DOI 10.37882/2223-2966.2025.08.16

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ РАЗРАБОТКИ ВЕБ-ПЛАТФОРМЫ ДЛЯ ПРОВЕДЕНИЯ НАУЧНЫХ КОНФЕРЕНЦИЙ

INFORMATION SECURITY METHODS IN THE CONTEXT OF DEVELOPING A WEB PLATFORM FOR SCIENTIFIC CONFERENCES

M. Malyavin

Summary. Modern web platforms designed for scientific conferences will play an important role in the development of academic cooperation and the dissemination of scientific knowledge. However, as the functionality becomes more complex and the user audience expands, the importance of ensuring the information security of such systems increases dramatically. The issues of protecting the personal data of participants, the safety of scientific materials, resistance to external attacks and ensuring the continuous functioning of the platform are becoming particularly critical. The purpose of this article is to substantiate the need for a systematic approach to information security when developing a web application for scientific conferences, analyze current threats and vulnerabilities, and build a multi-level protection model adapted to the features of the software solution in question. In the course of the study, a structural assessment of the risks associated with the operation of the web platform carried out, potential threats classified, and vulnerable links in the system architecture identified. Based on the analysis, the concept of a multi-level information security system been developed. The practical significance of the work is to create an integrated approach to the protection of web platforms for scientific conferences, which can be scalable and adaptable for various educational and scientific institutions.

Keywords: Web application, security, information security, data protection, threat, scientific conference, web platform.

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

Аннотация. Современные веб-платформы, предназначенные для проведения научных конференций, станут играть важную роль в развитии академического взаимодействия и распространении научных знаний. Однако по мере усложнения функциональности и расширения пользовательской аудитории резко возрастает значимость обеспечения информационной безопасности таких систем. Особенно критичными становятся вопросы защиты персональных данных участников, сохранности научных материалов, устойчивости к внешним атакам и гарантии непрерывного функционирования платформы. Целью данной статьи является обоснование необходимости системного подхода к обеспечению информационной безопасности при разработке веб-приложения для проведения научных конференций, анализ актуальных угроз и уязвимостей, а также построение многоуровневой модели защиты, адаптированной под особенности рассматриваемого программного решения. В ходе исследования проведена структурная оценка рисков, связанных с эксплуатацией веб-платформы, классифицированы потенциальные угрозы, а также выделены уязвимые звенья в архитектуре системы. На основе проведённого анализа разработана концепция многоуровневой системы информационной безопасности. Практическая значимость работы заключается в создании комплексного подхода к защите веб-платформ научных конференций, который может быть масштабируемым и адаптируемым для различных образовательных и научных учреждений.

Ключевые слова: Веб-приложение, безопасность, информационная безопасность, защита данных, угроза, научная конференция, веб-платформа.

Введение

Развитие цифровых технологий значительно изменило подходы к организации научных мероприятий, включая конференции, симпозиумы и круглые столы. В условиях глобализации и удалённой коммуникации всё больше научных сообществ переходят на онлайн-формат, что обусловило необходимость создания специализированных веб-платформ, обеспечивающих полный цикл проведения конференции от регистрации участников и подачи статей до организации видеосессий и публикации итоговых сборников. Разрабатываемое веб-приложение представляет собой универсальную платформу для проведения научных конференций, объединяющую в себе ряд ключевых функций: регистрацию пользователей с распределением ролей (участники, рецензенты, модераторы), подачу и отслеживание научных работ, систему автоматического и экспертного рецензирования, проведение онлайн-сессий с использованием видеоконференций (на базе LiveKit), формирование сборников с присвоением DOI, мультиязычный интерфейс, а также интеграцию с внешними сервисами и элементами геймификации. Основная идея платформы создать единое, удобное, безопасное и технологически современное пространство для взаимодействия исследователей, экспертов и организаторов.

