



PT

# Уязвимости и угрозы

**мобильных банков**

ptsecurity.com

# Содержание

Об исследовании	3
Резюме	4
Уязвимости клиентских частей приложений	5
Уязвимости серверных частей приложений	11
Что нужно знать пользователю	14
Заключение	15

## 7 банков клиентов Android клиентов iOS серверных частей

### Об исследовании

В 2019 году для исследования мы выбрали 14 полнофункциональных банковских мобильных приложений по следующим критериям:

- проведен анализ мобильных приложений для обеих ОС — Android и iOS;
- приложение установлено более 500 000 раз из официальных магазинов приложений Google Play и App Store;
- владельцы систем не возражают против использования результатов анализа за защищенности в исследовательских целях.

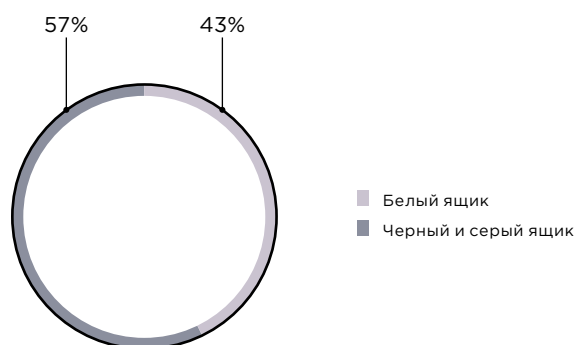


Рисунок 1. Методы анализа защищенности (доля приложений)

Оценка защищенности проводилась вручную методами черного, серого и белого ящика с использованием вспомогательных автоматизированных средств. Метод черного ящика заключается в проведении работ со стороны внешнего атакующего без предварительного получения дополнительных данных об информационной системе от ее владельца. Метод серого ящика аналогичен, но в роли нарушителя выступает пользователь, имеющий определенные привилегии в системе. При анализе методом белого ящика для оценки защищенности используются все имеющиеся данные о приложении, включая исходный код.

В данном исследовании приведены уязвимости клиентской и серверной частей мобильных банковских приложений, связанные с ошибками в коде, недостатками клиент-серверного взаимодействия, а также ошибками реализации механизмов защиты. Другие распространенные проблемы информационной безопасности (к примеру, недостатки управления обновлениями ПО) не рассматриваются. Уровень риска уязвимостей оценивался исходя из степени влияния потенциальной атаки на пользовательские данные и само приложение, а также с учетом сложности проведения атаки; выделены качественные оценки высокого, среднего и низкого уровней риска.

## Резюме

Ни одно из исследованных мобильных банковских приложений не обладает приемлемым уровнем защищенности.

### Клиентская часть

Клиентская часть мобильного банка — это мобильное приложение, которое устанавливается непосредственно на устройство пользователя.

- В 13 из 14 клиентских частей возможен доступ к данным пользователей.
- 76% уязвимостей в мобильных банках могут быть проэксплуатированы без физического доступа к устройству.
- Более трети уязвимостей не требуют административных прав для эксплуатации (jailbreak или root).

### Серверная часть

Серверная часть мобильного банка — это веб-приложение, которое находится на стороне банка и взаимодействует с мобильным клиентом через интернет посредством специального интерфейса (API).

- 54% всех уязвимостей содержатся в серверной части приложений.
- В серверной части каждого мобильного банка содержится в среднем 23 уязвимости.
- В каждом втором мобильном банке возможны проведение мошеннических операций и кража денежных средств.
- В пяти из семи приложений под угрозой логины и пароли от личных кабинетов пользователей, а в каждом третьем приложении могут быть украдены данные банковских карт.

## Уязвимости клиентских частей приложений



Ни одна из исследованных клиентских частей мобильных банковских приложений не обладает приемлемым уровнем защищенности.

Клиентские части мобильных банковских приложений, разработанные для iOS, содержали меньше уязвимостей, чем приложения для Android. Все недостатки в мобильных банках для iOS были не выше среднего уровня риска. В то время как 29% приложений для Android содержали уязвимости высокого уровня риска.



