О подходе к обеспечению защищённости мобильных устройств

А.А. Обласов, Д.В. Воропаев

Комсомольский-на-Амуре государственный университет

Аннотация: В работе рассмотрен подход к комплексному обеспечению защищённости мобильных устройств, являющихся основными инструментами для общения, совершения банковских операций и использования медицинских сервисов, содержащих пароли, документы и переписки. Защита мобильных устройств рассмотрена на нескольких уровнях. Выделены уровни защиты мобильных платформ, приложений, операторов связи, а также пользовательский уровень. Проведён анализ атак на мобильные устройства и выделены векторы наиболее распространённых видов атак. Проведён сравнительный анализ мобильных платформ iOS и Android, выделены их сильные и слабые стороны. Проведён анализ основных направлений защиты мобильных устройств со стороны операторов связи. Проведён анализ некоторых успешных атак на мобильные банковские системы и приведена классификация основных угроз для мобильных банков.
Ключевые слова: защита мобильных устройств, кибератака, вектор атаки, Android, iOS, методы защиты приложений, мобильные банковские системы.

Введение

Актуальность обеспечения эффективной защиты мобильных устройств в 2024 – 2026 годах достигла критического уровня из-за тотальной цифровизации, хранения банковских/персональных данных в смартфонах, планшетах, стабильного роста количества уязвимостей и постоянного совершенствования сложных, многоуровневых атак, использующих искусственный интеллект (далее ИИ) [1,2].

Средства и методы защиты мобильных устройств непрерывно развиваются и совершенствуются. Производители устройств, разработчики мобильных платформ, приложений, мобильных банковских систем, операторы связи и, конечно, сами пользователи мобильных устройств, каждый на своём уровне обеспечивают безопасность мобильных устройств.

Количество обнаруженных уязвимостей мобильных приложений ежегодно бьёт рекорды, превышая десятки тысяч. Киберпреступники автоматизируют поиск уязвимостей и создают более сложные схемы проникновений [3]. Угрозы кибербезопасности делают защиту мобильных

устройств необходимой как для частных лиц, так и для корпоративного сектора.

В 2024 году финансовые потери от кибератак и мошенничества, совершаемых преимущественно через мобильные устройства и социальную инженерию, достигли рекордных значений: 1 трлн. рублей и в России и 9,5 трлн. долларов в мире [4]. При этом, Россия остается одной из главных целей на которую приходится в 2024 году – 14%, а уже в 2025 году – 16% всех мировых кибератак [4].

Основными векторами для успешных атак являются: социальная инженерия, вредоносное программное обеспечение (далее ПО) и некачественное написание кода. Мобильные приложения являются основным каналом доступа к финансовым и личным данным. Количество уязвимостей увеличивается ежегодно, превышая 25 тыс. в год [1]. Кроме того, злоумышленники активно используют ИИ для быстрого нахождения уязвимостей.

Статистические данные демонстрируют, что 76% мобильных приложений содержат уязвимости в хранении данных, и 89% этих уязвимостей уже эксплуатируются вредоносным ПО [1]. В результате кража учетных записей и перехват транзакций приводят к значительным финансовым потерям.

В таких условиях мобильные устройства стали мишенью номер один для киберпреступников. Пользователи часто сталкиваются с попытками мошенничества через короткие сообщения (Short Message Service – SMS-сообщения), звонки и электронные письма. Многие пользователи хранят важные данные в облаке, которое связано с мобильными устройствами. Взломанное устройство компрометирует доступ к облачным сервисам. Потеря или кража мобильного устройства представляет риск утраты важных данных и конфиденциальной информации. Даже заблокированный экран

становится недостаточной защитой против современных методов разблокировки.

Атаки на мобильные платформы в 2025 году

Android и iOS самые популярные мобильные платформы на сегодняшний день в мире и в России. Успешные атаки на устройства Android и iOS за 2025 год [4], демонстрируют рост количества угроз для мобильных устройств, в частности:

1. Рост числа троянов.

