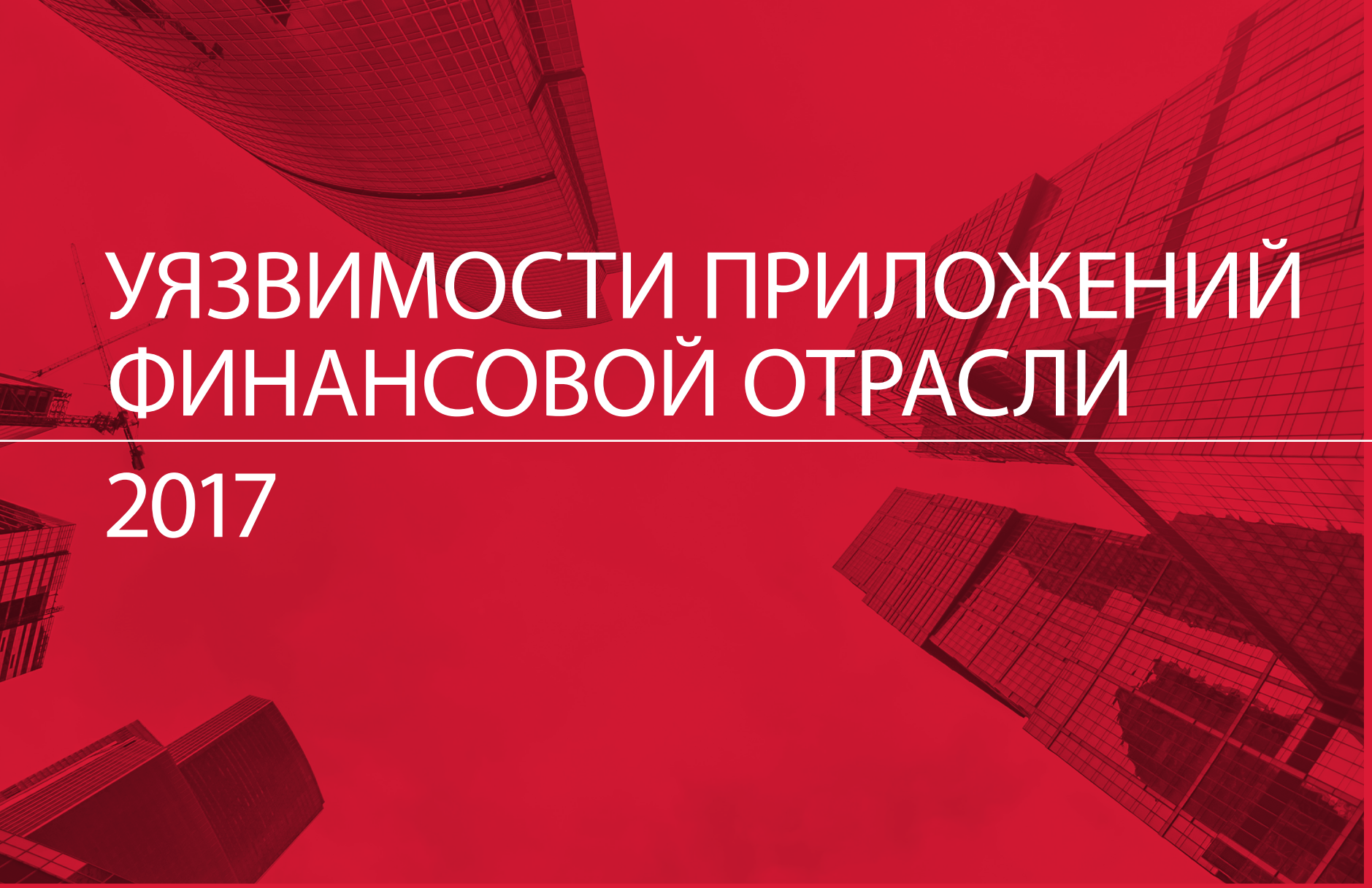


УЯЗВИМОСТИ ПРИЛОЖЕНИЙ ФИНАНСОВОЙ ОТРАСЛИ

2017

POSITIVE TECHNOLOGIES

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

С каждым годом банки все активнее используют передовые информационные технологии, позволяющие клиентам удаленно управлять банковскими продуктами для осуществления платежей, денежных переводов и других операций в максимально удобной форме. В 2016 году популярность подобных финансовых инструментов в России значительно выросла благодаря развитию бесконтактных систем оплаты: к уже привычным PayPass и payWave присоединились технологии NFC-платежей с помощью смартфонов — Apple Pay и Google Wallet.

