|  |
| --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  РОССИЙСКОЙ ФЕДЕРАЦИИ  Федеральное государственное бюджетное образовательное учреждение высшего образования  «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» |
| Исследовательская работа по проекту № 42  Мобильное приложение Ак Барс  На тему:  «Угрозы и уязвимости серверной части мобильного банковского приложения» |
|  |
| Выполнили:  Студенты 3 курса  Группы 181-352  Захаров В.А.  Констанитов Д.А. |

Москва – 2020

# CОДЕРЖАНИЕ

[1. Введение 2](#_Toc60598712)

[1.1 Серверная часть 2](#_Toc60598713)

[2. Уязвимости серверных частей приложений 3](#_Toc60598714)

[3. Модель нарушителя 4](#_Toc60598715)

[4. Модель угроз 9](#_Toc60598716)

# Введение

В данном исследовании приведены уязвимости серверной части мобильного банковского приложения, 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 сами сервера, а также с учетом сложности проведения атаки; выделены качественные оценки высокого, среднего и низкого уровней риска.

## 1.1 Серверная часть

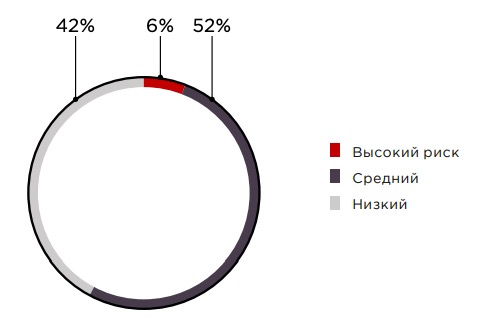
Серверная часть мобильного банка — это веб-приложение, которое находится на стороне банка и взаимодействует с мобильным клиентом через интернет посредством специального интерфейса (API).

Согласно исследованиям Positive Technologies:

* 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 серверных частей приложений

Согласно исследованиям Positive Technologies в более половина серверных частей мобильных банков содержат уязвимости высокого уровня риска. А среднее число уязвимостей, которые содержатся в серверной части каждого мобильного банка равно 23.

*Рисунок 1. Доля уязвимостей различного уровня риска*



*Рисунок 2. Доля уязвимостей разных типов*

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.

40% серверных частей мобильных банков содержат ошибки бизнеслогики. 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.

Уязвимости серверных частей мобильных банков могут быть использованы для атак на пользователей в 70% 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. 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.

# Модель нарушителя

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

По признаку принадлежности к ИС серверной части все нарушители делятся на две группы:

**Внешние нарушители** – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

**Внутренние нарушители** – физические лица, имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

**Внешний нарушитель**

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИС, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

**Внутренний нарушитель**

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИС обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам в соответствии с принятой политикой информационной безопасности.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой ИС предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

К внутренним нарушителям могут относиться:

* администратор безопасности (категория I);
* администраторы конкретных подсистем или баз данных (категория II);
* пользователи (категория III);
* лица, обладающие возможностью доступа к системе передачи данных (категория V);
* сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИС, но не имеющие права доступа к ним (категория VI);
* обслуживающий персонал (водитель, уборщик помещений и т.п.) (категория VII);
* уполномоченный персонал разработчиков, которые на договорной основе имеют право на техническое обслуживание и модификацию компонентов (категория VIII).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

На лиц категорий I-II возложены задачи по администрированию программно-аппаратных средств и баз данных для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИС мобильного приложения. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИС а также к техническим и программным средствам, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИС в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

К лицам категорий I-II ввиду их исключительной роли ИС должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I-II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз.

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

* Общая информация – информации о назначении и общих характеристиках ИС
* Эксплуатационная информация – информация, полученная из эксплуатационной документации;
* Чувствительная информация – информация, дополняющая эксплуатационную информацию об ИС (например, сведения из проектной документации).

В частности, нарушитель может иметь:

* Данные об организации работы, структуре и используемых технических, программных и программно-технических средствах;
* Сведения об информационных ресурсах: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
* Данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств;
* Данные о реализованных в программных средствах защиты информации принципах и алгоритмах;
* Исходные тексты программного обеспечения;
* Сведения о возможных каналах реализации угроз;
* Информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в автоматизированной информационной системе (АИС), к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией о ИС и функционально ориентированных АС, включая информацию об уязвимостях технических и программных средств. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными о ИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные технические меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности, предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

Предположения об имеющихся у нарушителя средствах реализации угроз:

* аппаратные компоненты средства защиты;
* доступные в свободной продаже технические средства и программное обеспечение;
* специально разработанные технические средства и программное обеспечение.