Рисунок 2. Уровень защищенности клиентских частей (число приложений)

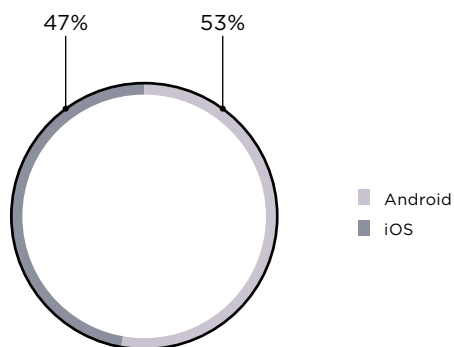


Рисунок 3. Доля всех уязвимостей в клиентских частях для разных мобильных ОС

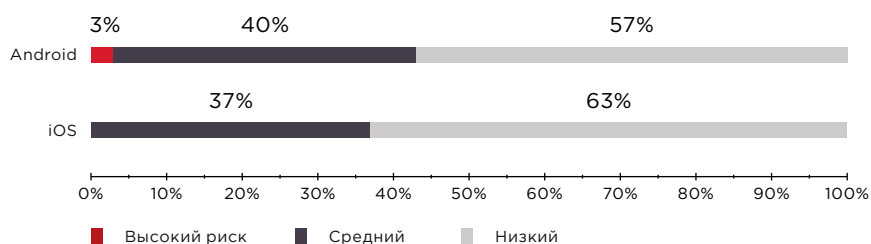


Рисунок 4. Доля уязвимостей различного уровня риска

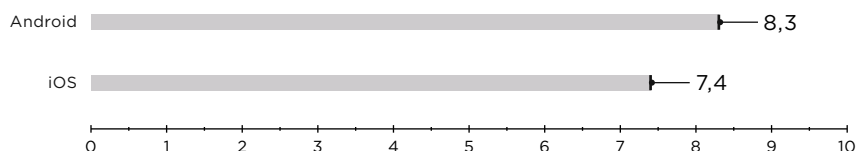


Рисунок 5. Среднее количество уязвимостей на одно приложение

## Больше возможностей — больше уязвимостей

Наиболее опасные уязвимости выявлены в Android-приложениях и связаны с небезопасной обработкой ссылок deeplink. Технология deep linking используется по-разному в версиях для iOS и для Android. Разработчикам Android-приложений предоставляется больше свободы в реализации различной функциональности. Это причина большего количества уязвимостей в сравнении с iOS-приложениями. Но это не значит, что разработчики iOS-приложений не могут допустить ошибки. Безопасность мобильного банка в первую очередь зависит от практики безопасной разработки (Security Development Lifecycle, SDL).

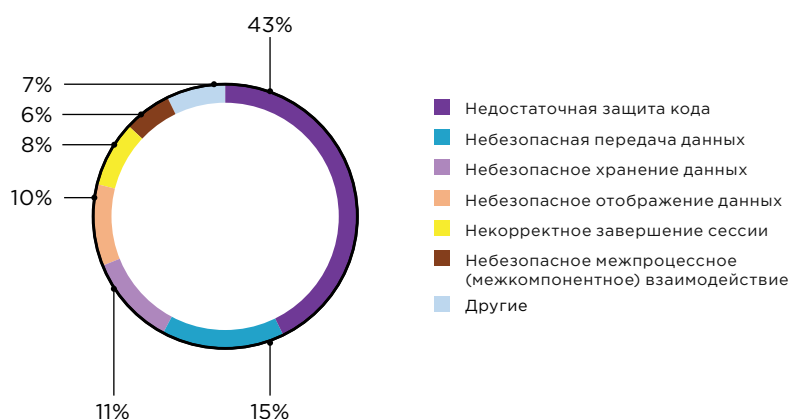


Рисунок 6. Доля уязвимостей разных типов

## В 100%

клиентских частей мобильных банков недостаточно защищен код:

- отсутствует обфускация кода;
- отсутствует защита от внедрения кода и «перепакетки»;
- в коде содержатся имена классов и методов.