На фоне активного расширения функционала и пользовательской базы особую актуальность приобретает вопрос информационной безопасности веб-

приложений. Защита данных и устойчивость платформы к киберугрозам становятся не просто технической задачей, а важным условием доверия со стороны научного сообщества. Информационная безопасность (далее — ИБ) веб-приложений сегодня находится в центре внимания специалистов, поскольку любые уязвимости могут привести к компрометации персональных данных, утечке интеллектуальной собственности, сбоям в работе системы и значительным финансовым потерям. Аналитики отмечают устойчивый рост атак на веб-сервисы: по данным отчёта В. Бесединой (Positive Technologies), количество инцидентов в третьем квартале 2024 года увеличилось на 15 % по сравнению с аналогичным периодом 2023 года [1]. Причём вредоносное ПО по-прежнему используется в 65 % атак на организации и в 72 % на частных лиц [2]. Специалисты компании BI.Zone добавляют, что четверть всех веб-уязвимостей, выявляемых ежемесячно, несут высокий уровень риска для ИБ-инфраструктуры организаций. Эти факты подтверждают необходимость системного подхода к обеспечению защиты веб-приложений, особенно тех, которые работают с конфиденциальной и научной информацией.

Целью настоящей статьи является анализ угроз и уязвимостей веб-платформ, используемых для проведения научных конференций, а также разработка многоуровневой системы информационной безопасности, которая обеспечит надёжную защиту данных, устойчивость к атакам и стабильность функционирования приложения в условиях постоянно меняющейся цифровой среды.

Результаты и обсуждение

На момент 2025 года цифровые платформы, особенно те, которые обрабатывают научные данные, персональную информацию и материалы интеллектуальной собственности, подвергаются всё более изощрённым видам атак. Актуальность системной оценки рисков для веб-приложений обусловлена как глобальной динамикой киберугроз, так и высокой стоимостью потенциальных утечек данных. Согласно М.А. Лапиной, А.Р. Багаутдиновой и Н. Загнетову (2024), более 70 % атак на веб-приложения связаны с использованием известных уязвимостей, оставленных без внимания в течение полугода и более [4].

Это говорит не только о слабых местах в архитектуре, но и о недостаточности процессов контроля и обновления безопасности. Для анализа текущей картины используется структурная модель оценки рисков, где каждое событие описывается через взаимосвязь угрозы, уязвимости и потенциального ущерба, оцениваемого по шкале вероятности воздействия. Ниже представлена таблица (табл. 1), классифицирующая типичные риски веб-приложений в 2025 году.

Таблица 1.

Шкала оценки совокупного риска (R)

Уровень риска	Диапазон значений
Очень низкий	0.00–0.20
Низкий	0.21–0.40
Средний	0.41–0.60
Высокий	0.61— 0.80
Очень высокий	0.81–1.00

В данной модели совокупный риск *R* рассчитывается как произведение вероятности возникновения события (P) и интенсивности возможного ущерба (I):

$$R = P * I,$$

где *P* — вероятность реализации угрозы, оценённая экспертно или на основе статистики инцидентов (диапазон от 0 до 1);

I — потенциальный урон (ущерб) в случае реализации угрозы, также по шкале от 0 до

R — совокупный риск, подлежащий интерпретации по уровневой шкале.

По мнению И.И. Иванова (2020), подобный подход позволяет количественно сравнивать риски и приоритизировать усилия по обеспечению безопасности системы, особенно в условиях ограниченных ресурсов [3]. Методика была адаптирована для оценки рисков, возникающих в разработке веб-платформы для проведения научных конференций, с учётом специфики её архитектуры: распределённые пользовательские роли, обработка публикаций, хранение персональных данных, онлайн-сессии в реальном времени (табл. 2). Важно отметить, что каждая из угроз в таблице оказывает влияние на как минимум два аспекта: стабильность функционирования системы и доверие со стороны участников.

При этом в табл. 3 отражены основные угрозы безопасности данных участников и материалов конференций.

