УДК 004.45

УЯЗВИМОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Шафикова А.Э., студент гр. 28107, 1 курс магистратуры
Научный руководитель: Лямов Ю.О., ст. преп.
Лениногорский филиал Казанского национального исследовательского технического университета им. А.Н. Туполева–КАИ, г. Лениногорск

С точки зрения терминологии, мобильные приложения – это разновидность прикладного программного обеспечения, предназначенное для упрощения выполнения задач, обеспечения различными сервисами и использования на мобильных и портативных устройствах. Но простыми словами, мобильное приложение – неисчерпаемый источник информации о человеке. Поэтому данная сфера занимает лидирующие позиции среди уязвимых областей кибербезопасности.

Существует множество рейтингов уязвимостей мобильных приложений, которыми пользуются специалисты по обеспечению безопасности. Самым популярным является OWASP Top 10. На основе полученных статистик составляется широкий консенсус относительно наиболее важных рисков безопасности. Крайнее обновление произошло в мае 2025 года [4]:

1. Нарушение контроля доступа

Данная уязвимость возглавляет список OWASP Top 10 который год. Это связано с большим кругом возможностей по реализации атаки на безопасность приложения, поскольку практически каждое приложение запрашивает персональные данные пользователя.

В 2025 году системы управления доступом стали главной мишенью хакеров. С распространением микросервисных архитектур и serverless-функций разработчики часто забывают о последовательной проверке прав доступа. Типичная ситуация: функция доступна всем аутентифицированным пользователям, хотя должна быть ограничена для администраторов.

Эта уязвимость имела огромную популярность еще в 2021 году, когда в API Peloton пользователи смогли получать доступ к данным аккаунта другого пользователя, поскольку был неправильно настроен процесс аутентификации на уровне объекта.

2. Неправильная настройка безопасности

Эта уязвимость связана с слабыми настройками по умолчанию, непоследовательные средства контроля безопасности в разных средствах. Настройки приложения, сервера и других компонентов системы не являются безопасными: отсутствие или ненадежные настройки аутентификации, авторизации и доступа. В этом случае можно взломать административную панель и совершить незаконные действия.

Данный вид уязвимости, по сравнению с рейтингом 2021 года, приобретает большую популярность [5].

3. Сбои в цепочке поставок программного обеспечения

Является расширенным вариантом «Уязвимых и устаревших компонентов», представленных в рейтинге в 2021 году на 6 месте. Включает более широкий спектр компрометаций, происходящих внутри или через зависимости ПО, систем сборки и инфраструктуры распространения.

4. Недостатки криптографии

С масштабным развитием квантовых компьютеров привычные для специалистов алгоритмы шифрования, как RSA и ECC, стали уязвимы. Алгоритмы уязвимы к атакам с использованием алгоритма Шора на квантовом компьютере.

Недостаточность шифрования данных может привести к большим последствиям. В 2022 году злоумышленники получили доступ к хранилищам LastPass, где лежали пароли, логины, незашифрованные метаданные.

5. Инъекции

Наиболее часто тестируемая категория уязвимостей. В рамках эксплуатации злоумышленник использует вредоносный код или команды (запросы) для получения данных, необходимых для дальнейшей реализации атаки.

Приложение уязвимо для такого типа атаки, если предоставленные пользователем данные не проверяются приложением, или динамические запросы напрямую используются в работе, или несанированные данные в параметрах поиска для извлечения чувствительных записей.

6. Ненадежная архитектура

Это также обширная категория основывается на «отсутствии или неэффективности проектирования средств контроля». Например, высокая связанность компонентов друг от друга (изменение в одном месте ломает остальные), использование устаревших технология или отсутствие масштабируемости (система не справляется с ростом нагрузки).

7. Неправильная аутентификация и управление сессиями

Уязвимость связана с отсутствием встроенной валидации пароля и многофакторной аутентификации, примитивные токены, сессии и утечки идентификаторов сессий.

За ее реализацией следует захват учетных записей, а следом несанкционированный доступ к конфиденциальным данным.

В 2020 году хакеры использовали слабые пароли взломали камеры Ring и получили доступ к видеопотокам, что привело к нарушению приватности тысячи пользователей.

8. Сбои целостности ПО или данных

Подобные сбои возникают, когда приложение не проверяется подлинность и целостность получаемых данных, поэтому злоумышленники способны подменить информацию, внедрить вредоносный код, тем самым нарушить работу системы.