Исследование показало, что банки не защищаются от угрозы анализа исходного кода, которая возникает в случае недостаточной его защиты. Для эксплуатации уязвимостей в коде злоумышленникам нужно получить к нему доступ, а для этого достаточно скачать приложение из Google Play или App Store и затем его декомпилировать.

Отсутствие обфускации кода позволяет его анализировать и находить такие важные данные, как:

- тестовые логины и пароли;
- ключи шифрования или параметры, из которых они однозначно получаются;
- соль, используемую для хеширования или шифрования.

Эта информация может быть в дальнейшем использована злоумышленниками для получения аутентификационных данных и доступа к веб-серверам. Кроме того, хакеры могут проанализировать алгоритм работы приложения и затем воспользоваться недостатками в бизнес-логике. Также информация о том, как устроено приложение, может быть интересна конкурентам для внесения в свои продукты новой функциональности.

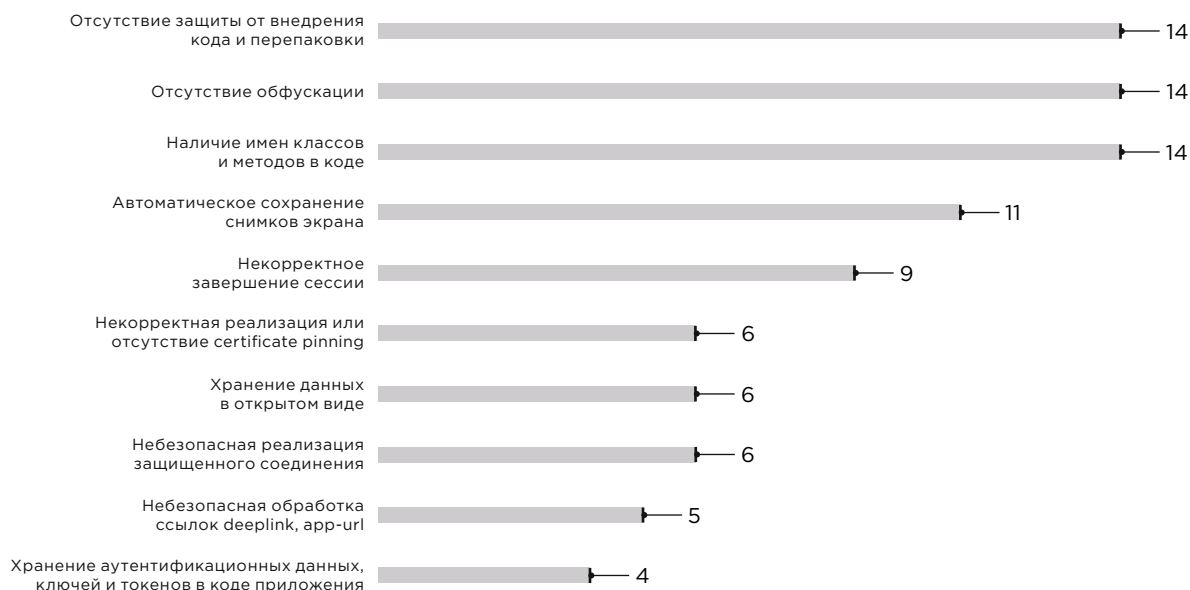


Рисунок 7. Топ-10 уязвимостей мобильных банков (количество уязвимых приложений)

## Рекомендация для разработчиков

Используйте методы запутывания кода, усложняющие злоумышленникам его чтение и анализ. Примером запутывания может служить процедура удаления символов, проводимая на этапе сборки приложения. Она заключается в замене исходных имен классов и методов случайными или однобуквенными именами. Можно использовать специализированные программные средства, например ProGuard для Android или Sirius Obfuscator и SwiftShield для iOS.

