DOI 10.37882/2223-2966.2023.12-2.31

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ И УГРОЗ ПРИ РАЗРАБОТКЕ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

RESEARCH OF VULNERABILITIES AND THREATS IN THE DEVELOPMENT OF MOBILE APPLICATIONS

I. Tarasova

Summary. Information security and data protection are a mandatory part of software development. The largest market volume in software development is occupy by mobile applications. The purpose of this article is to conduct a study of the most relevant threats and vulnerabilities related to the development of mobile applications. The scientific value of the article consists in an attempt to comprehensively investigate the issue and systematize knowledge about the most pressing threats in the development of mobile applications. The materials of the article can become indispensable information for modern developers pursuing the goal of creating efficiently and safely functioning mobile applications.

Keywords: mobile application, information security, data protection, threat, vulnerability, software.

Тарасова Юлия Андреевна
Инженер-программист,
ООО «Антифишинг» (Санкт-Петербург)
tarasovayuliya00@gmail.com

Аннотация. Информационная безопасность и защита данных являются обязательной частью при разработке программного обеспечения. Наибольший объем рынка в разработке программного обеспечения занимают именно мобильные приложения. Цель представленной статьи заключается в проведении исследования наиболее актуальных угроз и уязвимостей, относящихся к разработке мобильных приложений. Научная ценность статьи состоит в предпринимаемой попытке комплексного исследования вопроса и систематизации знаний относительно наиболее актуальных угроз при разработке мобильных приложений. Материалы статьи могут стать незаменимой информацией для современных разработчиков, преследующих цель создания эффективно и безопасно функционирующих мобильных приложений.

Ключевые слова: мобильное приложение, информационная безопасность, защита данных, угроза, уязвимость, программное обеспечение, разработка, информационные технологии, фишинг, защита данных.

Введение

Современные мобильные приложения являются ключевым звеном в мире информационных технологий. Вычислительные мощности мобильных устройств позволяют разработать программы любой сложности, предназначенных для решения как бытовых, так и профессиональных задач. Вместе с этим, особенно остро встает вопрос, связанный с аспектами информационной безопасности при разработке мобильных приложений.

На сегодняшний день выделяется целое множество угроз и уязвимостей, которые наблюдаются при разработке мобильных приложений. Основная угроза в рамках данного вопроса связана с возможностью хищение конфиденциальной информации и фальсификации данных. В связи с этим, актуализируются задачи, связанные с исследованием уязвимостей и угроз, а также разработкой эффективных инструментов для обеспечения защиты мобильных устройств [1, 2].

Актуальность вопроса подтверждается и статистическими данными, на которых прослеживается значительное увеличение объемы рынка мобильных приложений. Главная проблема заключается и в том, что вместе с увеличением рынка, растет и количество угроз информационной безопасности. Так, представленная работа более подробно отражает такие аспекты, как уязвимости, угрозы и методы по защите от них при разработке мобильных приложений. В работе отражается результат комплексного исследования вопроса, который может быть использован на практике при разработке приложений для мобильных устройств.

Результаты и обсуждение

Развитие мобильных приложений стало неотъемлемой частью современного цифрового мира, которое отражает технологический прогресс и изменения в повседневной жизни. В наше время мобильные устройства перешли далеко за пределы простых средств связи, превратившись в мощные инструменты для общения, работы и развлечений. В бизнес-сфере мобильные приложения открывают новые возможности для привлечения клиентов, улучшения сервиса и увеличения эффективности операций. Компании активно инвестируют в разработку приложений, чтобы создать уникальный пользовательский опыт и поддерживать конкурентоспособность. В области здравоохранения, образования и государственного управления мобильные приложения помогают оптимизировать процессы, улучшать доступ к информации и повышать общественную эффективность. Таким образом, разработка мобильных приложений продолжает играть ключевую роль в формировании современной информационной среды, обогащая наш повседневный опыт и улучшая различные аспекты жизни и бизнеса [3].