Однако безопасность общедоступных веб- и мобильных приложений в финансовой сфере до сих пор оставляет желать лучшего, поскольку для таких приложений характерны все уязвимости и угрозы, известные в области безопасности приложений (WASC TC v. 2). При этом в случае банковских приложений реализация угроз приводит к серьезным последствиям — включая хищение денежных средств, несанкционированный доступ к персональным данным и банковской тайне, а также репутационные потери для бизнеса.

Данный аналитический отчет основан на статистике, собранной экспертами Positive Technologies в 2016 году в ходе работ по анализу защищенности систем дистанционного банковского обслуживания (ДБО) и автоматизированных банковских систем (АБС). Здесь же представлен сравнительный анализ данных 2016 года с результатами аналогичных исследований 2015 года. Исследование позволяет оценить текущий уровень защищенности финансовых приложений и динамику их развития с точки зрения обеспечения информационной безопасности. Работа также содержит рекомендации, которые помогут вендорам, разработчикам ПО, сотрудникам и клиентам банков повысить уровень защищенности при разработке, поддержке и использовании финансовых приложений.

РЕЗЮМЕ

Больше опасных уязвимостей. Хотя общее число уязвимостей в финансовых приложениях в 2016 году снизилось, доля критически опасных уязвимостей выросла на 8%, а доля уязвимостей среднего уровня риска — на 18%. Наиболее распространены оказались уязвимости, связанные с недостатками механизмов идентификации, аутентификации и авторизации.

Внедрено — не значит защищено. В продуктивных системах выявлено почти в два раза больше уязвимостей, чем в системах, находящихся в разработке.

Собственная разработка безопасней. Финансовые приложения, разработанные вендорами, в среднем содержат в два раза больше уязвимостей, чем те, которые разработаны банками самостоятельно.

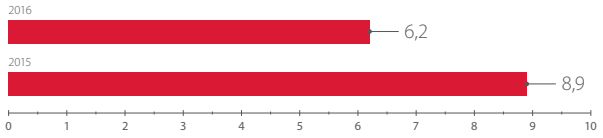
Большинство онлайн-банков (71%) имеют недостатки в реализации двухфакторной аутентификации. Каждый третий онлайн-банк содержит уязвимости, позволяющие украсть деньги.

Мобильные банки отличаются проблемами с хранением и передачей данных: в каждом третьем приложении можно перехватить или подобрать учетные данные для доступа. Банковские iOS-приложения по-прежнему безопаснее, чем их аналоги для Android. При этом серверные части мобильных банков защищены значительно хуже клиентских: уязвимости высокой степени риска найдены в каждой исследованной системе.

Автоматизированные банковские системы обычно считаются недоступными для внешнего злоумышленника. Однако две трети уязвимостей, выявленных в АБС, оказались критически опасными — включая такие, которые позволяют получить административный доступ к серверу. Тренды целевых атак 2016 года показывают[1], что злоумышленники все активнее используют подобные возможности для атак на финансовый сектор.

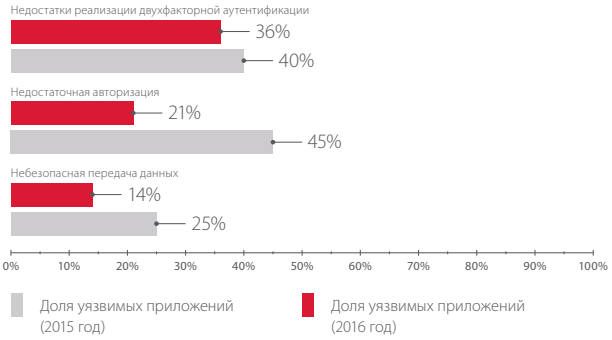
1 www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf

В 2016 году отмечается уменьшение количества уязвимостей, выявленных в финансовых приложениях.

