

**УДК 004.056.**

**Разработка защищенного мобильного приложения для платформы iOS с учетом современных угроз информационной безопасности.**

**Пинигин Д. (ИТМО)**

**Научный руководитель – Ассистент Мухамеджанов С.  
(ИТМО)**

**Введение.** Современные мобильные приложения играют ключевую роль в повседневной жизни пользователей, обеспечивая доступ к различным сервисам и данным. Однако с ростом популярности мобильных устройств увеличиваются и угрозы информационной безопасности, что требует разработки надежных решений для защиты данных и обеспечения конфиденциальности. Разработка защищенного мобильного приложения для платформы iOS с учетом современных угроз информационной безопасности становится важной задачей, поскольку она направлена на минимизацию рисков утечек данных и атак на устройства пользователей. Установление связи между архитектурой приложения, методами защиты и механизмами обеспечения безопасности данных имеет практическое значение, так как это позволяет создавать решения, которые обеспечат высокий уровень защиты и соответствуют требованиям безопасности. Актуальность исследования также определяется растущей зависимостью бизнеса и частных пользователей от мобильных приложений, что делает необходимость защиты данных особенно важной для их функционирования [1].

**Основная часть.** С помощью современных методов разработки и инструментов создаются мобильные приложения, учитывающие актуальные угрозы информационной безопасности. Одной из важнейших задач является разработка защищенного мобильного приложения для платформы iOS, которое способно эффективно противодействовать современным киберугрозам.

При разработке мобильных приложений особое внимание уделяется следующим вопросам [3]:

1. **Безопасность хранения данных.** Это включает защиту пользовательской информации, хранимой в локальной памяти устройства, через использование шифрования данных, безопасных хранилищ (например, Keychain), а также управление доступом к этим данным.
2. **Защита данных при передаче.** Для обеспечения конфиденциальности информации, передаваемой между приложением и сервером, применяются современные методы криптографической защиты, такие как SSL/TLS. Важно также учитывать защиту от атак типа "man-in-the-middle", использование сертификатов безопасности и механизмы верификации серверов.
3. **Аутентификация и авторизация.** Для защиты от несанкционированного доступа к приложению используются многофакторная аутентификация (MFA), биометрия (Touch ID, Face ID), а также безопасные механизмы авторизации с использованием токенов и OAuth2.
4. **Защита от вредоносных программ и уязвимостей.** Современные угрозы включают использование руткитов и вирусов для взлома мобильных устройств. Для противодействия этому применяются методы безопасности на уровне самой операционной системы, такие как системы защиты от выполнения вредоносного кода.

Таким образом, защита мобильных приложений на платформе iOS от современных угроз требует комплексного подхода, включающего как технические, так и организационные меры, направленные на снижение рисков и повышение уровня безопасности данных пользователей.

**Выводы.** Проведен анализ уязвимостей мобильных приложений и разработана методика защиты с использованием определенных технологий. При разработке приложения будут решены следующие проблемы: безопасная авторизация, биометрическая аутентификация, безопасное хранение данных.

**Список использованных источников:**

1. Positive Technologies. Статистика уязвимости финансовых приложений [Электронный ресурс].  
<https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Mobile-Application-Vulnerabilities-and-Threats-2019-rus.pdf>
2. Positive Technologies. Уязвимости и угрозы мобильных приложений, 2019 [Электронный ресурс].  
<https://www.ptsecurity.com/ru-ru/research/analytics/mobile-application-security-threats-and-vulnerabilities-2019/>
3. Перспективный мониторинг. Анализ мобильных приложений [Электронный ресурс].  
<https://amonitoring.ru/service/security-analysis/mobile-app/>