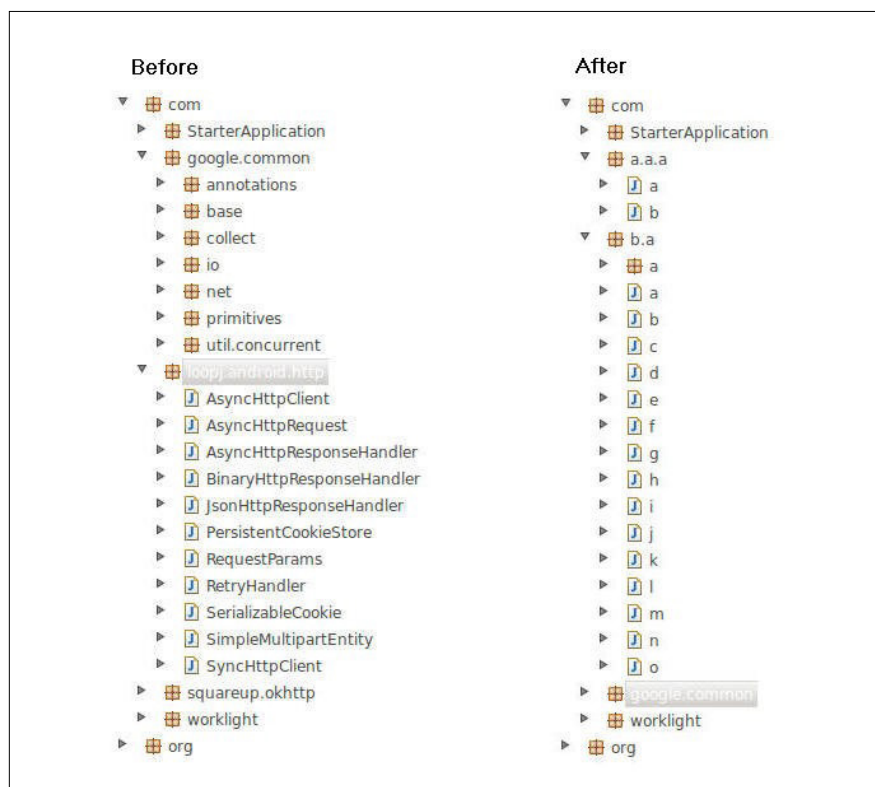


Рисунок 8. Примеры декомпилированных исполняемых файлов с сохраненными символами и без



Рисунок 9. Условия эксплуатации уязвимостей

# 67%

атак на частных лиц в IV квартале 2019 года были реализованы с использованием методов социальной инженерии

Для эксплуатации ряда уязвимостей в клиентских частях мобильных банков злоумышленнику достаточно установить на устройство жертвы вредоносное приложение, например в ходе фишинговой атаки.

Небезопасная обработка ссылок deeplink — одна из уязвимостей высокой степени риска, эксплуатация которой может привести к финансовым потерям банка. Например, в одном из исследованных банковских приложений отсутствовала фильтрация URL, получаемого с помощью механизма deep linking. Используя возможность загружать во встроенных компонентах WebView произвольные ссылки, атакующий мог загрузить ссылку на веб-страницу с вредоносным кодом и взаимодействовать с JavaScript-интерфейсами, доступными в этих компонентах WebView. Специалисты Positive Technologies разработали тестовые сценарии и продемонстрировали перехват SMS, а также получение номера банковской карты через манипуляции с функциональностью сканирования банковской карты камерой или через NFC. Злоумышленник может отобразить мошенническую страницу в интерфейсе мобильного приложения и попросить пользователя отсканировать банковскую карту. Для пользователя это будет выглядеть как работа с его обычным мобильным банком, но на самом деле данные получит злоумышленник, а не банк.