В 2025 году наблюдался резкий рост числа троянов, направленных на Android-платформу [4]. Особенно выделяется широко распространившийся «ClayRat» (КлейРат), активно действующий на территории России [5]. Он был найден более чем в 600 вариациях и использовался для распространения среди пользователей через обмен сообщениями в мессенджерах и фальшивые веб-сайты. Цель атаки заключалась в хищении личной информации и финансов.

2. Фальсификация банковских транзакций.

Тенденцией 2025 года стало широкое распространение атак на банковские операции через смартфоны. Мошенники использовали техники, называемые «NFC-обман» (обман ближней бесконтактной связи) [6]:

2.1 Прямая схема: потерпевшего вынуждали скачать вредоносное приложение, которое просит прикрепить банковскую карту к задней панели устройства и ввести персональный идентификационный номер (ПИН-код). Таким образом злоумышленники получали доступ к средствам пользователя.

2.2 Обратная схема: фальшивое приложение заменяло настоящие данные банковского счета на реквизиты преступников, создавая иллюзию совершения платежа самим владельцем устройства. Подобные атаки привели к значительному росту потерь денежных средств среди пользователей Android.

3. Предустановленные вредоносные программы.

Предустановленные вредоносные программы стали тревожным событием 2025. Выявлено предустановленное вредоносное ПО на продаваемых устройствах Android. Смартфоны неизвестных брендов, приобретаемые на онлайн-рынках, оказывались заранее зараженными троянами. Один из распространяемых вирусов — «Triada» (Триада), умеющий внедряться в каждое установленное приложение и воровать конфиденциальные данные, SMS, токены, контакты [6]. Подобные случаи продемонстрировали опасность приобретения дешёвых устройств сомнительного качества.

4. Взлом через уязвимости нулевого дня (далее 0-day).

Разработчик шпионского ПО использовал 0-day уязвимости для целевых атак на устройства iOS и Android [6]. В частности, эксплуатация уязвимостей «WebKit» (ВебКит) позволила осуществлять дистанционное выполнение кода на устройствах от Apple [6]. Выявленные уязвимости вскоре были исправлены производителем, демонстрируя оперативное реагирование на новые угрозы.

5. Недостаточная защита приложений.

Исследования показали, что значительная часть мобильных приложений на обеих платформах страдает от серьёзных недостатков безопасности. Согласно отчету компании Positive Technologies (ПАО «Группа Позитив») [7], большая часть уязвимостей связана с отсутствием шифрования пользовательских данных, слабым контролем целостности приложений и недостаточной защитой конфиденциальной информации в коде.

Типология атак на мобильные устройства

Атаки на мобильные устройства представляют серьёзную угрозу кибербезопасности для своих пользователей. Из числа наиболее распространённых таких атак, выделим следующие типы:

1. По типу воздействия на устройство:

1.1 Человек по середине (Man-in-the-Middle – MitM) – на перехват данных, проходящих между устройством и сервером [6]. Использование поддельных точек в беспроводной сети (Wireless Fidelity – Wi-Fi) или посредством атак на понижение протокола безопасного уровня сокетов (Secure Sockets Layer stripping – SSL stripping) [6].

1.2 Фишинг (phishing) и социальная инженерия (Social Engineering) – обман пользователя, с целью раскрытия его личных данных или установки вредоносного ПО [6]. Реализация осуществляется через фальшивые страницы входа, письма или SMS-сообщения.

1.3 Физический доступ – получение физического контроля над устройством. В результате большинство цифровых мер безопасности, отпечатки пальцев, скрытие резервных копий становятся бездейственными.

1.4 Установка вредоносного ПО – вредонос распространяется через неофициальные магазины, социальные сети, почтовые вложения или инфицированные рекламные баннеры [6].

1.5 Рутирование/Джейлбрейк (Rooting/Jailbreaking) – устранение ограничений безопасности операционной системы [6]. В результате злоумышленники получают полный доступ ко всем файлам и функциям устройства.

