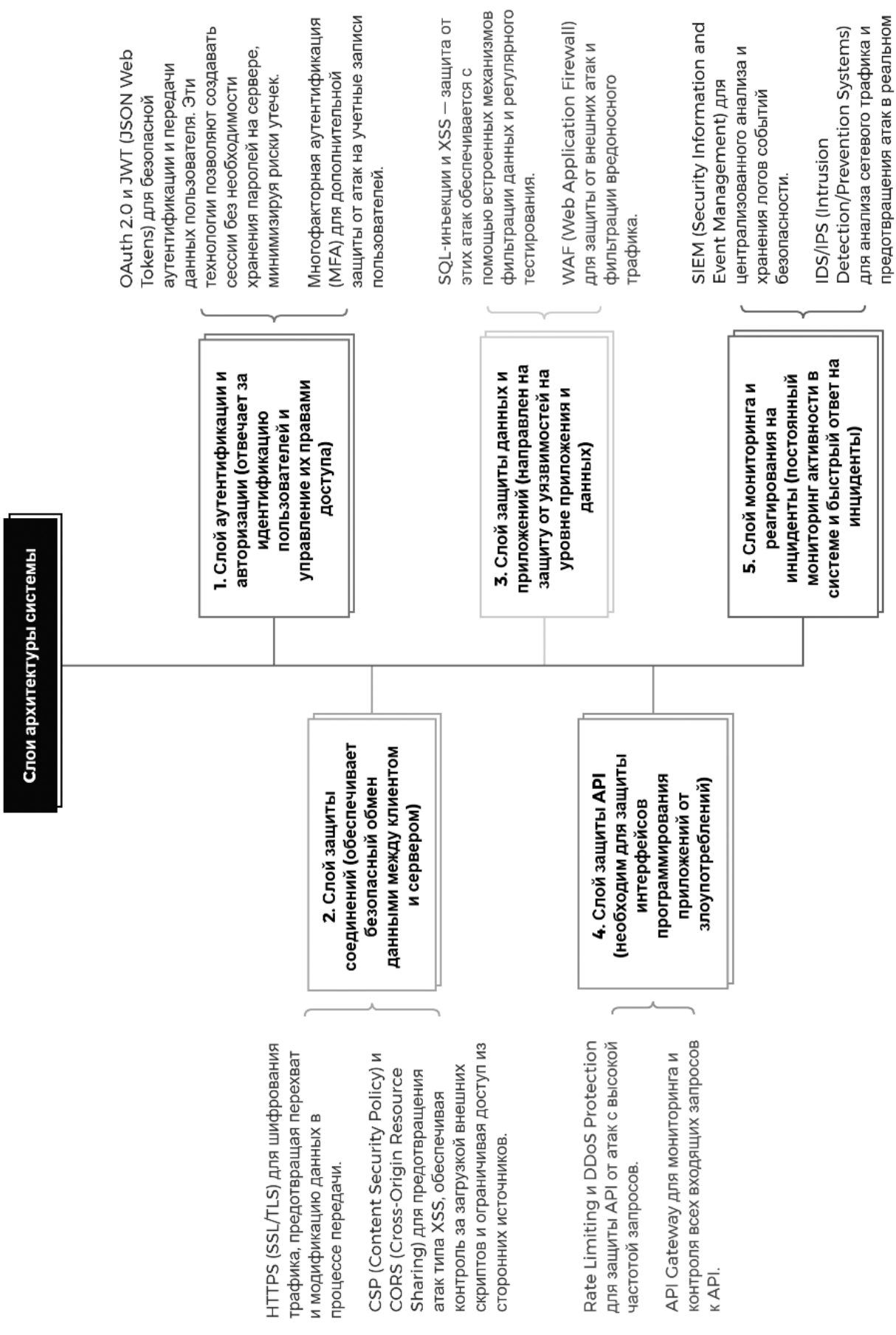

Рис. 2. Основные слои предлагаемой автором архитектуры системы обеспечения защиты веб-приложений