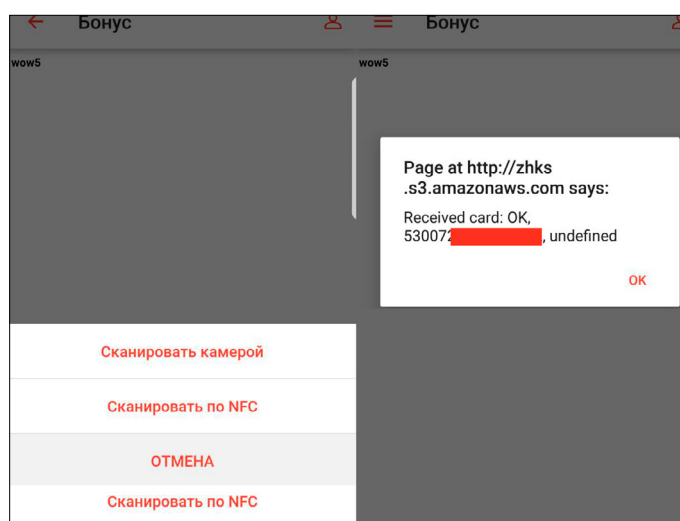


Рисунок 10. Манипуляции с функциональностью сканирования банковской карты





**Deep linking** — технология, благодаря которой пользователь может перемещаться между приложениями или разделами одного приложения в заранее определенные разделы с помощью специальных ссылок, подобно тому, как это сделано в веб-приложениях.

### Рекомендация для разработчиков

При реализации deep linking появляется еще одна точка входа в приложение, которой может воспользоваться злоумышленник. Необходимо учитывать, что все параметры, передаваемые с помощью механизма deep linking, поступают из ненадежного источника и должны проходить проверку и фильтрацию перед передачей в соответствующие методы исходного кода.



**11 из 14 мобильных банков позволяют автоматически сохранять снимки экрана** для быстрого просмотра недавно использованных программ.

На скриншоте экрана может содержаться конфиденциальная информация, например данные платежной карты и состояние банковского счета.

В файловой системе клиентской части практически каждого второго приложения хранится конфиденциальная информация в незашифрованном виде. Для доступа к этим данным злоумышленнику необходимы права root или jailbreak. Доступ к устройству может быть как физический, так и с использованием вредоносного приложения, которое эти права может получить. Так, при исследовании одного из мобильных банков специалисты Positive Technologies обнаружили выписки по банковской карте, которые сохранялись в телефоне. А в другом случае приложение и вовсе сохраняло пинкод пользователя и злоумышленник мог получить доступ к личному кабинету мобильного банка.



Рисунок 11. Разглашенная информация (число приложений)

## Рекомендация для разработчиков

На мобильном устройстве нужно хранить только необходимый объем данных. Требуемые данные должны запрашиваться с сервера только во время работы с приложением и после завершения работы должны быть удалены. Шифруйте конфиденциальную информацию, хранящуюся на устройстве, но при этом обеспечьте безопасное управление ключами шифрования. Для защиты данных на снимках состояния экрана используйте специальное фоновое изображение, которое будет перекрывать экран мобильного банка, содержащий важную информацию.

# 43%

**приложений** хранят  
важные данные  
на мобильном  
устройстве  
в открытом виде

Только один мобильный банк из исследованных не содержал уязвимостей, позволяющих злоумышленнику получить доступ к данным пользователя. В 13 из 14 приложений возможно проведение атаки типа «человек посередине» из-за отсутствия механизма certificate pinning для осуществления проверки SSL-сертификатов, небезопасной реализации защищенного соединения, а также использования небезопасных внешних ссылок на объекты. В случае реализации данной атаки злоумышленник может получить доступ к важной информации пользователя, читать и изменять передаваемые данные между сервером и клиентским приложением.



## Уязвимости серверных частей приложений

Более половины серверных частей мобильных банков содержат уязвимости высокого уровня риска. Уровень защищенности серверных частей не превышает средний, для трех приложений он был оценен как низкий, а у одного — крайне низкий.