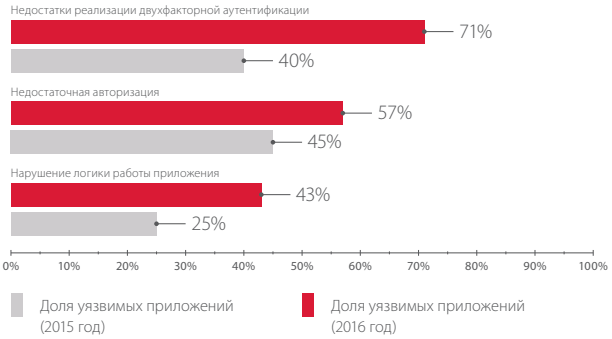


Среднее число уязвимостей в одном приложении

Наиболее распространены уязвимости, связанные с недостатками механизмов идентификации, аутентификации и авторизации.

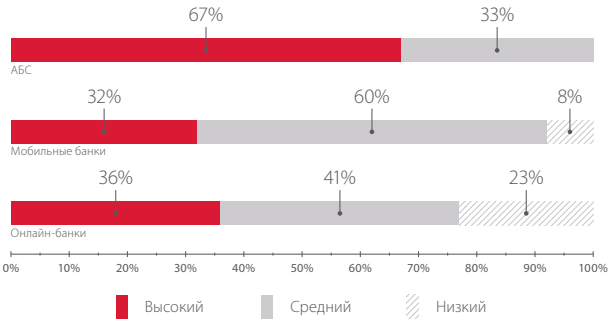


Критически опасные уязвимости мобильных банков



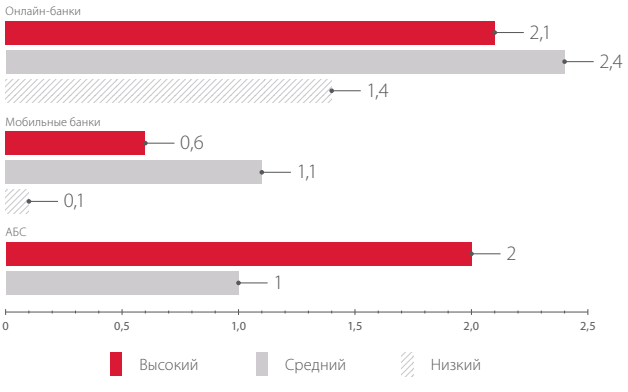
Критически опасные уязвимости онлайн-банков

Уровень риска выявленных уязвимостей значительно вырос.



Доли уязвимостей различного уровня риска

В среднем онлайн-банки содержат больше уязвимостей, чем мобильные банки и АБС.

