

Поддержите миссию OWASP по улучшению безопасности программного обеспечения с помощью инициатив с открытым исходным кодом и обучения сообщества. [Пожертвуйте сейчас!](#)

[Магазин](#)[ТЫ ГЛАВ](#)[Пожертвовать](#)[агазин](#)[Присоединиться](#)[СОБЫТИЯ](#)[О](#)[Q](#)[Присоединиться](#)

## Топ-10 мобильных приложений OWASP

[Watch](#)

38

[Star](#)

94

[Основной](#)[Благодарности](#)

## Mobile Top 10 2024: финальные обновления релиза

Новый список Mobile Top 10 на 2024 год уже опубликован. Мы будем рады, если вы примете участие и внесете свой вклад в исследование, которое мы проводим.

[Присоединяйтесь к каналу SLACK](#)

Если у вас возникли какие-либо проблемы с присоединением к нам в Slack, пожалуйста, свяжитесь с руководителями проектов.

Давайте начнем!

Присоединяйтесь к нам на канале Slack и делитесь своими идеями!

**Фонд OWASP<sup>®</sup>** работает над повышением безопасности программного обеспечения посредством возглавляемых сообществом проектов по разработке программного обеспечения с открытым исходным кодом, сотен отделений по всему миру, десятков тысяч членов, а также путем проведения локальных и международных конференций.

### Другие мобильные проекты OWASP

Скоро появятся и другие обновления...

Ниже представлен рейтинг OWASP Mobile Top-10 за 2024 год.

## 10 главных мобильных рисков — финальная версия 2024 г.



- M1: Неправильное использование учетных данных
- M2: Недостаточная безопасность цепочки поставок
- M3: небезопасная аутентификация/авторизация
- M4: Недостаточная проверка ввода/вывода
- M5: небезопасная коммуникация
- M6: Недостаточный контроль конфиденциальности
- M7: Недостаточная двоичная защита
- M8: Неправильная конфигурация безопасности
- M9: небезопасное хранение данных
- M10: Недостаточная криптография

## Сравнение 2016 и 2024 годов

[Руководство OWASP по тестированию безопасности мобильных устройств](#)

**Репозиторий кода**

[Репозиторий Github](#)

## Лидеры

[Милан Сингх Такур](#)  
[Алаеддин МЕСБАХИ](#)  
[Кунвар Атул](#)  
[Мохамед Бенчих](#)

## Лучшие участники

[Мохаммед Джунаид](#)  
[Тарик](#)  
[Штеффен Лорц](#)

## Предстоящие глобальные мероприятия OWASP

[OWASP Global AppSec EC 2025](#)

- 26-30 мая 2025 г.

[OWASP Global AppSec USA 2025 — Вашингтон, округ Колумбия](#)

- 3-7 ноября 2025 г.

[OWASP Global AppSec USA 2026 – Сан-Франциско, Калифорния](#)

- 2-6 ноября 2026 г.

| Comparison Between 2016-2024  |   |                              |
|-------------------------------|---|------------------------------|
| OWASP-2016                    | OWASP-2024-Release                          | Comparison Between 2016-2024 |
| M1: Improper Platform Usage   | M1: Improper Credential Usage               | New                          |
| M2: Insecure Data Storage     | M2: Inadequate Supply Chain Security        | New                          |
| M3: Insecure Communication    | M3: Insecure Authentication / Authorization | Merged M4&M6 to M3           |
| M4: Insecure Authentication   | M4: Insufficient Input/Output Validation    | New                          |
| M5: Insufficient Cryptography | M5: Insecure Communication                  | Moved from M3 to M5          |
| M6: Insecure Authorization    | M6: Inadequate Privacy Controls             | New                          |
| M7: Client Code Quality       | M7: Insufficient Binary Protections         | Merged M8&M9 to M7           |
| M8: Code Tampering            | M8: Security Misconfiguration               | Rewording [M10]              |
| M9: Reverse Engineering       | M9: Insecure Data Storage                   | Moved from M2 to M9          |
| M10: Extraneous Functionality | M10: Insufficient Cryptography              | Moved from M5 to M10         |

**Уязвимости, которые не попали в первоначальный список исправлений, но в будущем мы, возможно, рассмотрим их.**

- Утечка данных
- Жестко закодированные секреты
- небезопасный контроль доступа
- Перезапись пути и обход пути
- незащищенные конечные точки (Deerlink, Activity, Service...)
- небезопасный обмен

## **10 главных мобильных рисков — окончательный список 2016 г.**

- [M1: Неправильное использование платформы](#)
- [M2: небезопасное хранение данных](#)
- [M3: небезопасная коммуникация](#)
- [M4: небезопасная аутентификация](#)
- [M5: Недостаточная криптография](#)
- [M6: небезопасная авторизация](#)
- [M7: Качество клиентского кода](#)
- [M8: Подделка кода](#)
- [M9: Обратное проектирование](#)
- [M10: Посторонние функции](#)

# 10 главных мобильных рисков — окончательный список 2014 г.

- M1: Слабый контроль на стороне сервера
- M2: небезопасное хранение данных
- M3: Недостаточная защита транспортного уровня
- M4: Непреднамеренная утечка данных
- M5: Плохая авторизация и аутентификация
- M6: Нарушенная криптография
- M7: Внедрение на стороне клиента
- M8: Решения по безопасности с использованием ненадежных входных данных
- M9: Неправильная обработка сеанса
- M10: Отсутствие двоичной защиты

---

 [Редактировать на GitHub](#)

## В центре внимания: ОккамСек



OccamSec преуспевает в предоставлении широкого спектра услуг, включая тестирование на проникновение, непрерывное тестирование на проникновение, операции красной команды, взаимодействие фиолетовой команды и исследование уязвимостей.

Приверженность передовым методологиям позволяет организациям укреплять свою позицию безопасности и заблаговременно обнаруживать и устранять уязвимости до того, как они могут быть использованы.

## Корпоративные спонсоры





[Станьте корпоративным сторонником](#)

[HOME](#) [PROJECTS](#) [CHAPTERS](#) [EVENTS](#) [ABOUT](#)



[КОНФИДЕНЦИАЛЬНОСТЬ](#) [КАРТА САЙТА](#) [КОНТАКТ](#)

OWASP, логотип OWASP и Global AppSec являются зарегистрированными товарными знаками, а AppSec Days, AppSec California, AppSec Cali, SnowFROC и LASCON являются товарными знаками OWASP Foundation, Inc. Если не указано иное, весь контент на сайте имеет лицензию Creative Commons Attribution-ShareAlike v4.0 и предоставляется без гарантии обслуживания или точности. Для получения дополнительной информации см. наш [Общий отказ от ответственности](#). OWASP не одобряет и не рекомендует коммерческие продукты или услуги, что позволяет нашему сообществу оставаться нейтральным по отношению к поставщикам с коллективной мудростью лучших умов в области безопасности программного обеспечения во всем мире. Авторские права 2024, OWASP Foundation, Inc.