Об этом же свидетельствуют и статистические данные, отражающие ежегодный прирост объема инвестиций в данный рынок. На рис. 1 представлены диаграммы, на которых изображена динамика изменения в период с 2022 по 2023 год.

Однако вместе с рядом преимуществ, высокая популярность мобильных приложений несет с собой и множество проблем, ключевой из которых является информационная безопасность. Проблема информационной безопасности при разработке мобильных приложений является одной из наиболее актуальных и серьезных в цифровой эпохе. Мобильные приложения собирают и обрабатывают огромное количество данных о пользователях, таких как личная информация, финансовые данные и геолокационные сведения. Ответственность за защиту этих данных лежит на разработчиках приложений, и любые уязвимости или недоразумения в этой области могут иметь серьезные последствия [4].

Одной из главных угроз является возможность несанкционированного доступа к данным пользователей, что может привести к утечкам информации или злоупотреблению ею. Также важно обеспечить защиту от вредоносных программ и взломов, которые могут повредить как само приложение, так и устройство пользователя. Борьба с фишингом и социальной инженерией также остается актуальной задачей.

Разработчики должны активно следить за обновлениями безопасности, использовать современные методы шифрования и аутентификации, а также проводить регулярные аудиты безопасности для выявления и устранения уязвимостей. Все это подчеркивает, что информационная безопасность является неотъемлемой частью разработки мобильных приложений и требует постоянного внимания и инвестиций.

При разработке мобильных приложений существует ряд серьезных угроз и уязвимостей, которые могут потенциально подвергнуть риск безопасность приложения и данных пользователей. Вот некоторые из них:

— несанкционированный доступ и утечка данных. Злоумышленники могут попытаться проникнуть в приложение и получить доступ к личным данным пользователей, таким как имена, адреса электронной почты, финансовые сведения и другая чувствительная информация. Утечка таких данных может привести к серьезным последствиям для пользователей и разработчиков;
— вредоносные программы и мошенничество. Загрузка вредоносных приложений или изменение существующих может повредить устройства пользователей, воровать информацию или злоупотреблять доступом. Мошенничество, включая фишинг и социальную инженерию, также представляет угрозу для пользователей;
— недостаточная аутентификация и управление сеансами. Плохая аутентификация или недостаточное управление сеансами может оставить открытыми двери для несанкционированного доступа. Это может привести к компрометации аккаунтов пользователей;
— недостаточная защита хранилища данных. Если приложение хранит данные на устройстве пользователя или на серверах, они должны быть надежно защищены. Недостаточная защита может привести к утечкам данных;
— недостаточное обновление и поддержка. Отсутствие регулярных обновлений безопасности