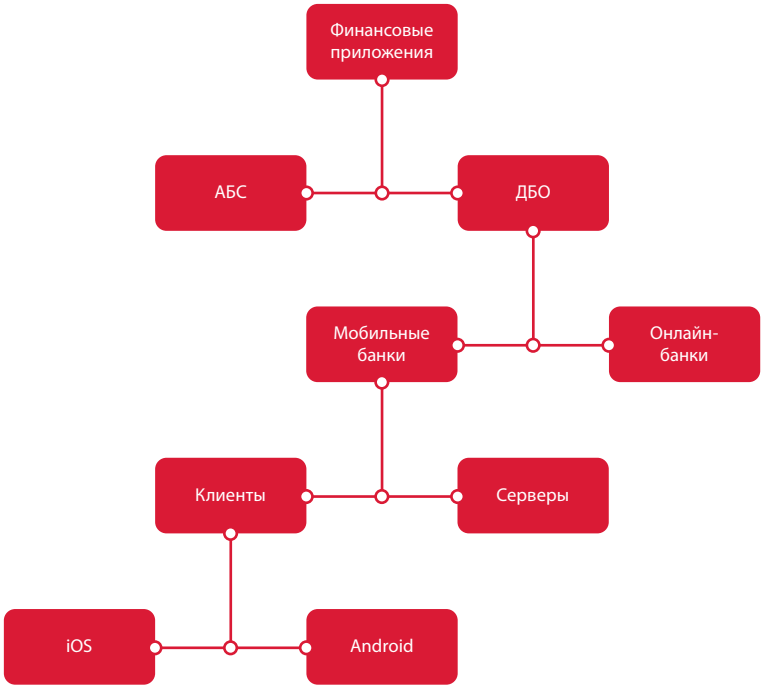


Среднее число уязвимостей различного уровня риска в одном приложении

1. ИСХОДНЫЕ ДАННЫЕ

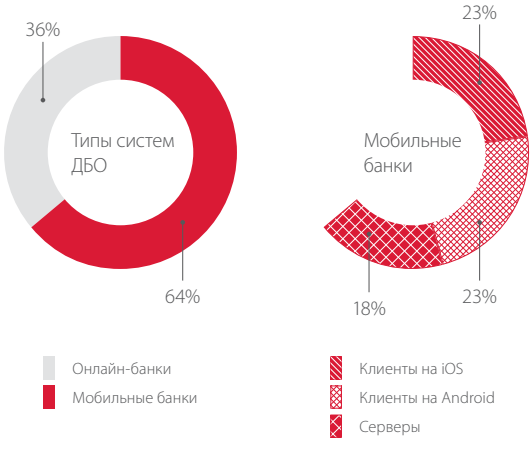
В рамках исследования были рассмотрены 24 системы, используемые для проведения финансовых операций и автоматизации банковской деятельности. Исходные данные получены в ходе работ по анализу защищенности, проведенных специалистами Positive Technologies в 2016 году.

Объектами исследования в 2016 году стали онлайн-банки, мобильные банки и системы АБС.



Две трети анализируемых систем ДБО составили мобильные банки, среди которых были клиенты для мобильных операционных систем Android и iOS, а также их серверные части.

Все рассмотренные системы ДБО применялись для обслуживания физических лиц.

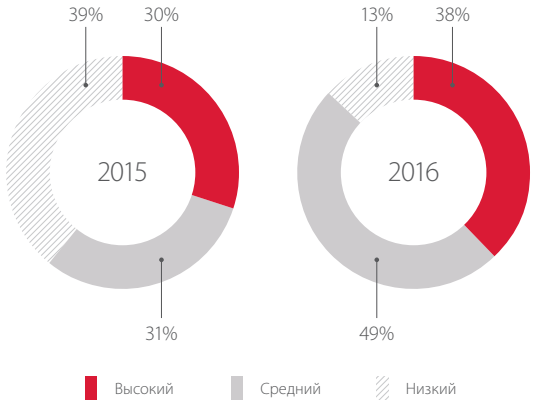


2. НЕДОСТАТКИ ЗАЩИТЫ ФИНАНСОВЫХ ПРИЛОЖЕНИЙ

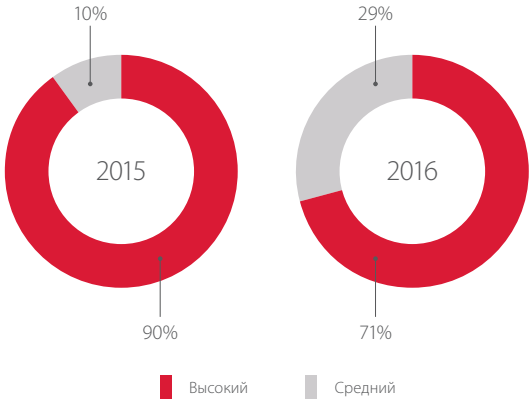
2.1. Общая статистика

В каждом из рассмотренных приложений были выявлены недостатки безопасности. В среднем в 2016 году на каждое финансовое приложение приходилось по 6 уязвимостей, что значительно меньше показателей предыдущего года, когда на каждую систему ДБО приходилось около 9 уязвимостей. Это говорит о том, что компании не игнорируют сведения о возможных угрозах, а принимают меры по защите приложений.

В 2016 году доля уязвимостей высокого уровня риска возросла на 8%, среднего — на 18%.