2. По уровню взаимодействия с целевой системой:

2.1 Внутренняя атака (insider attack) – атаки совершаются людьми внутри организации или теми, кому доверяют. Могут быть реализованы через инсайдеров, сотрудников или подрядчиков.

2.2 Внешняя атака (external attack) – происходит извне сети, обычно инициируется хакерами или организованными преступниками, использующими средства дистанционного проникновения.

3. По степени автоматизации:

3.1 Автоматизированные атаки – используют ботов и специализированные сценарии для быстрого обнаружения и эксплуатации слабых мест. Примером являются спам и массовое распространение вредоносного ПО.

3.2 Ручные атаки – требуют человеческого участия, используются высококвалифицированными специалистами, нацелены на конкретные цели и часто включают элементы социальной инженерии.

4. По источнику происхождения:

4.1 Государственно-спонсируемые атаки – инициативы государств или правительственных организаций, направленные на шпионаж, саботаж или влияние на политические процессы.

4.2 Хакерские группы и одиночки – самостоятельные или коллективные усилия, мотивированных финансовой выгодой, идеологией или удовольствием от самого процесса взлома.

5. По направлению атаки:

5.1 Атаки на сетевом уровне (network-based attacks) – направлены на инфраструктуру сетей и подключения (отказ в обслуживании (Distributed Denial of Service – DDoS), MitM, подмена протокола разрешения адресов (подмена Address Resolution Protocol – ARP spoofing)) [1].

5.2 Атаки на уровне приложений (application-level attacks) – нацелены в слабые места конкретных приложений (межсайтовый скриптинг (Cross-Site Scripting – XSS), внедрение кода в структурированный язык запросов (Structured Query Language injection – SQL-инъекции), межсайтовая подделка запроса (Cross-Site Request Forgery – CSRF)) [1].

5.3 Атаки на уровне устройства (device-specific attacks) – целью становится конкретное мобильное устройство (физическое манипулирование устройством (physical tampering), установка вредоносного ПО (malware installation)) [1].

Понимание возможных типов атак позволяет производителям устройств, разработчикам приложений проектировать, реализовывать максимально эффективные стратегии защиты и правильно оценивать возможные риски для пользователей мобильных устройств и приложений. Android и iOS — две лидирующие мобильные платформы, каждая из которых имеет свои сильные и слабые стороны в плане безопасности. Общие рекомендации касаются фундаментальных аспектов безопасности приложений независимо от платформы.

Основные инструменты и методы защиты мобильных приложений

1. Защита на уровне операционной системы. Современные мобильные операционные системы (iOS, Android) имеют встроенные механизмы защиты:

1.1 Политики управления доступом. Ограниченный доступ приложений к данным устройства и аппаратным компонентам (микрофону, камере, контактам и др.).

1.2 Обфускация кода [6]. Преобразование исходного кода приложения таким образом, чтобы сделать его труднопонимаемым для злоумышленника, занимающегося обратной разработкой (reverse engineering).

1.3 Проверка целостности приложения [6]. Проверка наличия изменений в структуре и поведении приложения, вызванные попытками вмешательства извне (получение привилегий администратора (root-доступ), эмуляторы, модификации файлов, пакет приложений Android и iOS (Android Package Kit и iOS App Store Package – APK/IPA)).

1.4 Использование специальных библиотек. Библиотеки, вроде «ProGuard» (ПроГард) для Android, позволяют оптимизировать и минимизировать размер приложения, одновременно обеспечивая дополнительную безопасность благодаря удалению неиспользуемых классов и методов [6].

2. Защита серверной части:

2.1 Аутентификация и авторизация сервера. Важна проверка подлинности запросов от клиента, применение токенов доступа и одноразовых сессионных ключей.

2.2 Фильтрация запросов. Запросы обрабатываются на стороне сервера с проверкой на наличие SQL-инъекций, XSS-уязвимостей и иных видов атак.