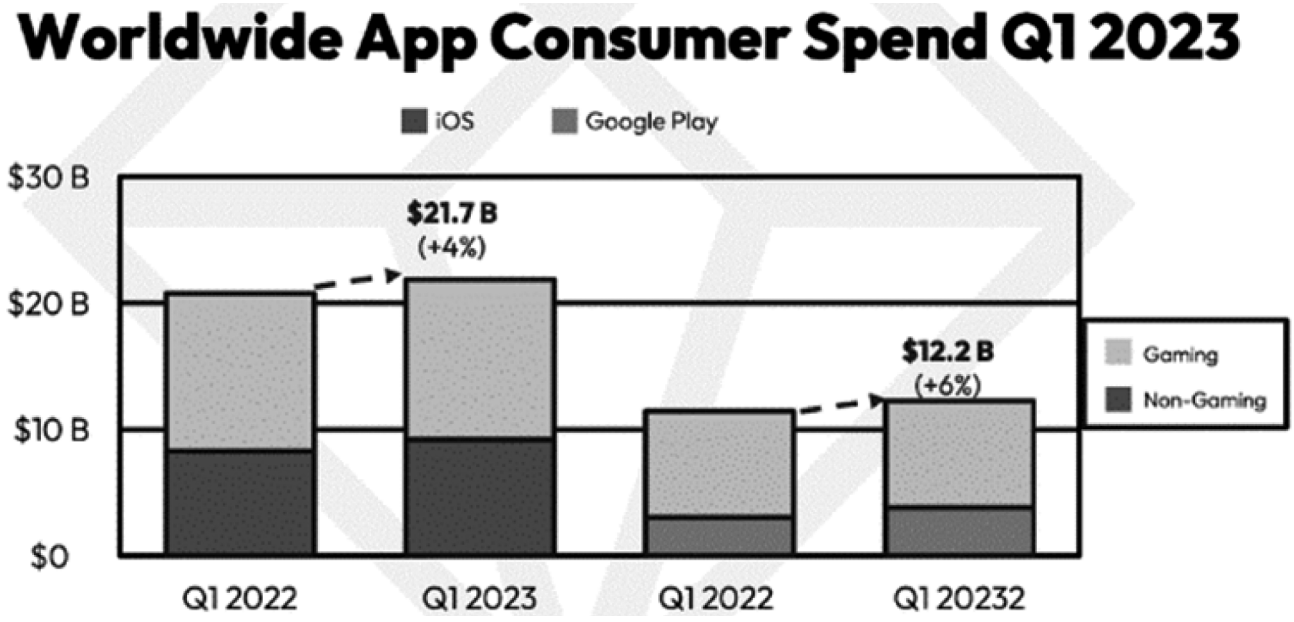

Рис. 1. Динамика изменения объема инвестиций в рынок мобильных приложений

и поддержки приложения может оставить уязвимости без устранения, что делает его подверженным атакам с течением времени;
— неадекватное тестирование. Недостаточное тестирование на уровне безопасности может привести к не выявленным уязвимостям и ошибкам в приложении [5].

Каждая из данных угроз имеет свой уровень распространения и риска. Для предотвращения этих угроз и уязвимостей, разработчики должны активно следить за безопасностью приложения, проводить тщательное тестирование, использовать современные методы шифрования и аутентификации, а также регулярно обновлять приложение с учетом изменяющейся среды угроз [6, 7].

Так, на сегодняшний день получило актуальность направление создания специализированных инструментов, предназначенных для выявления угроз и уязвимостей при разработке мобильных приложений. Одним из наиболее эффективных из таких инструментов считается инновационный продукт MAST — метод анализа мобильных приложений (Mobile Application Security Testing, MAST). Он является критически-важным инструментом для выявления угроз и уязвимостей в мобильных приложениях. MAST включает в себя широкий спектр методик и инструментов, предназначенных для тестирования безопасности мобильных приложений на предмет возможных уязвимостей (рис. 2).

Основными задачами MAST являются обнаружение уязвимостей, связанных с недостаточной аутентификацией, несанкционированным доступом, недостаточной защитой данных, а также других потенциальных проблем с безопасностью. Этот метод анализа может также оценить мобильное приложение на предмет соответствия стандартам безопасности и рекомендациям. Именно на основе данного инструмента разработчики получают возможность исключить уязвимости на этапе разработки приложения, что снижает риски для пользователей и бизнеса. Этот подход важен в контексте растущей угрозной среды и повышенного интереса со стороны злоумышленников к мобильным приложениям. Таким образом, MAST является неотъемлемым инструментом в обеспечении безопасности мобильных приложений и защите данных пользователей [8, 9].