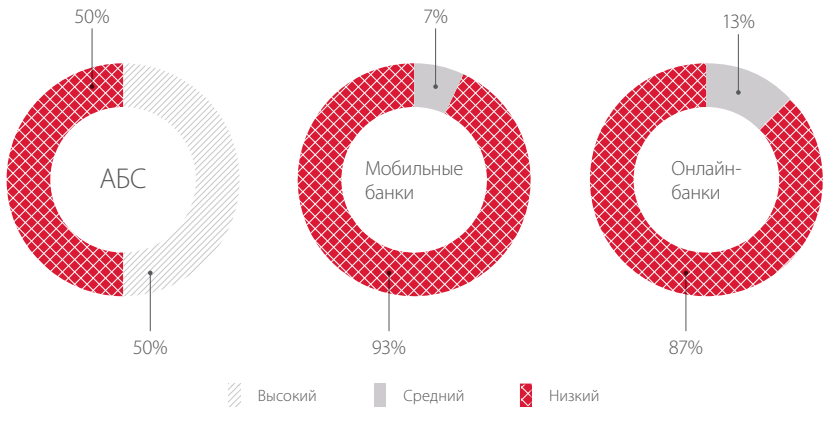
Уязвимости различного уровня риска



Доли приложений по максимальному уровню риска уязвимостей

В 2015 году всего треть уязвимостей имели высокий уровень риска, но они были распределены равномерно практически по всем исследованным системам, лишь в 10% систем ДБО не было найдено критически опасных уязвимостей. В 2016 году картина изменилась: 38% выявленных недостатков — критически опасные, однако сосредоточены они в 71% проанализированных систем. А каждое третье приложение содержало уязвимости не выше среднего уровня опасности.

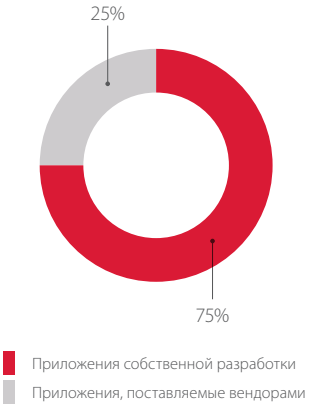
Уровень защищенности финансовых приложений остается низким.

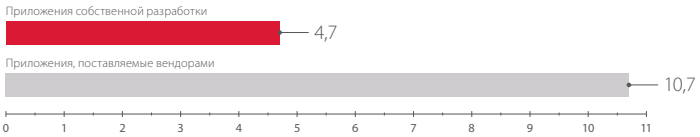


Доли приложений по уровню защищенности

2.2. Сравнение приложений собственной разработки и поставляемых вендорами

75% рассмотренных систем разработаны финансовыми организациями самостоятельно.

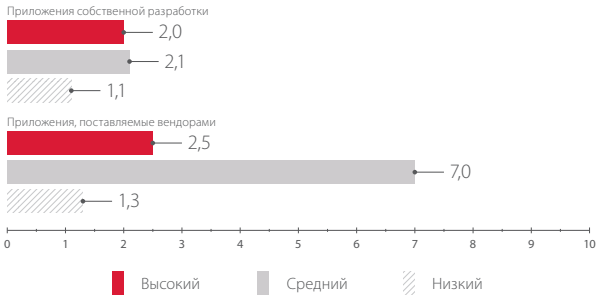




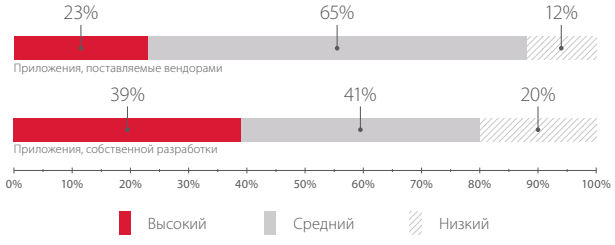
Среднее количество уязвимостей в одном приложении

Анализ защищенности финансовых приложений, разработанных вендорами, по прежнему показывает не лучшие результаты. Такие приложения в среднем содержали два раза больше недостатков чем те, которые банки разработали самостоятельно.

Причем в приложениях, разработанных профессиональными вендорами, 23% выявленных уязвимостей характеризовались высокой степенью риска, и среди них преобладали «Внедрение внешних сущностей XML» и «Нарушение логики работы приложения», а 65% уязвимостей представляли средний уровень опасности. Среди финансовых приложений собственной разработки 39% также содержали критически опасные уязвимости, большую часть из которых составляли ошибки, связанные с недостаточной авторизацией и с реализацией двухфакторной аутентификации.