**23** уязвимости

в среднем содержатся  
в серверной части каж-  
дого мобильного банка

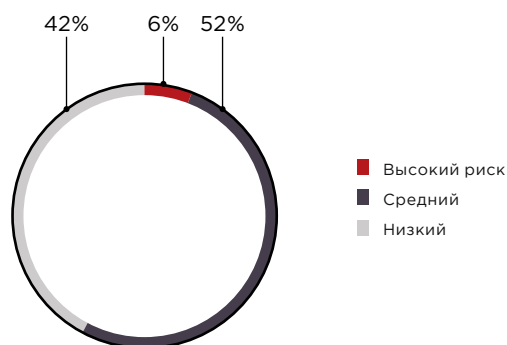


Рисунок 12. Доля уязвимостей различного уровня риска

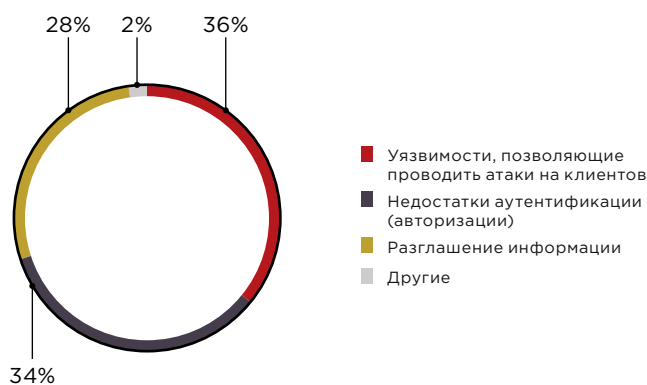


Рисунок 13. Доля уязвимостей разных типов

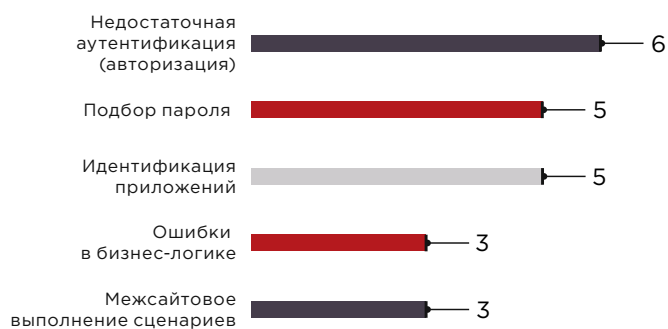


Рисунок 14. Топ-5 уязвимостей (число серверных частей)

Большинство уязвимостей, позволяющих проводить подбор пароля, связаны с недостатками реализации механизма предоставления одноразовых паролей (one-time password, OTP). Наиболее распространенная проблема — когда при превышении количества попыток ввода одноразовый пароль продолжает оставаться действительным. Получив доступ к личному кабинету пользователя и используя недостатки реализации механизма предоставления OTP, злоумышленник может совершать различные операции (в том числе финансовые) от имени этого пользователя.

Три из семи серверных частей мобильных банков содержат ошибки бизнес-логики. Как правило, они связаны с функциональностью, которой могут воспользоваться злоумышленники для совершения мошеннических операций. Ошибки в бизнес-логике могут принести банку существенные финансовые убытки и даже повлечь судебные разбирательства.

## Рекомендация для разработчиков

Интегрируйте в жизненный цикл разработки принципы SDL, в которые входит анализ защищенности кода еще в процессе его написания.



Рисунок 15. Угрозы мобильных банков (число серверных частей)

**Данные банковских карт под угрозой в трети мобильных банков**

Уязвимости серверных частей мобильных банков могут быть использованы для атак на пользователей в пяти из семи случаев. Например, из-за недостаточной проверки расширений загружаемых файлов в одном из исследованных мобильных банков злоумышленник мог загрузить на сервер исполняемые вредоносные файлы. Их запуск мог инициировать сотрудник банка, и это бы привело к исполнению злонамеренного сценария, например к получению данных с сервера.

Несанкционированный доступ к приложению, как правило, следствие недостатков аутентификации или авторизации. К примеру, нарушитель может подобрать пароль пользователя при аутентификации и получить доступ к личному кабинету атакуемого. Затем, если ему удастся обойти защиту с помощью одноразового пароля, используя недостатки в отправке OTP, хакер сможет выполнять различные действия в мобильном банке от имени этого пользователя.

Именно аутентификационные данные оказались наиболее уязвимы: логины и пароли от личных кабинетов пользователей мобильных банков под угрозой в пяти серверных частях мобильных банков. Персональные данные могут попасть в руки злоумышленников более чем в половине приложений. Среди информации, доступной нарушителю, имена и фамилии пользователей, баланс денежных средств, квитанции по переводам, лимиты банковских карт, а также возможность установить связь между платежной картой и номером мобильного телефона.