2.3 Регулярное обновление инфраструктуры. Своевременное устранение выявленных уязвимостей (патчи, обновления библиотеки безопасности).

3. Пользовательские меры предосторожности:

3.1 Регулярное обновление.

3.2 Использование надёжных паролей.

3.3 Двухфакторная аутентификация.

3.4 Отсутствие загрузок приложений из ненадежных источников.

3.5 Повышенная осмотрительность при работе с публичными сетями Wi-Fi.

3.6 Внимательность при предоставлении приложениям разрешений на доступ к личным данным.

Сравнительная характеристика iOS и Android

Специфика платформ Android и iOS накладывает свои нюансы, связанные с открытой архитектурой Android и закрытостью экосистемы iOS [8]. Благодаря закрытым принципам и единству аппаратного и ПО, iOS демонстрирует лучшую защиту от угроз по сравнению с Android. Вместе с

тем, безопасность достигается ценой ограничений и меньшей свободой для пользователей и разработчиков. Платформа iOS от Apple характеризуется высокой целостностью и развитой системой безопасности, что отличает её от Android.

Сравнительная характеристика iOS и Android:

1. Особенность экосистем:

1.1 iOS построена на принципе закрытости: вся экосистема регулируется и контролируется Apple [8]. Пользователи могут устанавливать приложения только из официального магазина App Store, прошедшего проверку безопасности.

1.2 Android, предоставляет больше свободы разработчикам и пользователям, позволяя устанавливать сторонние приложения вне Google Play, что повышает риск заражения вредоносным ПО.

2. Исходный код:

2.1 Исходный код операционной системы iOS доступен частично и избирательно. Ядро iOS основано на «Darwin» (Дарвин) [8], модифицированной версии БСД Юникс (Berkeley Software Distribution – BSD Unix). Только часть кода ядра «Darwin» доступна публично.

2.2 Ядро Android основано на Линукс (Linux), что делает его открытым для анализа и доработки [8]. С одной стороны, это позволяет находить и устранять уязвимости быстрее, с другой — увеличивает риск атаки со стороны опытных хакеров.

3. Возможности интеграции [8]:

3.1 Почти все устройства iOS создаются компанией Apple, что позволяет оптимизировать и унифицировать безопасность. Обновления системы или ПО с исправлениями ошибок выходят сразу для всех устройств, гарантируя единую безопасность.

3.2 Android представлен огромным количеством производителей. Разнообразие производителей значительно затрудняет быстрое развертывание апдейтов безопасности. Старые устройства часто вовсе не получают своевременных обновлений безопасности.

4. Отсутствие фрагментации [8]:

4.1 В iOS проблемы с фрагментацией отсутствуют. Новая версия iOS доступна практически для всех активных устройств одновременно. Пользователи практически всегда находятся на последней версии и регулярно получают актуальные обновления безопасности.

4.2 Android испытывает с фрагментацией большие проблемы, так как многие производители выпускают обновления нерегулярно. Кроме того, к серьёзной проблеме фрагментации, приводит огромное разнообразие Android – устройств и их производителей.

5. Защита критически важных данных:

5.1 Аппаратные компоненты (Hardware-элементы) iOS (защищённый анклав – secure enclave), обеспечивают защиту критически важных данных [8], пароли и биометрию с помощью специализированного процессора безопасности.

5.2 Подобная технология не предусмотрена в Android, хотя некоторые производители добавляют собственные аналоги.

6. Возможность использования кастомных прошивок [8]:

6.1 Apple официально не поддерживает использование кастомных прошивок, считает их нарушением лицензионного соглашения и возможным источником проблем с безопасностью.

6.2 Пользователи Android могут самостоятельно, легально устанавливать кастомные прошивки (например, «LineageOS» (ЛинейджОС)), давая свободу в изменении настроек безопасности и производительности.

7. Система песочниц (Sandboxing) [8]:

7.1 В iOS изоляция приложений друг от друга строгая и обеспечивается наличием отдельного пространства для каждого приложения. Доступ к ресурсам устройства ограничен на уровне приложений: каждое разрешение должно быть явно одобрено пользователем.