**Нарушители согласно банку данных угроз ФСТЭК России**

Дополнительно в банке данных угроз ФСТЭК России определены три типа внешних и внутренних нарушителей – с низким потенциалом, со средним потенциалом и с высоким потенциалом.

Нарушители с низким потенциалом имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Также такие нарушители имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак и реализацию атак на информационную систему.

Нарушители со средним потенциалом обладают всеми возможностями нарушителей с низким потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы.

Нарушители с высоким потенциалом обладают всеми возможностями нарушителей с низким и средним потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.

# Модель угроз

| **№ п/п** | **Идентификатор** | **Описание угрозы** | **Способ реализации угрозы** | **Источники угрозы** | **Объекты воздействия** | **Нарушаемые свойства безопасности информации** |
| --- | --- | --- | --- | --- | --- | --- |
|  | УБИ.006 | Угроза внедрения кода или данных Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устройство вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями, автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.) или с использованием аутентификационных данных, заданных «по умолчанию», а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов, и блокирования работы устройства при выполнении определенных команд. | Реализация данной угрозы возможна:  в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников;  при наличии у него привилегий установки программного обеспечения;  в случае неизмененных владельцем учетных данных IoT-устройства (заводских пароля и логина) | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение | К, Ц, Д |
|  | УБИ.007 | Угроза воздействия на программы с высокими привилегиями. Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. | Реализация данной угрозы возможна при условиях:  обладания дискредитируемой программой повышенными привилегиями в системе;  осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя;  нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе | Внутренний нарушитель со средним потенциалом  Внешний нарушитель со средним потенциалом | Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик | К, Ц |
|  | УБИ.008 | Угроза восстановления и/или повторного использования аутентификационной информации. Угроза заключается в возможности доступа к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хэша пароля, для восстановления сеанса. |  | Внутренний нарушитель с низким потенциалом  Внешний нарушитель с низким потенциалом | Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя | К |
|  | УБИ.015 | Угроза доступа к защищаемым файлам с использованием обходного пути. Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения).  Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. | Реализация данной угрозы возможна при условиях:  наличие у нарушителя прав доступа к некоторым объектам файловой системы;  отсутствие проверки вводимых пользователем данных;  наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью | Внутренний нарушитель с низким потенциалом  Внешний нарушитель с низким потенциалом | Объекты файловой системы | К |
|  | УБИ.023 | Угроза изменения компонентов информационной (автоматизированной) системы Угроза заключается в возможности получения нарушителем доступа к сети, файлам, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому - внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе.  Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации информационной системы. | Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе и возможности подключения дополнительного периферийного оборудования | Внутренний нарушитель с низким потенциалом | Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение | К, Ц, Д |
|  | УБИ.027 | Угроза искажения вводимой и выводимой на периферийные устройства информацииУгроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены, или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства.  Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. | Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок | Внутренний нарушитель с низким потенциалом | Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение | Ц |
|  | УБИ.028 | Угроза использования альтернативных путей доступа к ресурсам. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса).  Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. | Реализация данной угрозы возможна при условии наличия у нарушителя:  возможности ввода произвольных данных в адресную строку;  сведений о пути к защищаемому ресурсу;  возможности изменения интерфейса ввода входных данных | Внутренний нарушитель с низким потенциалом | Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение | К |
|  | УБИ.030: | Угроза использования информации идентификации/аутентификации, заданной по умолчанию. Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников  или от информационного сервиса идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты.  Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему или тем, что при прохождении на информационном сервисе процедуры регистрации механизм автоматической генерации паролей выдает одинаковые или сходные пароли пользователям с похожими логинами. Более того, на многих устройствах  идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). | Реализация данной угрозы возможна при одном из следующих условий:  наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты;  успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты  наличие у нарушителя сведений о логине используемом при регистрации атакуемым пользователем | Внутренний нарушитель с низким потенциалом | Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты | К, Ц, Д |
|  | УБИ.067 | Угроза неправомерного ознакомления с защищаемой информацией. Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей.  Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. | Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др. | Внутренний нарушитель с низким потенциалом | Аппаратное обеспечение, носители информации, объекты файловой системы | К |
|  | УБИ.115 | Угроза перехвата вводимой и выводимой на периферийные устройства информации. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств.  Данная угроза обусловлена недостаточностью мер защиты информации от утечки и контроля потоков данных, а также невозможностью осуществления защиты вводимой и выводимой на периферийные устройства информации с помощью криптографических средств (т.к. представление пользователям системы информации должно осуществляться в доступном для понимания виде). | Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др. | Внутренний нарушитель с низким потенциалом | Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение | К |
|  | УБИ.139 | Угроза преодоления физической защиты . Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия.  Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.). | Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.) | Внутренний нарушитель со средним потенциалом | Сервер, рабочая станция, носитель информации, аппаратное обеспечение | К, Ц, Д |
|  | УБИ.140 | Угроза несанкционированного использования привилегированных функций мобильного устройства. Угроза заключается в возможности снятия нарушителем предустановленных производителем ограничений на конфигурирование привилегированных функций мобильного устройства. Данная угроза обусловлена наличием уязвимостей в операционных системах мобильного устройства, позволяющих получить доступ к настройкам привилегированных функций. | Реализация данной угрозы возможна при получении нарушителем доступа к мобильному устройству | Внешний нарушитель с высоким потенциалом | Мобильное устройство | К, Ц, Д |
|  | УБИ.157 | Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации. Угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации.  Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. | Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.) | Внутренний нарушитель с высоким потенциалом | Сервер, рабочая станция, носитель информации, аппаратное обеспечение | Ц, Д |
|  | УБИ.160 | Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.  Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации.  Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. | Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.) | Внутренний нарушитель со средним потенциалом | Сервер, рабочая станция, носитель информации, аппаратное обеспечение | К, Д |
|  | УБИ.169 | Угроза наличия механизмов разработчика. Угроза заключается в возможности перехвата управления программой за счёт использования отладочных механизмов (специальных программных функций или аппаратных элементов, помогающих проводить тестирование и отладку средств во время их разработки).  Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе разработки средств защиты информации.  Реализация данной угрозы возможна при условии, что в программе не удалены отладочные механизмы |  | Внутренний нарушитель со средним потенциалом | Программное обеспечение, техническое средство | К, Ц, Д |
|  | УБИ.182 | Угроза физического устаревания аппаратных компонентов. Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций).  Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем |  | Внутренний нарушитель с низким потенциалом | Аппаратное средство | Д |