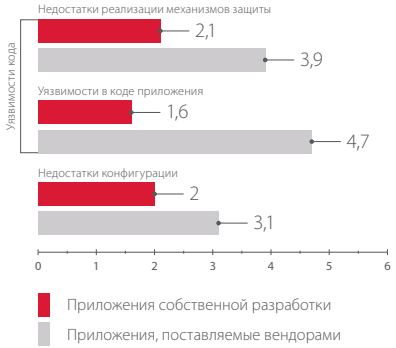
Среднее количество уязвимостей разных категорий риска в одном приложении



Уязвимости различного уровня риска

В приложениях, разработанных финансовыми учреждениями, преобладали недостатки реализации механизмов защиты, однако их код содержал меньше ошибок и уязвимостей, чем разработанный вендорами. Здесь стоит отметить, что недостатки механизмов защиты также относятся к уязвимостям в коде, однако возникают они из-за ошибок, допущенных на этапе проектирования и разработки технического задания. И виноваты в них не разработчики, которые написали код в строгом соответствии с планом, а проектировщики, которые не учли все нюансы методов защиты, например аутентификации или авторизации.

Среднее число уязвимостей в одном приложении (2016)



Среднее число уязвимостей в одном приложении (2015)

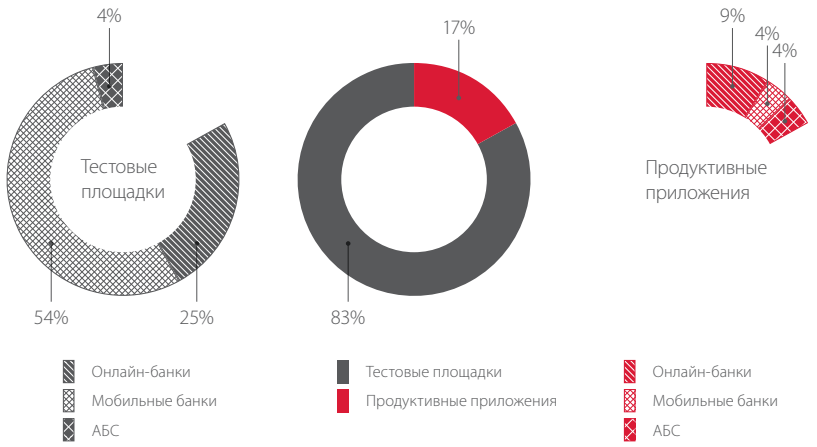
Полученные результаты показывают, что системы собственной разработки банков лучше защищены. Таким образом, создание собственных команд разработчиков и построение процесса безопасной разработки оправдывает вложение необходимых ресурсов.

Стоит отметить, что устранение уязвимостей для вендоров — довольно длительный процесс. Сначала уязвимости выявляются заказчиком или исследователем безопасности, затем эта информация передается вендору, которому необходимо разобраться в истинной причине возникновения уязвимости и убедиться, что проблема кроется именно в его продукте. Затем специалисты вендора разрабатывают патч, тестируют его на всех версиях своего продукта и, наконец, передают заказчикам, которые в свою очередь тоже должны сначала его протестировать, а потом только устанавливать в «боевую» систему. Таким образом все заказчики одновременно получают обновления, если у кого-то из них была выявлена уязвимость, и это можно отнести как к преимуществам (теоретически можно не тратиться на анализ защищенности используемых приложений), так и к недостаткам (злоумышленник, обнаруживший уязвимость в одном приложении, может атаковать и другие банки, зная, что они используют решения одного вендора).

Однако если банк разрабатывал финансовое приложение самостоятельно, то процесс устранения уязвимостей пройдет значительно быстрее. Затягивая с выпуском обновлений, банк рискует собственными финансами и доверием клиентов.