Существует также множество инструментов и платформ, аналогичных MAST, предназначенных для анализа безопасности мобильных приложений. Одними из наиболее популярных и эффективных являются:
— Static Application Security Testing (SAST). Этот тип инструментов проводит анализ исходного кода мобильного приложения на предмет потенциальных уязвимостей. Он может выявлять проблемы безопасности, такие как недостаточное шифрование данных и недостаточная обработка ввода данных;
— Dynamic Application Security Testing (DAST). DAST сканирует работающее приложение в режиме реального времени, пытаясь обнаружить уязвимо-

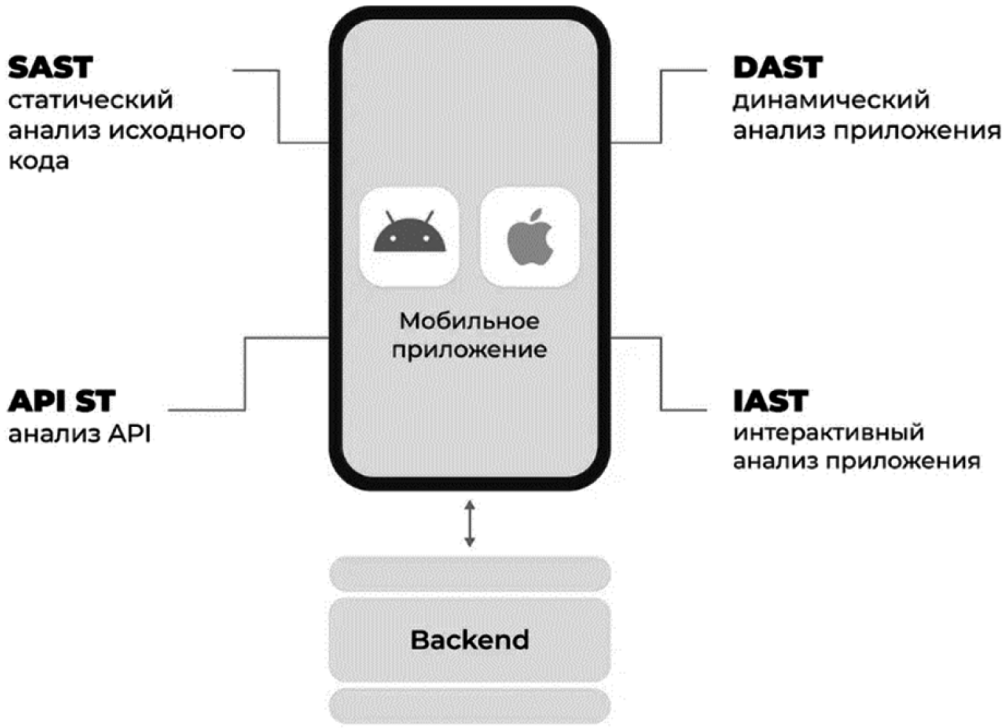

Рис. 2. Направления использования инструмента MAST

сти во взаимодействии с приложением, такие как утечки данных и проблемы аутентификации;
— Interactive Application Security Testing (IAST). IAST комбинирует элементы SAST и DAST, анализируя код и работу приложения в реальном времени. Это позволяет выявлять уязвимости, связанные с конкретными сценариями использования;
— Mobile App Security Frameworks. Существуют фреймворки, которые предоставляют советы и рекомендации по тестированию безопасности мобильных приложений. Данные инструменты предоставляют набор проверок безопасности, которые можно выполнить вручную и определить актуальные угрозы и уязвимости безопасности [10].

Так, исследование угроз и уязвимостей безопасности мобильных приложений — это важный процесс, направленный на обнаружение и анализ потенциальных уязвимостей, которые могут быть использованы злоумышленниками для атак на приложения и устройства пользователей. В ходе исследования угроз проводится анализ кода приложения, его архитектуры и конфигураций, а также взаимодействия с внешними ресурсами и серверами. Это позволяет выявить возможные слабые места, такие как недостаточная обработка ввода данных, отсутствие аутентификации и авторизации, недостаточная защита хранимых данных и другие потенциальные уязвимости [11, 12].