Исходя из вышеизложенного следует, что угрозы безопасности данных участников и материалов конференции являются важным аспектом, требующим внимания при разработке и эксплуатации систем для проведения научных мероприятий. Основные угрозы включают несанкционированный доступ, утечку конфиденциальной информации, нарушения интеллектуальной собственности, а также атаки, направленные на отказ в обслуживании и распространение вредоносного ПО. Учитывая высокий уровень рисков, важно внедрять комплекс-

Таблица 2.

Структурная оценка рисков веб-приложений

№	Угроза	Уязвимость	Возможные последствия	Вероятность (P)	Урон (I)	Совокупный риск (R)	Уровень
1	SQL-инъекции	Отсутствие фильтрации пользовательского ввода	Захват базы данных, утечка персональных данных	0.8	0.9	0.72	Высокий
2	Межсайтовый скриптинг (XSS)	Недостаточная обработка HTML/JS	Кража сессий, подмена контента	0.6	0.7	0.42	Средний
3	Атаки на сессии (Session Hijack)	Незащищённые cookie, отсутствие HTTPS	Перехват учётных данных, вход от имени другого	0.5	0.8	0.40	Низкий
4	DDoS-атака	Отсутствие защиты на уровне сети	Потеря доступа к системе, отказ в обслуживании	0.7	0.9	0.63	Высокий
5	Утечка конфиденциальных данных	Слабое шифрование, хранение открытым текстом	Нарушение ФЗ-152, ответственность перед участниками	0.6	1.0	0.60	Средний
6	Эскалация привилегий	Ошибки в управлении правами пользователей	Доступ к административным функциям	0.4	0.7	0.28	Низкий
7	Вредоносные вложения/файлы	Отсутствие проверки загружаемых файлов	Загрузка эксплойтов, внедрение вредоносного ПО	0.6	0.8	0.48	Средний

Таблица 3.

Основные угрозы безопасности данных участников и материалов конференций

№	Угроза	Описание	Уровень риска	Воздействие
1	Несанкционированный доступ к личным данным участников	Возможность несанкционированного доступа к данным участников конференции.	Высокий	Внешнее
2	Утечка конфиденциальной информации	Перехват или утечка данных участников, таких как личные контакты или материалы статей.	Высокий	Внутреннее/Внешнее
3	Нарушение интеллектуальной собственности	Использование материалов конференции без разрешения авторов, копирование или распространение статей.	Средний	Внешнее
4	Вредоносное ПО (вирусы, трояны)	Вредоносное ПО, которое может заразить систему конференции или устройства участников, приводя к утечке данных.	Средний	Внешнее
5	Отказ в обслуживании (DDoS-атаки)	Атака на серверы системы, которая может привести к недоступности платформы конференции.	Высокий	Внешнее
6	Недостаточное управление правами доступа	Ошибки в управлении правами доступа, которые позволяют неавторизованным пользователям получить доступ к чувствительным данным.	Средний	Внутреннее
7	Недостаточная защита от фишинга	Попытки получения конфиденциальной информации участников через обманные сообщения (например, фишинг).	Средний	Внешнее

ные меры безопасности, такие как шифрование данных, строгие процедуры аутентификации и регулярный мониторинг систем. Только с учетом этих угроз можно обеспечить надежную защиту информации и снизить возможное воздействие на репутацию и доверие участников конференций.

Как видно из представленной модели, основными зонами повышенного риска остаются уязвимости, связанные с работой с базами данных, некорректной обработкой пользовательского ввода, отсутствием сетевой фильтрации и слабой реализацией механизмов аутентификации. По мнению М.А. Иконникова и И.Н. Карманова (2019), именно эти участки чаще всего подвергаются атакам, особенно в условиях отсутствия регулярного тестирования на проникновение и обновлений безопасности [3]. Актуальность оценки риска заключается не в пас-

сивном учёте угроз, а в построении активной стратегии защиты, где каждое решение базируется на точном понимании вероятностей и потенциального ущерба. В следующем разделе будет предложена многоуровневая система информационной безопасности, учитывающая выявленные риски и уязвимости, а также архитектурные особенности разрабатываемой платформы.

