

опасной рабочей зоне, в стационарный диспетчерский центр, географически удаленный от производственной площадки. Реализация данной концепции требует применения технологий машинного зрения и предиктивной аналитики на базе машинного обучения. Данные технологии обеспечат не только управление механизмами, но и автоматический контроль технического состояния контейнеров, мониторинг соблюдения требований безопасности и оптимизацию использования парка оборудования.

Развитие мультимодальных терминалов является важной задачей в обеспечении интеграции национальных транспортных систем в международные логистические цепи. Для преодоления существующих ограничений, связанных с износом инфраструктуры, недостаточным уровнем цифровизации и дефицитом кадров, необходима реализация комплексного подхода. Он должен предусматривать не только техническое перевооружение объектов, но и внедрение интеллектуальных систем управления и роботизированных технологий.

СПИСОК ЛИТЕРАТУРЫ

1 Погрузочно-разгрузочные работы на железнодорожном транспорте : учеб. пособие : в 2 ч. Ч. I / Н. П. Берлин, В. Н. Кирик, Е. В. Настаченко ; М-во трансп. и коммуникаций Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2023. – 187 с.

2 Железнодорожный транспорт России: вызовы до 2025 года (доклад ИПЭМ) // Aftershock. – URL: <https://aftershock.news/?q=node/746091> (дата обращения: 16.05.2026).

3 **Шумаев, В. А.** Основы логистики : учеб. пособие / В. А. Шумаев. – М. : Юридический институт МИИТ, 2016. – 267 с.

Получено 18.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.

Вып. 31. Гомель, 2026

УДК 004.051

А. Э. ОРЕХВА, А. С. ШАЛАЕВА (ЭК-11)

Научный руководитель – канд. физ.-мат. наук *Е. А. ЗАДОРЖНИК*

ЭВОЛЮЦИЯ ВЕБ-УГРОЗ OWASP TOP 10 2025

Безопасность программного обеспечения в современных реалиях требует от команд разработки не просто точечного устранения ошибок, а стратегического подхода. Понимание динамики развития риска помогает выстроить такой процесс проектирования, тестирования и развертывания, который гарантирует устойчивость приложений к самым актуальным векторам атак.

Международный проект Open Worldwide Application Security Project (OWASP) выступает главным источником знаний в этой области. Его регулярный отчет OWASP Top 10 служит базовым ориентиром для разработчиков, DevOps-инженеров и аналитиков. И если отчет 2021 года фиксировал смещение фокуса в сторону архитектурных проблем (Security by Design), то обновленный стандарт OWASP Top 10 2025 отражает наступление эпохи искусственного интеллекта, тотальной интеграции API и усложнения цепочек поставок программного обеспечения (ПО) [1].

Ниже представлен актуальный список OWASP Top 10 2025, пришедший на смену редакции 2021 года [2]:

- 1 Нарушения управления доступом (Broken Access Control).
- 2 Уязвимости ИИ и интеграции LLM (AI and LLM Vulnerabilities).
- 3 Небезопасные дизайн и архитектура (Insecure Design).
- 4 Инъекции, включая Prompt Injection (Injections).
- 5 Уязвимости API и микросервисов (API Security Failures).
- 6 Атаки на цепочки поставок ПО (Software and Supply Chain Attacks).
- 7 Недостатки конфигурации и Cloud-сред (Security Misconfiguration).
- 8 Ошибка идентификации и управления сессиями (Identification and Authentication Failures).
- 9 Нарушение целостности ПО и данных (Software and Data Integrity Failures).
- 10 Недостатки логирования, мониторинга и видимости (Security Logging and Monitoring Failures).

Детальный разбор категорий OWASP Top 10 2025 и их отличие от 2021 года.

Нарушения управления доступом (Broken Access Control) – эта категория сохранила свое первое место с 2021 года, оставаясь самой частной и опасной уязвимостью, позволяющей злоумышленнику обойти ограничения и получить доступ к чужим учетным записям, конфиденциальным файлам или административным функциям. В отчете 2025 года значимость проблемы увеличилась из-за сложности B2B-интерфейсов и многопользовательских облачных платформ (Multi-tenancy), что требует обязательной проверки прав строго на стороне сервера для каждого запроса, использования централизованных механизмов контроля доступа (например, RBAC/ABAC) и повсеместного внедрения принципа «запрещено по умолчанию» [1].