7.2 Android использует песочницу (sandbox) для изоляции приложений друг от друга, но это разделение менее строгое, чем в iOS. Одно приложение может влиять на поведение другого через объект для межкомпонентного взаимодействия «Intent» (Интент).

8. Шифрование по умолчанию [8]:

8.1 Практически все данные на iOS – устройстве шифруются по умолчанию. Это обеспечивает высочайший уровень защиты от физических атак и доступа третьих лиц к данным, если устройство потеряно или украдено.

8.2 В Android шифрование как мера защиты возможна, но далеко не обязательна.

9. Система обновлений [8]:

9.1 Каждый пользователь Apple получает свежие обновления безопасности одновременно с выходом новой версии iOS. Благодаря этому уязвимости закрываются быстро и повсеместно.

9.2 В Android обновление безопасности зависит от производителя устройства, что часто приводит к задержкам и невозможности установки свежих патчей.

Таким образом, отличительные особенности мобильных платформ влияют на защищенность мобильных устройств.

Меры мобильных операторов по защите от интернет-угроз

Одним из ключевых аспектов в процессе обеспечения защищённости мобильных устройств является функционал мобильных операторов, ориентированный на обеспечение безопасности своих клиентов.

В качестве основных направлений для обеспечения безопасности частных клиентов и их защиты от угроз в интернете, выделяются:

1. Доступ к надежным антивирусным программам, которые защищают устройства от вредоносного ПО, фишинга и прочих угроз.

2. Сервис системы фильтрации доменных имен (service of domain name system – DNS-фильтрации), блокирующий опасные сайты и запрещающий доступ к контенту, содержащему вирусы или мошенничество.

3. Виртуальные частные сети (Virtual Private Network – VPN), позволяющие шифровать весь интернет-трафик.

4. Специализированные сервисы – «антифрод-решения», предупреждающие клиентов о возможностях мошеннических схем, таких как финансовые пирамиды, смс-разводы и фишинг.

5. Автоматическая защита модуля идентификации абонента (Subscriber Identification Module – SIM-карта). Благодаря технологиям аналитики SIM-карты клиентов защищены от попыток смены номеров и SIM-клонирования;

6. Контроль семейного бюджета – можно ограничить расход на звонки, SMS и покупку контента.

7. Родительский контроль – для родителей, желающих контролировать деятельность детей в интернете.

8. Отслеживание геолокации – позволяют родителям следить за перемещением ребенка и получать уведомления о нарушении границ заданных зон.

Для корпоративных клиентов более продвинутые решения:

1. Система обнаружения вторжений и система предотвращения вторжений (Intrusion Detection System / Intrusion Prevention System – IDS/IPS) – Система для раннего обнаружения и предотвращения вторжений.

2. SSL и защита шифрованием протокола транспортного уровня (encryption with Transport Layer Security – TLS-шифрование) – позволяет

компаниям обеспечивать безопасный канал передачи данных между офисами и филиалами

3. Центры мониторинга и реагирования на инциденты (Security Operations Center – SOC) – центры обеспечивают круглосуточный мониторинг состояния ИТ-инфраструктуры и немедленную реакцию на любые нарушения безопасности.

Необходимо отметить, что российские мобильные операторы функционируют в сложной и регулируемой среде, выполняют требования международных и российских стандартов, а также соответствуют требованиям российского законодательства в сфере обеспечения безопасности мобильных сетей. Кроме разработчиков мобильных платформ и операторов мобильной связи защиту мобильных устройств обеспечивают также разработчики мобильных приложений.

Классификация атак на банковские приложения

Из всего разнообразия мобильных приложений наиболее защищенными считаются банковские приложения, выступающие в роли прямого посредника между банком и клиентом. Они содержат критически важную информацию и имеют непосредственный доступ к счетам своих клиентов.