К частым причинам возникновения такой уязвимости относят использование устаревших или ненадежных библиотек, загрузка обновления из ненадежных источников или без проверки их подлинности.

В 2020 году произошел инцидент с SolarWinds. Компонент программы обновлялся через официальный сервер разработчиков,а в один из пакетов обновлений внедрили вредоносный код.

9. Сбои журналирования и оповещения

Представленные проблемы связаны с тем, что система перестает корректно записывать события или отправлять уведомления о критических событиях, что затрудняет реагирование на инциденты безопасности.

Проблемы с ресурсами (нехватка памяти или GPU на сервере), ошибка конфигурации, сбои сервиса, проблемы сети или ошибки в коде приложения являются причинами подобных уязвимостей.

10. Некорректная обработка исключительных ситуаций

Это некорректное написание кода, который должен перехватывать и реагировать события, возникающее во время работы программы, которое отклоняется от нормального хода выполнения.

Примерами этой проблемы могут быть: полное отсутствие обработки, пустые блоки, логирование неинформативных сообщений, неправильное восстановление.

Данный рейтинг обновляется в течение некоторого промежутка времени, последнее было 4 года назад. За это время сфера кибербезопасности претерпела изменения.

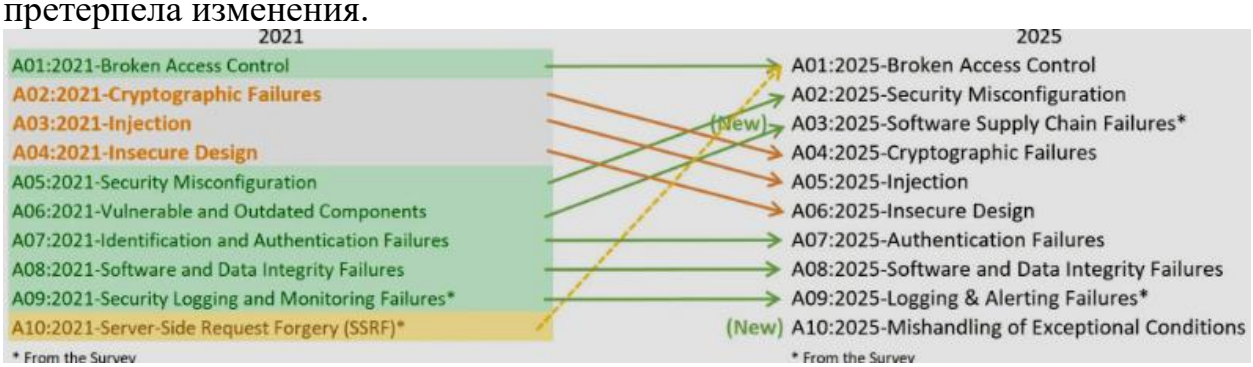

Рисунок 1 – Сравнение рейтингов OWASP Top 10 за 2021 и 2025 годы

Опираясь на рисунок 1, можно сделать несколько выводов о тенденции кибербезопасности программного обеспечения. Некоторые категории остались в рейтинге на своих позициях, сохраняя свою популярность. В обновленном списке к каждой позиции добавлены дополнительные уточнения, например, расширены категории с учетом обновленных данных, смещены акценты. К тенденциям и изменениям между данными рейтингами можно отнести следующее:

– больший упор на облачную безопасность и инфраструктуру как код, поскольку многие категории адаптированы под облачные паттерны угроз;
– особое внимание обратили на безопасность цепочки поставок;
– рост внимания к API- и микросервисным проблемам;

– упор на моделирование угроз на ранних стадиях разработки программного обеспечения;

– автоматизация безопасности: IAC-сканеры, SAST/DAST в CI.

Список литературы:

1. ГОСТ Р 56545 – 2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Введ. 2016-04-01. М.: Стандартинформ, 2015. 22 с.
2. Косов Н. А., Голубничев И. А. Анализ Уязвимостей Мобильных Приложений На Android //Экономика и качество систем связи. – 2023. – №. 1 (27). – С. 84-91.
3. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. №1(1). С. 44-48.
4. OWASP Top Ten Web Application Security Risks // OWASP Top 10 URL: https://share.google/FVeOqFjCDJ0Du1SMj (дата обращения: 01.02.2026).
5. OWASP Топ-10 (2025) // SEC-1275-1 URL: https://1275.ru/articles/owasp-top-10-2025_16183 (дата обращения: 07.02.2026).