Уязвимости искусственного интеллекта (ИИ) и интеграции LLM (AI and LLM Vulnerabilities) – абсолютно новое направление рисков, стремительно поднявшееся на второе место, отражает повсеместную интеграцию больших языковых моделей (LLM), чат-ботов и умных помощников, которые в 2021 году были редкостью. Опасность здесь заключается в возможности манипулирования моделью (jailbreaking), утечки конфиденциальных данных, на которых обучался ИИ, или выполнении ИИ-системой вредоносных команд в

бэкенде, для нейтрализации чего необходима жесткая изоляция контекста ИИ, фильтрации входных и выходных данных модели, а также строгое ограничение прав доступа ИИ-агентов к внутренним базам данных и API [1].

Небезопасные дизайн и архитектура (Insecure Design) – в 2025 году этот архитектурный пласт поднялся выше (занимал 4-е место в 2021 году), поскольку он связан не с ошибками в написании кода, а с фундаментальными просчетами на этапе планирования – например, созданием микросервисной архитектуры, где сервисы безоговорочно «доверяют» друг другу внутри периметра без взаимной аутентификации. Для минимизации этих рисков критически важны реализация концепции нулевого доверия (Zero Trust) на уровне архитектуры, регулярное моделирование угроз (Threat Modeling) до написания первой строчки кода и проведение постоянных стратегических ревизий [3].

Инъекции, включая Prompt Injection (Injections), классические SQL-, NoSQL-инъекции и инъекции команд операционной системы, доминировавшие в прошлые десятилетия, продолжают сдавать позиции благодаря защите на уровне современных фреймворков, однако к 2025 году данный вектор атаки серьезно трансформировался и теперь включает в себя инъекции в промты (Prompt Injection), когда пользователь через текстовое поле заставляет ИИ-компонент веб-приложения выполнить непредусмотренные действия. Противодействие этой угрозе требует как использования параметризованных запросов для традиционных баз данных, так и надежного разделения инструкций разработчика и пользовательского ввода на уровне API для ИИ-систем [1].

Уязвимости API и микросервисов (API Security Failures) в 2025 году, из-за того, что современные фронтенд-приложения (SPA) и мобильные бэкенды полностью построены на API, вошли в основной топ, объединив ошибки контроля доступа на уровне объектов (BOLA/IDOR), отсутствие лимитов на количество запросов (Rate Limiting) и избыточную выгрузку данных в JSON-ответах. Эффективная защита от подобных дефектов предполагает обязательное внедрение шлюзов безопасности (API Gateways), валидацию схем запросов и ответов, а также строгое ограничение частоты запросов (Throttling) [4].

Атаки на цепочки поставок ПО (Software and Supply Chain Attacks) – проблема, которая в 2021 году называлась «Уязвимые и устаревшие компоненты», серьезно эволюционировала: сегодня данный тип угроз заключается в том, что злоумышленники целенаправленно атакуют репозитории (npm, PyPI, NuGet), внедряя вредоносный код в популярные пакеты через перехват аккаунтов разработчиков или подмену имен (Typosquatting). Снижение этих рисков достигается за счет обязательного использования спецификации SBOM (Software Bill of Materials) для полного контроля состава ПО, автоматического аудита зависимостей в CI/CD пайплайнах и подписания коммитов цифровыми подписями [3].

Недостатки конфигурации и Cloud-сред (Security Misconfiguration) – этот сектор проблем поднялся выше из-за массового перехода на Cloude Na-

tive разработку, ведь если в 2021 году под этим чаще понимали включенный debug-режим на сервере, то в 2025 году это прежде всего ошибки в настройках доступа к облачным хранилищам (например, публичные AWS S3 бакеты), дефолтные конфигурации в кластерах Kubernetes и неверно настроенные политики CORS. Для исправления ситуации необходимо повсеместное использование подхода «Инфраструктура как код» (IaC) с автоматической проверкой безопасности конфигураций и регулярное сканирование облачной среды на предмет отклонений от эталона [4].

Ошибка идентификации и управления сессиями (Identification and Authentication Failures) – по сравнению с 2021 годом данный раздел рейтинга опустился ниже, так как большинство компаний внедрило многофакторную аутентификацию (MFA) и перешли на проверенные облачные провайдеры идентификации (OAuth, AuthO, Keycloak), однако атаки на угон сессий (Session Hijacking) и обход слабых реализаций MFA все еще представляют серьезную угрозу. Надежная защита здесь строится на переходе к беспарольной аутентификации (Passkeys, WebAuthn), защите сессионных куки специальными флагами (HttpOnly, Secure, SameSite) и внедрении систем адаптивного MFA [1].