Мобильные приложения банков сталкиваются с множеством различных угроз, что и порождает потребность в применении серьёзных многослойных систем защиты.

Стандарты и нормативные акты устанавливают единые правила и рекомендации, помогающие банкам и финансовым учреждениям гарантировать защиту данных и минимизировать риски при создании и эксплуатации мобильных банковских приложений.

Центральный Банк Российской Федерации (ЦБ РФ) предъявляет строгие требования к безопасности мобильных банковских приложений,

направленные на защиту пользователей и сохранность их данных. Эти требования определены в нормативных актах и рекомендациях, таких как положения ЦБ РФ и информационно-технических требованиях безопасности банковских систем.

Несмотря на серьёзные, многоуровневые системы защиты банковских приложений, максимально возможное неразглашение информации о выявлении уязвимостей таких систем и о реализации возникающих угроз в их отношении, анализ мировой практики даёт возможность привести примеры реальных атак за последние несколько лет и классифицировать их.

Классификация атак на мобильные банковские системы:

1. Атаки на мобильные устройства:

1.1 Joint-Banking (Джойнт-Банкинг) (2021 г., Россия) [9,10]: Банковский троян маскировался под популярное приложение банка и воровал коды подтверждения для переводов.

1.2 «Flubot» (Флубот) (2022 г., Европа) [11]: Зловредная программа распространялась через SMS и позволяла удаленно управлять устройством, включая возможность скрытия приложений и перезагрузки устройства.

2. Веб-фишинг и социальная инженерия:

2.1 Смишинг (SMS-фишинг – SMShing) (2023 г., Австралия) [11]: Широкомасштабная компания, в ходе которой пользователям приходили сообщения с предложением подтвердить аккаунт в банке через ссылку, ведущую на фальшивый ресурс.

2.2 Клонирование приложений (2024 г., Китай) [7]: Мошенники создавали точные копии интерфейсов банковских приложений, чтобы собрать данные клиентов.

3. Уязвимости мобильных приложений:

3.1 Небезопасные прямые ссылки на объекты (Insecure Direct Object References – IDOR) (2022 г., Турция) [7]: Разработчик оставил уязвимость в

приложении, позволявшую изменять баланс чужого счёта, просто подставив чужой идентификатор (identifier – ID) в запрос.

3.2 MitM (2023 г., Бразилия) [8]: Незащищённое соединение позволило злоумышленникам перехватывать данные пользователей через публичные Wi-Fi сети.

4. Атаки на серверную часть:

4.1 SQL-инъекции (2024 г., Германия) [8]: Некорректная обработка данных на сервере привела к массовым утечкам персональных данных клиентов банка.

4.2 DDoS (2025 г., Япония) [8]: Массированные атаки парализовали работу мобильных приложений крупного японского банка, нарушив обслуживание клиентов.

Типы угроз для мобильных банков варьируются от классических атак на устройства до уязвимостей серверного оборудования [11].

Основные категории угроз и их характеристики:

1. Угрозы на стороне устройства:

1.1. Уязвимости в приложениях:

1.1.1 Отсутствие или недостаточное шифрование трафика между клиентом и сервером [11].

1.1.2 Логические ошибки в коде, ведущие к раскрытию важных данных (например, SQL-инъекции) [11].

2. Угрозы на стороне пользователя:

2.1. Фишинг и социальная инженерия:

2.1.1 Создание фальшивых страниц входа, выглядящих как интерфейс банка, чтобы заполучить личные данные [11].

2.1.2 Телефонные звонки или сообщения, цель которых — вытянуть финансовую информацию у пользователя [2,11].

2.2. Невнимательность и халатность:

2.2.1 Пользователи могут передавать свои пароли друзьям или родственникам, хранить пароли на бумаге или в легко доступной форме [11].

2.2.2 Использование общедоступных точек доступа Wi-Fi без надлежащей защиты (защищённый доступ Wi -Fi / защищённый доступ Wi-Fi 2 / защищённый доступ Wi-Fi 3 (Wi-Fi Protected Access / Wi-Fi Protected Access 2 / Wi-Fi Protected Access 3 – WPA/WPA2/WPA3)) приводит к MitM-атакам [5,11].