Заключение

В ходе проведенного исследования автором систематизированы актуальные угрозы безопасности веб-приложений, с учетом современных киберугроз и уязвимостей, с которыми сталкиваются компании и пользователи. Проведенный анализ позволил выделить ключевые риски, такие как SQL-инъекции, XSS-атаки, утечки данных, а также атаки на API и DDoS-атаки, которые составляют основу большинства угроз для веб-приложений. Автором разработана комплексная система защиты, включающая многоуровневую архитектуру, основанную на применении передовых технологий и методов безопасности. Важнейшими компонентами системы являются OAuth 2.0, JWT, HTTPS, CSP, CORS, WAF, а также защита API через Rate Limiting и DDoS Protection. Все эти методы составляют единый комплекс, обеспечивающий надежную защиту на всех уровнях — от аутентификации и авторизации пользователей до защиты от атак на сервер и базу данных.

На основе проведенного анализа можно утверждать, что предложенная система может обеспечить защиту от 90–95 % актуальных угроз веб-приложений. Этот показатель является результатом системного подхода к интеграции различных методов защиты и их сочетания для предотвращения как технических, так и организационных уязвимостей. Процентная оценка защиты основана на статистике о распространенности атак, а также на эффективности внедренных решений, таких как WAF и HTTPS, которые обеспечивают надежную защиту от наиболее распространенных атак.

Также важно подчеркнуть, что предложенная система имеет высокую степень универсальности и масштабируемости. Ее архитектура позволяет адаптировать компоненты и усиливать защиту в зависимости от специфики веб-приложений, что делает систему гибкой и удобной для применения в различных отраслях, от финансовых сервисов до медиаплатформ. Как итог, выводы работы подтверждают, что комплексный подход к защите веб-приложений, основанный на интеграции нескольких уровней безопасности и использовании передовых технологий, является наиболее эффективным для защиты от современных угроз. В результате применения предложенной системы можно значительно снизить риски и повысить уровень безопасности веб-приложений, что крайне важно в условиях постоянно растущей активности киберпреступников и новых угроз.

ЛИТЕРАТУРА

1. Безопасность веб-приложений. Электронный ресурс. Режим доступа: https://www.tadviser.ru/index.php/Статья: Безопасность_веб-приложений (дата обращения 06.03.2025 г.).
2. Актуальные киберугрозы: III квартал 2024 года. Электронный ресурс. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id1 (дата обращения 06.03.2025 г.).
3. М.Ю. Быков, А.В. Звягинцева Анализ актуальных угроз безопасности веб-приложений // Пожарная безопасность: проблемы и перспективы. 2019. №10. С. 65–67.
4. Обзор крупнейших киберинцидентов 2024 года. Электронный ресурс. Режим доступа: https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda/ (дата обращения 06.03.2025 г.).
5. Актуальные киберугрозы: I квартал 2023 года. Электронный ресурс. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ cybersecurity-threatscape-2023-q1/ (дата обращения 06.03.2025 г.).
6. Лапина М.А., Багаутдинова А.Р., Загнетов Н. Исследование уязвимостей безопасности веб-приложений // Auditorium. 2024. №1 (41). С. 58–62.
7. М.В. Шатурный Анализ актуальных угроз и разработка подходов к защите веб приложений // ИВД. 2024. №7 (115). С. 9–18.
8. Зейкан М.В., Вершинин Е.В., Фёдоров В.О. Проблема защиты данных при проектировании веб-приложения // Нацбезопасность. 2022. №1 (3). С. 4–7.
9. Лесько С.А. Модели и методы защиты веб-ресурсов: систематический обзор // Cloud of science. 2020. №3.
10. Жилина А.А. Актуальные веб-уязвимости сервисов финансово-банковского сектора и способы защиты веб-приложения // Научные записки молодых исследователей. 2021. №1. С. 53–70.

Журнал «Современная наука: актуальные проблемы теории и практики»