С учётом выявленных угроз и уровня их критичности для веб-приложений, обслуживающих сферу научной деятельности, обеспечение информационной безопасности должно носить не шаблонный, а контекстно-адаптированный характер. Научные платформы обрабатывают чувствительные данные: персональные сведения участников, материалы статей до публикации, экспертные отзывы и переписку, элементы конференционного управления. Компрометация таких данных не только нарушает нормы защиты информации (например, требования ФЗ-152), но и подрывает доверие научного сообщества. В этой связи оправдано применение трёхуровневой модели защиты, которая позволяет организовать системный, но при этом гибкий подход к выстраиванию ИБ-архитектуры. Каждый уровень выстраивается как логическое расширение предыдущего, включая более сложные механизмы контроля, мониторинга и реагирования. Такая модель масштабируется и адаптироваться под специфику бюджета, количества пользователей и сложности функционала.

Подход базируется на принципах управления киберрисками, при котором инвестиции в защиту пропорциональны масштабам потенциального ущерба и вероятности наступления событий. По мнению В.А. Довгаля и Д.И. Шередько (2022), особенно в условиях импортозамещения, построение информационной безопасности должно учитывать реальные угрозы, быть ориентированным на независимость от дорогостоящих решений и обеспечивать достаточный уровень защиты с использованием проверенных отечественных и открытых решений [8]. Модель реализуется в виде трёх ступеней:

1. Минимальный уровень — обеспечивает базовую устойчивость к самым распространённым видам атак (SQL-инъекции, XSS, перехват сессий), делает невозможной эксплуатацию уязвимостей «нулевого уровня»;
2. Базовый уровень — расширяет сферу защиты, вводя механизмы контроля внутренних операций, управления доступом, мониторинга действий пользователей и защиты хранимых данных;
3. Максимальный уровень — включает в себя элементы активной обороны, автоматизированного анализа и поведенческого моделирования, мониторинга инцидентов и реагирования на угрозы в реальном времени.

Каждый уровень может использоваться как самостоятельно, так и в совокупности с другими, в зависимости от масштаба проекта и критичности данных (табл. 4). Подобная иерархическая структура позволяет выстраивать защиту последовательно, начиная с самых необходимых мер, и постепенно наращивать её глубину без необходимости полной перестройки архитектуры.

Таблица 4.

Уровни защиты и соответствующие меры.

Уровень защиты	Описание уровня	Методы и средства
Минимальный	Базовая защита от наиболее частых угроз (SQL-инъекции, XSS, перехват сессий)	Валидация данных, HTTPS, Content Security Policy (CSP), ограничения CORS, базовая авторизация
Базовый	Расширенная защита, включающая контроль привилегий и управление доступом	Роль-ориентированный доступ (RBAC), шифрование данных в БД, защита cookie, контроль сессий
Максимальный	Комплексная модель с активным мониторингом и аналитикой поведения	Web Application Firewall (WAF), IDS/IPS, AI-сканирование, логирование и SIEM-интеграция

Далее представлены авторские рекомендации по реализации на каждом уровне:

1. Минимальный уровень. На этом этапе акцент делается на нейтрализацию самых массовых и распространённых атак:

— внедрение строгой серверной валидации данных (например, с использованием библиотеки class-validator для Nest.js);
— использование HTTPS с TLS 1.3 для всего трафика. Сегодня даже краткосрочная передача данных по HTTP способна стать точкой компрометации;
— настройка CSP-заголовков (Content Security Policy) для предотвращения внедрения вредоносного JavaScript;
— внедрение параметризованных SQL-запросов и ORM (например, Prisma или Sequelize), что исключает возможность SQL-инъекций;
— обязательная настройка HTTPOnly и Secure-флагов для cookie, чтобы минимизировать риск кражи сессий;
— использование двухфакторной аутентификации (2FA), например, через Google Authenticator.