3.Угрозы на стороне инфраструктуры банка:

3.1. Атакующие серверы банка:

3.1.1 DDoS-атаки: Парализация работоспособности банка путём перегрузки серверов большим количеством запросов [6].

3.1.2 SQL-инъекции: Нападения, нацеленные на базы данных банка для похищения информации [1,11].

3.2. Нарушение стандартов безопасности:

3.2.1 Несоблюдение норм стандарта безопасности данных индустрии платёжных карт (Payment Card Industry Data Security Standard – PCI DSS), что ведет к утечке данных карточек.

3.2.2 Взлом в контексте фингерпринтинга (fingerprinting hacking) – проблемы с аутентификацией и управлением доступом через подбор отпечатков пальцев [6].

3.2.3 Несанкционированный доступ через рутирование или джейлбрейк (Unauthorized Access via Rooting or Jailbreaking) – владельцы устройств, прошедшие процедуру jailbreak (iOS) или root (Android), теряют большую часть встроенных уровней защиты, что облегчает атаки [6].

4. Угроза, связанная с физическим доступом – кража устройства (physical theft) с последующим доступом к финансовым данным.

Поддержание высокого уровня безопасности мобильных банков требует комплексного подхода, учитывающего технологические достижения и эволюцию методов атак.

Также, нельзя не упомянуть актуальные методы социальной инженерии, применяемые против пользователей мобильных банков:

1. SMShing [6]: Злоумышленники отправляют SMS, притворяясь официальным представителем банка. Сообщения могут выглядеть убедительно и предлагать подтвердить данные, изменить пароль или восстановить доступ к счету.

2. Голосовой фишинг (Voice phishing – Vishing) [6]: Звонки, выдаваемые за звонок от банка, сотрудники которого просят пользователя назвать данные карты, значение проверки подлинности карты (Card Verification Value – CVV-код) или пароль для верификации. Иногда мошенники создают голосовую почту, звучащую крайне реалистично.

3. Фишинговая атака на руководящий состав (Whaling) [6]: Целевые атаки на высокопоставленных сотрудников банка или крупных вкладчиков, которые ведутся персонализировано и долго готовятся.

Бороться с ними можно путём сочетания технических средств защиты (фильтрация почты, шифрование, антиспам и антивирусные решения) и образовательных мероприятий, повышающих осведомленность пользователей о признаках мошенничества.

Заключение

Обеспечение защищённости мобильных устройств является необходимым элементом цифровой гигиены каждого пользователя и важнейшим направлением для развития и совершенствования мобильных платформ, приложений и экосистем мобильной связи.

В рамках данной работы поведён анализ различных уровней обеспечивающих защищённость мобильных устройств. Рассмотрены

примеры успешных атак за последние годы. Приведена классификация основных угроз для мобильных банковских экосистем. Рассмотрены средства и методы защиты для каждого выделенного уровня. Средства и методы защиты мобильных устройств непрерывно развиваются и совершенствуются. Производители устройств, разработчики мобильных платформ, приложений, мобильных банков, операторы связи и, конечно, сами пользователи мобильных устройств, каждый на своём уровне обеспечивают безопасность мобильного устройства.

Литература

1. Erukude, S.T., Marella, V.C. Veluru, S.R. AI-Driven Cybersecurity Threats: A Survey of Emerging Risks and Defensive Strategies // International Conference on Data Science and Applications. 2026. Vol 1723. pp. 185 – 197. DOI: 10.1007/978-3-032-10783-1_14.

2. Fu J., Wang Y., Yi Y., Wang X. Research on Mobile Computing and Network Security // ICAISM '25: Proceedings of the 2025 International Conference on Artificial Intelligence and Smart Manufacturing. 2025. pp. 872 – 876 DOI: 10.1145/3756423.3756567.