Нарушение целостности ПО и данных (Software and Data Integrity Failures) – указанная уязвимость связана с принятием данных или обновлений программного обеспечения без надлежащей проверки их подлинности, причем в контексте 2025 года критическим фактором стало слепое доверие к данным, которые генерируют внешние плагины или ИИ-системы (проблема галлюцинаций данных), что может привести к порче баз данных приложения. Защитные меры в данном случае диктуют необходимость строгой валидации и верификации любых данных, поступающих из сторонних систем, а также обязательное использование цифровых подписей для файлов обновлений [1].

И наконец, Недостатки логирования, мониторинга и видимости (Security Logging and Monitoring Failures) замыкают список инструментального комплекса, который из простого сбора логов перерос в концепцию Observability (наблюдаемости), поскольку отсутствие глубокого мониторинга внутри контейнеров и микросервисов мешает вовремя заметить целенаправленную атаку, увеличивая среднее время обнаружения взлома до нескольких недель. Чтобы этого избежать, требуется создание централизованных систем сбора логов (SIEM), мониторинг подозрительной активности в реальном времени и настройка мгновенных оповещений (Alerting) для команды информационной безопасности при аномальном поведении API или ИИ-компонентов [4].

Каждые несколько лет OWASP пересматривает список актуальных угроз на основе изменений в реальном ландшафте угроз. На рисунке 1 можно увидеть, как сместился фокус с комплексных проблем архитектуры и контроля доступа (OWASP Top 10 – 2021) к новым глобальным вызовам искусственного интеллекта, безопасности API и цепочек поставок ПО (OWASP Top 10 – 2025) [1].

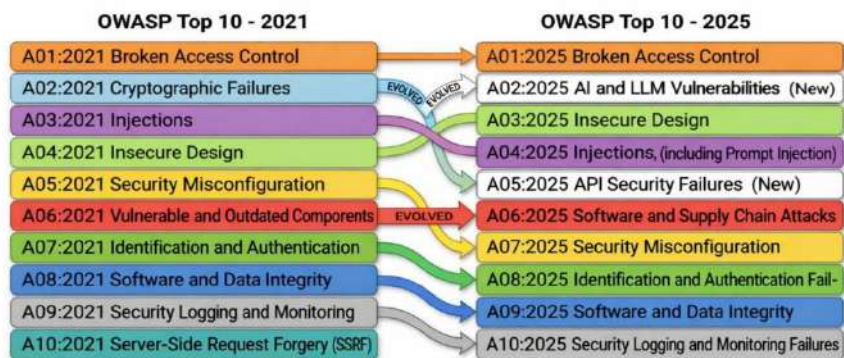


Рисунок 1 – Изменения в рекомендациях OWASP Top 10

Выпуск актуальной редакции OWASP Top 10 состоялся в конце 2025 года. Очередной плановый пересмотр перечня актуальных угроз и выпуск следующей версии стандарта ожидается в 2028–2029 годах.

OWASP Top 10 – это не просто справочник, а ключ к пониманию рисков, с которыми сталкивается любой разработчик или DevOps-инженер.

Крайне важно проводить регулярное тестирование приложений с учетом рекомендаций OWASP Top 10. Это может быть как автоматический анализ (SAST/Dast), так и ручной аудит кода вместе с пентестом [5]. Не менее важно строить процессы на принципах безопасного программирования (Secure by Design), внедряя валидацию данных, токенизацию и разграничение прав в культуру команды разработчиков ПО [3].

СПИСОК ЛИТЕРАТУРЫ

1 OWASP Top 10 // Open Worldwide Application Security Project (OWASP). – URL: <https://owasp.org/www-project-top-ten/> (дата обращения: 11.04.2026).

2 OWASP Top 10:2021. Основные риски безопасности веб-приложений // Open Worldwide Application Security Project. – URL: <https://owasp.org/Top10/> (дата обращения: 11.04.2026).

3 Методология безопасной разработки программного обеспечения (Secure by Design) // Агентство по кибербезопасности и инфраструктуре (CISA). – URL: <https://www.cisa.gov/resources-tools/resources/secure-by-design> (дата обращения: 11.04.2026).

4 Шаньгин, В. Ф. Информационная безопасность и защита информации в корпоративных сетях : учеб. пособие / В. Ф. Шаньгин. – М. : ДМК Пресс, 2023. – 512 с. – ISBN 978-5-97060-988-0.

5 Сканирование и аудит уязвимостей (SAST/DAST) // Информационный портал по кибербезопасности SecurityLab. – URL: <https://www.securitylab.ru> (дата обращения: 11.04.2026).

Получено 12.06.2026