# 5. Перечень наиболее популярный уязвимостей серверной части мобильного банковское приложение и рекомендации по противодействия им.

**1. Слабый контроль серверных компонентов**

API-сервисы доступны в Интернете даже без мобильных приложений, для которых они были созданы. Хакеры могут прослушивать беспроводную сеть или произвести атаку с «человеком посередине», чтобы выявить вызовы API, модифицировать их и напрямую атаковать API.

*Рекомендации. В серверной части мобильного приложения должны применяться безопасные практики написания программного кода и конфигурирования. В частности, API-интерфейс должен надежно проверять идентификацию и полномочия лица, его вызывающего.*

**2. Ненадлежащая обработка сеанса**

Атакующие могут использовать учетные данные сессии при аутентификации для доступа к серверным сервисам и осуществлять действия от имени конкретного пользователя.

*Рекомендации. Применяйте механизм ограничения времени действия cookie для сессий как на сервере, так и на клиенте. В общем случае рекомендуется ограничить время одним часом или менее. Проследите, чтобы ваш сервер открывал новую сессию для каждого пользователя всякий раз, когда требуется аутентификация. Убедитесь, что на сервере прежние сессии уничтожаются/объявляются недействительными для предотвращения повторного использования.*

**3. Недостаточная аутентификация**

Данная угроза возникает, когда сервер позволяет получать доступ к важной информации или функциям без должной аутентификации. Также существуют сценарии, когда веб-сервер позволяет несанкционированноо восстанавливать, модифицировать или получать пароли других пользователей

*Рекомендации. Большинство атак на аутентификацию связано с использованием исключительно паролей. Ранее считавшиеся хорошими требования к смене пароля и его сложности способствуют использованию ненадежных паролей пользователями. Согласно последним рекомендациям NIST, организациям следует применять многофакторную аутентификацию.*

**4. Подбор пароля**

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.

*Рекомендации. Использовать надежные пароли* *длиной как минимум 10–12 символов, состоящие из разнотипных комбинаций заглавных и строчных буквы, символов, цифр. Также для генерации и хранения паролей можно применять специальные менеджеры. Нельзя хранить пароли просто на компьютере, в браузерах и FTP-клиентах, нужно регулярно их менять.*

**5. Ошибки в бизнес-логике**

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.

*Рекомендации. ?*

# 6. Оценка рисков?

## 7. Заключение

Множество банков 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.

В настоящее время банкам стоит 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, стоит тщательно тестировать приложения, их механизмы защиты и не забывать про анализ исходного кода