При этом для анализа угроз могут использоваться инструменты сканирования, статический и динамический анализ кода, а также тестирование на проникновение, а также ряд иных методов специальных инструментов. Результатом исследования является список выявленных уязвимостей и рекомендации по их устранению, что позволяет повысить безопасность мобильного приложения и защитить пользователей от потенциальных атак.

Заключение

Таким образом, основной целью представленной статьи являлось выполнение анализа относительно вопроса исследования угроз и уязвимостей при разработке мобильных приложений. В рамках работы проведен комплексный анализ и представлены результаты исследования относительно таких вопросов, как актуальность разработки мобильных приложений и увеличение степени актуальности их защищенности, наиболее актуальные и требующие особого внимания угрозы и уязвимости при разработке мобильных приложений, методы и средства по их противодействию, а также обеспечению защищенной и эффективной работы для пользователя.

В заключение необходимо отметить, что представленные к рассмотрению вопросы имеют одну из наибольших актуальностей среди других проблем в сфере информационных технологий, что связано с повсеместным использованием мобильных устройств. Именно высокий уровень защищенности данных и информационной безопасности в целом способны обеспечить наиболее эффективную и оптимальную работу с такими приложениями. Материалы работы могут стать полезным инструментом для разработчиков, в задачи которых входит устранение угроз и уязвимостей при создании мобильных приложений.

ЛИТЕРАТУРА

1. Войнов А.С. Исследование уязвимостей и угроз в мобильных приложениях: стратегии противодействия // Вестник науки. 2023. №9 (66). С. 195–200.
2. Хромова А.Р., Петросян Л.Э. Анализ уязвимостей в системах безопасности данных // Инженерный вестник Дона. 2023. №6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8447.
3. Косов Н.А., Голубничев И.А. Анализ уязвимостей мобильных приложений на android // Экономика и качество систем связи. 2023. №1 (27). С. 84–91.
4. Казюлин Р.В., Чернышов Н.Г. Тестирования безопасности приложений // Инженерный вестник Дона. 2021. №5. URL: ivdon.ru/ru/magazine/archive/n5y2021/6947.
5. Фатхи В.А., Дьяченко Н.В. Разработка модели угроз android приложений, свойственных ошибкам разработчика // I-methods. 2022. №2. С. 4-12.
6. Barkan E., Biham E., Keller N. Instant ciphertext-only cryptanalysis of GSM encrypted communication // Journal of Cryptology. — 2008. — Т. 21. — № 3. — С. 392–429.
7. Коромыслов К.Е., Красов А.В., Ушаков И.А. Разработка модели угроз android приложений, свойственных ошибкам разработчика // I-methods. 2022. №2. С. 4–12.
8. Ревенков П.В., Крупенко Д.С. Оценка рисков информационной безопасности в условиях применения систем мобильного банкинга // Вопросы кибербезопасности. 2019. №2 (30). С. 21–28.
9. Бурлаков М.Е., Алейнов Ю.В., Голубых Д.А. Исследование динамики активности обнаружения угроз в мобильных операционных системах и программах обмена сообщениями // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. 2017. С. 141–151.
10. Путято М.М., Макарян А.С., Карманов М.А., Немчинова В.О. Сравнительный анализ существующих методик исследования защищенности мобильных приложений // Прикаспийский журнал: управление и высокие технологии. 2022. №4 (60). С. 89–97.
11. Diasamidze S. V. Implementation of the Role Based Access Control in Application for Mobile Device on the Android OS Platform / S. V. Diasamidze, E. Yu. Kuzmenkova, D. A. Kuznetsov, A. R. Sarkisyan // Интеллектуальные технологии на транспорте, 2016, № 1. С. 21–26.
12. Зубков К.Н., Диасамидзе С.В. Проблемы защиты информации в приложениях для мобильных систем // Интеллектуальные технологии на транспорте. 2017. №2. С. 40–46.

© Тарасова Юлия Андреевна (tarasovayuliya00@gmail.com)
Журнал «Современная наука: актуальные проблемы теории и практики»