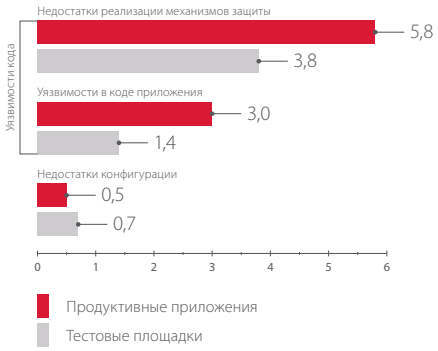
2.3. Сравнение тестовых и продуктивных приложений

Проведение анализа защищенности до начала промышленной эксплуатации финансовых приложений — это один из главных шагов на пути к созданию защищенной системы. 83% исследованных приложений находились на этапе разработки, однако среднее количество уязвимостей в них оказалось меньше, чем в продуктивных приложениях.

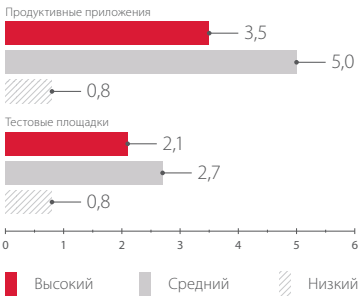


Доля тестовых и продуктивных приложений

В продуктивных системах было выявлено почти в 2 раза больше уязвимостей, чем в тестовых.



Среднее число уязвимостей разных категорий в тестовых и продуктивных системах



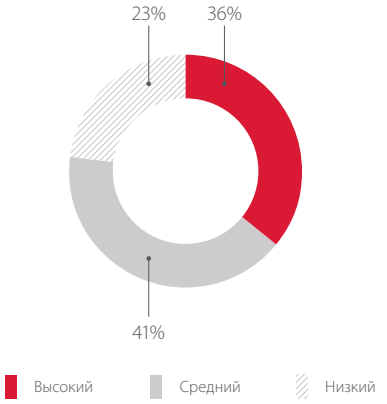
Среднее число уязвимостей разного уровня риска в тестовых и продуктивных системах

Наибольшее количество уязвимостей как в тестовых, так и продуктивных системах относились к недостаткам реализации механизмов защиты. В коде финансовых приложений, находящихся в эксплуатации, было выявлено довольно много уязвимостей, среди которых преобладали «Межсайтовое выполнение сценариев» и «Внедрение внешних сущностей XML». Предположительно это связано с тем, что анализ защищенности продуктивных систем преимущественно проводился для приложений, в которые недавно была внедрена новая функциональность. Внесение изменений в код приложения может привносить в систему новые уязвимости, поэтому необходимо проводить анализ защищенности регулярно.

Напомним, что на уровне исходного кода веб-приложение может содержать множество критически опасных уязвимостей. Количество этих уязвимостей можно минимизировать, если при разработке приложения придерживаться практик безопасного программирования (SSDLC). А для своевременного выявления уязвимостей в коде необходимо проводить регулярные проверки качества кода, например путем его анализа методом белого ящика (в том числе — с использованием автоматизированных средств).

3. УЯЗВИМОСТИ И УГРОЗЫ ОНЛАЙН-БАНКОВ

Почти во всех онлайн-банках (кроме одного) была выявлена хотя бы одна критически опасная уязвимость. В среднем на каждый онлайн-банк пришлось по 2,1 уязвимости высокого уровня риска, что меньше показателей прошлого года, когда на каждую систему ДБО приходилось по 4,2.

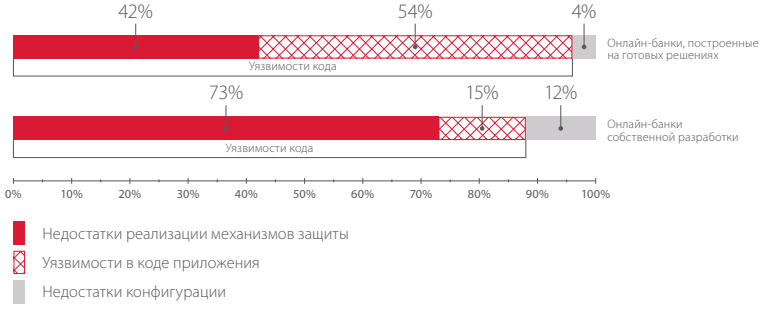


Уровень риска выявленных уязвимостей

100% онлайн-банков содержали недостатки реализации механизмов защиты.