Рисунок 16. Разглашенная информация (число серверных частей)



**Информация, полученная в результате эксплуатации уязвимостей в мобильном банке, может быть использована для совершения мошеннических операций, а также при планировании других атак на банк и его клиентов.**

## Что нужно знать пользователю

Все мобильные банковские приложения имеют свои недостатки. Согласно нашему исследованию, приложения для Android более уязвимы, чем для iOS. Стоит отметить, что недостатки, которые позволяют напрямую проводить мошеннические операции и похищать деньги, связаны с ошибками в исходном коде приложений, и защита от них лежит на плечах разработчиков. Но также есть значительная доля уязвимостей, эксплуатация которых невозможна без участия пользователей. Например, для некоторых атак хакеру потребуется физический доступ к устройству.

Если пользователь намеренно повышает свои привилегии в ОС (jailbreak в iOS или root для Android) или не устанавливает пинкод для разблокировки устройства, то у нарушителя появляется больше возможностей для злонамеренных действий.

### Рекомендация для пользователей

Не повышайте привилегии до административных (jailbreak или root). Это открывает доступ к файловой системе и отключает механизмы защиты ваших данных. Обязательно установите пинкод для разблокировки устройства, чтобы ограничить возможности злоумышленника при физическом доступе.

Для реализации некоторых сценариев атак хакеру могут потребоваться действия со стороны пользователя: переход по ссылке, установка вредоносного приложения, ввод данных на поддельном сайте.

### Рекомендация для пользователей

Не переходите по ссылкам от незнакомых людей в SMS и мессенджерах. Никогда не подтверждайте запросы на установку сторонних программ на ваш смартфон. Загрузку приложений осуществляйте только из официальных магазинов приложений Google Play и App Store. Обращайте внимание на информацию о разработчике приложения и количество скачиваний.

Некоторые уязвимости могут быть связаны с недостатками мобильной ОС. Однако компании Google и Apple активно вносят изменения в свои продукты и публикуют обновления. Примечательно, что информация об уязвимостях становится публичной после того, как вендор выпускает патч. Этой информацией могут воспользоваться злоумышленники для атак на пользователей, которые не успели установить обновление.

### Рекомендация для пользователей

Своевременно устанавливайте обновления ОС и мобильных приложений.

## Заключение

Ни одно из исследованных мобильных банковских приложений не обладает приемлемым уровнем защищенности. Банки не защищаются от угроз анализа мобильных приложений, не уделяют достаточно внимания защите исходного кода, хранят важные данные на мобильных устройствах в открытом виде, допускают ошибки, позволяющие обходить механизмы аутентификации и авторизации, подбирать учетные данные к приложению.

Исследование показывает, что мобильные банки содержат недостатки, которые могут привести к таким последствиям:

- утечка важных данных пользователей, включая персональные и данные банковских карт;
- несанкционированный доступ к приложению;
- проведение мошеннических операций и кража денежных средств.

Стоит также отметить, что безопасность данных и сохранность денежных средств в руках не только разработчиков мобильных банков, но и самих пользователей. Большинство сценариев атак не реализуемы без их участия. Для эксплуатации 87% уязвимостей злоумышленнику требуются какие-либо действия со стороны пользователя. Повышая привилегии в ОС до административных, устанавливая приложения не из официальных магазинов приложений, посещая подозрительные сайты и переходя по ссылкам из мессенджеров или SMS, пользователи помогают хакерам и ставят под угрозу свои данные.

Как и прежде, мы рекомендуем банкам уделять больше внимания вопросам безопасности как на этапе проектирования мобильных приложений, так и на стадии разработки. Ввиду большого количества недостатков в исходном коде стоит пересмотреть подходы к разработке на всех этапах жизненного цикла приложения: возможно, имеются недочеты или не применяются практики безопасного программирования SDL. А поскольку ряд уязвимостей, особенно связанных с логикой приложения, невозможно предусмотреть, мы также рекомендуем тщательно тестировать приложения, их механизмы защиты и не забывать про анализ исходного кода.

---

### О компании

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/PositiveTechnologies  
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.