3. Трещев И. А., Монастырная Е. И. Событийная формальная модель поведения злоумышленника // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2024. № 1(73). С. 42-46. EDN IZQRGT.

4. Calif S. 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics // Security & Identity. 2024. URL: cybersecurityventures.com/cybersecurity-almanac-2024/.

5. Pratapagiri V. ClayRat: A New Android Spyware Targeting Russia // Zimperium Blog. 2025. URL: zimperium.com/blog/clayrat-a-new-android-spyware-targeting-russia.

6. Зобнин Е.Е. Android глазами хакера // Санкт-Петербург. БХВ-Петербург. 2024. 272 с. ISBN 978-5-9775-1797-3.

7. Вяткина А.А., Осипова А.А. Cybersecurity threatscape: H1 2025 // Positive Technologies. 2025. URL: global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-h1-2025/.

8. Исаева К.В., Мардамшина А.А. Сравнительный анализ мобильных платформ Android и iOS // Лучшая научно-исследовательская работа 2022. 2022. С. 45 – 47. EDN INVFJA.

9. Лазарева Н.Б., Ефимов Д.С. Анализ сетевой устойчивости и оптимизация обмена данными в банковских системах // Инженерный вестник Дона. 2025. №2. URL: ivdon.ru/ru/magazine/archive/n2y2025/9838.

10. Кивва А.А. Мобильная вирусология 2024 // Securelist by Kaspersky. 2024. URL: securelist.ru/mobile-threat-report-2024/111730/.

11. Котиков Н.М., Горин Д.С., Шатовкин Р.Р. Исследование уязвимостей абонента телефонной связи с точки зрения деструктивной социальной инженерии // Инженерный вестник Дона. 2025. №12. URL: ivdon.ru/ru/magazine/archive/n12y2025/10595.

References

1. Erukude, S.T., Marella, V.C. Veluru, S.R. International Conference on Data Science and Applications. 2026. Vol 1723. pp. 185 – 197. DOI: 10.1007/978-3-032-10783-1_14.

2. Fu J., Wang Y., Yi Y., Wang X. ICAISM '25: Proceedings of the 2025 International Conference on Artificial Intelligence and Smart Manufacturing. 2025. pp. 872 – 876. DOI: 10.1145/3756423.3756567.

3. Treshhev I. A., Monasty`rnaya E. I Ucheny`e zapiski Komsomol`skogo-na-Amure gosudarstvennogo texnicheskogo universiteta. 2024. № 1(73). pp. 42-46. EDN IZQRGT.

4. Calif S. Security & Identity. 2024. URL: cybersecurityventures.com/cybersecurity-almanac-2024/.

5. Pratapagiri V. Zimperium Blog. 2025. URL: zimperium.com/blog/clayrat-a-new-android-spyware-targeting-russia.

6. Zobnin E.E. Android glazami xakera [Android through the eyes of a hacker]. Sankt-Peterburg. BXV-Peterburg. 2024. 272 p.

7. Vyatkina A.A., Osipova A.A. Cybersecurity threatscape: H1 2025. Positive Technologies. 2025. URL: global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-h1-2025/.

8. Isaeva K.V., Mardamshina A.A. Luchshaya nauchno-issledovatel`skaya rabota 2022. 2022. pp. 45 – 47. EDN INVFJA.

9. Lazareva N.B., Efimov D.S. Inzhenernyj vestnik Dona. 2025. №2. URL: ivdon.ru/ru/magazine/archive/n2y2025/9838.

10. Kivva A.A. Mobil`naya virusologiya 2024 [Mobile Virology 2024]. Securelist by Kaspersky. 2024. URL: securelist.ru/mobile-threat-report-2024/111730/.

11. Kotikov N.M., Gorin D.S., Shatovkin R.R. Inzhenernyj vestnik Dona. 2025. №12. URL: ivdon.ru/ru/magazine/archive/n12y2025/10595.

Дата поступления: 12.01.2026

Дата публикации: 3.03.2026