Как отмечает Н.А. Шутько (2022), именно эти меры позволяют свести на нет до 60 % типовых атак на веб-приложения при сравнительно невысоких затратах на реализацию [6].

2. Базовый уровень. Здесь задача расширяется до контроля внутренних процессов и доступа между ролями:

— реализация RBAC-модели (role-based access control) с разграничением по ролям (администратор, рецензент, участник и т.д.);
— шифрование конфиденциальных данных в базе данных с использованием алгоритма AES-256;
— ведение истории сессий пользователей и автозавершение неактивных сессий;
— аудит входов и действий пользователей;
— регулярное сканирование на уязвимости с использованием инструментов, таких как ZAP или Acunetix;
— ограничение количества логинов с одного IP-адреса, антибот-защита.

По мнению А.Ж. Кинтоновой и соавт. (2020), внедрение контроля привилегий и механизмов аудита снижает риск эскалации доступа минимум на 40–45%, что критично при работе с рецензируемыми материалами и служебной информацией [7].

3. Максимальный уровень. На этом уровне защита перестаёт быть пассивной и приобретает черты постоянного мониторинга и проактивного реагирования:
— установка WAF (например, NGINX App Protect или ModSecurity) — фильтрация запросов с возможностью автоматической блокировки атак (SQLi, XSS, CSRF);
— интеграция с SIEM-системами (например, ELK Stack или Splunk) для централизованного сбора, анализа и корреляции событий;
— использование AI-алгоритмов и поведенческой аналитики для отслеживания аномалий (например, резкий рост активности IP-адреса, входы ночью, неожиданные пути доступа);
— настройка IDS/IPS-систем (Suricata, Snort) для обнаружения вторжений;
— постоянный мониторинг журналов активности с ретроспективным анализом.

С.В. Богомолов и Д.А. Демкин (2024) подчёркивают, что использование WAF-систем и SIEM-инструментов позволяет обнаруживать до 85 % сложных атак на раннем этапе, предотвращая их развитие [5].

Реализация предложенной многоуровневой модели безопасности обеспечивает последовательное снижение совокупного риска. В табл. 5 отражено ожидаемое снижение угроз и рисков.

Показатели основаны на анализе сценариев угроз с использованием формулы риска и данных из исследований М.М. Путято, А.С. Макаряна, В.В. Лещенко, В.О. Немчиновой (2022), а также на практиках OWASP [9]. Снижение достигается за счёт: устранения критичных уязвимостей (например, через CSP и фильтрацию),

Таблица 5.

Ожидаемое снижение угроз и рисков

Уровень защиты	До внедрения (средний R)	После внедрения (средний R)	Снижение риска
Минимальный	0.60	0.32	~ 47 %
Базовый	0.60	0.22	~ 63 %
Максимальный	0.60	0.12	~ 80 %

снижения вероятности успешной атаки (за счёт AI-мониторинга и поведенческого анализа), локализации последствий за счёт детальной логики разграничения доступа и сессионного контроля.

Предложенная трёхуровневая модель защиты веб-приложений позволяет гибко и последовательно выстраивать систему информационной безопасности с учётом реальных угроз, выявленных в 2025 году. Минимальный уровень обеспечивает базовую защиту от наиболее распространённых атак, включая SQL-инъекции и XSS. Базовый уровень усиливает контроль доступа и безопасность хранения данных, тогда как максимальный вводит проактивные меры, включая WAF, SIEM и поведенческую аналитику [10]. Комплексное внедрение предложенных мер способно снизить совокупный уровень риска на 47–80 %, в зависимости от глубины реализации. Подход может быть адаптирован под различные масштабы систем, обеспечивая как защиту локальных научных конференций, так и платформ федерального уровня.

Заключение

В рамках данной статьи были разработаны и предложены практические рекомендации по обеспечению информационной безопасности веб-платформы, предназначенной для проведения научных конференций. Учитывая специфику такой платформы — наличие различных ролей пользователей, обработку научных данных, публикационную активность и интеграцию с внешними сервисами особое внимание было уделено построению системной защиты, способной обеспечить надёжную и безопасную работу всех участников цифрового научного взаимодействия. Была обоснована необходимость многоуровневого подхода к информационной безопасности, который представлен в виде трёх уровней защиты: минимального, базового и максимального. Каждый из них ориентирован на конкретные классы угроз и предполагает реализацию соответствующих технических и организационных мер от базовой фильтрации и шифрования до внедрения систем активного мониторинга и WAF-технологий. Проведённая структурная оценка рисков позволила количественно измерить угрозы и определить приоритетные направления для защиты. На основе этой оценки сформированы предложе-

ния, реализация которых может снизить уровень угроз до 80 %, в зависимости от полноты внедрения. Общие выводы по статье включают:

1. Научно обоснована необходимость усиленного внимания к информационной безопасности в проектах веб-приложений научного профиля;
2. Выявлены и классифицированы основные риски, наиболее актуальные для 2025 года;
3. Разработана и предложена трёхуровневая модель защиты, охватывающая как базовые меры, так и продвинутые инструменты анализа и реагирования на инциденты;
4. Подготовлены конкретные рекомендации с указанием применимых решений (MFA, CSP, WAF, SIEM и др.), проверенных практикой;
5. Произведена оценка эффективности модели с учётом снижения рисков и повышения устойчивости приложения.

Представленная модель и предложенные меры универсальны и не ограничиваются сферой научных конференций. Они могут быть адаптированы и применены в других типах веб-приложений от образовательных платформ и медицинских информационных систем до корпоративных порталов и электронных сервисов органов власти, где критически важны надёжность, конфиденциальность и доверие пользователей. Подход, основанный на рациональном сочетании уровней защиты, позволяет выстраивать устойчивую архитектуру безопасности, сохраняющую свою эффективность даже в условиях быстро меняющейся цифровой среды.

ЛИТЕРАТУРА

1. Безопасность веб-приложений. Электронный ресурс. Режим доступа: https://www.tadviser.ru/index.php/Статья:Безопасность_веб-приложений (дата обращения 23.05.2025 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 24.05.2025 г.).
3. Иконников М.А., Карманов И.Н. Меры и требования к защищенным веб-приложениям // Интерэкспо Гео-Сибирь. 2019. №2. С. 13–19.
4. Лапина М.А., Багаутдинова А.Р., Загнетов Н. Исследование уязвимостей безопасности веб-приложений // Auditorium. 2024. №1 (41). С. 58–62.
5. Богомолов С.В., Демкин Д.А. Технология WAF и информационная безопасность // Вестник науки. 2024. №9 (78). С. 279–282.
6. Шутько Н.А. Теоретические понятия защиты WEB-приложений от уязвимостей // Вестник науки. 2022. №11 (56). С. 253–269.
7. Кинтонова А.Ж., Баенова Г.М., Урынбасарова А.Ж. Вопросы безопасности веб приложений // Colloquium-journal. 2020. №13 (65). С. 12–13.
8. Довгаль В.А., Шередько Д.И. Обеспечение информационной безопасности веб-сайта в условиях импортозамещения // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2022. №2 (301). С. 67–77.
9. Путято М.М., Макарян А.С., Лещенко В.В., Немчинова В.О. Анализ типовых уязвимостей при построении веб-приложений // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2022. №3 (306). С. 77–85.
10. Байраммырадов П., Довлетназаров Ш., Гарягдыева Г. Атаки на веб-приложения: уязвимости и способы защиты // Вестник науки. 2024. №10 (79). С. 835–838.

Журнал «Современная наука: актуальные проблемы теории и практики»