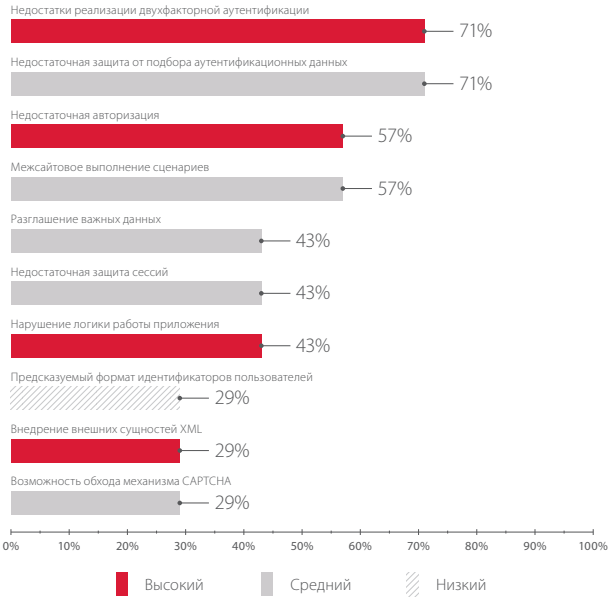
Среднее число уязвимостей разных категорий в финансовых веб-приложениях

В онлайн-банках собственной разработки преобладали уязвимости, связанные с недостатками реализации механизмов защиты (такие, как недостаточная защита от подбора аутентификационных данных, недостатки парольной политики, возможность обхода механизма CAPTCHA), а приложения, построенные на готовых решениях, содержали большое количество уязвимостей в коде (например, «Межсайтовое выполнение сценариев», «Внедрение внешних сущностей XML»).



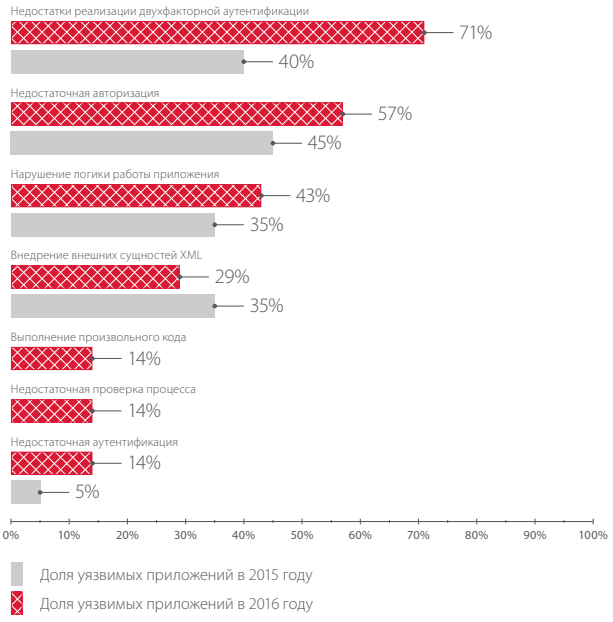
Доля уязвимостей разных категорий

Кроме того, в каждом втором онлайн-банке собственной разработки использовалось устаревшее ПО. Например, в одном анализируемом приложении использовался устаревший фреймворк PrimeFaces 5.3.x с уязвимостью, позволявшей нарушителю удаленно выполнять произвольный код в системе. Злоумышленник имел возможность загрузить на сервер произвольный файл, в том числе веб-интерпретатор командной строки, и проводить атаки с целью повышения привилегий. А в случае избыточности привилегий приложения либо в результате эксплуатации уязвимостей ОС злоумышленник мог получить полный контроль над сервером.



Топ-10 уязвимостей онлайн-банков

Перечень наиболее распространенных уязвимостей год от года меняется незначительно. Несмотря на постоянное упоминание, одни и те же уязвимости занимают лидирующие позиции в наших отчетах. Однако в 2016 году на первые строчки рейтинга поднялись уязвимости высокого уровня риска, хотя прежде первые места занимали уязвимости низкого уровня риска.



Критически опасные уязвимости онлайн-банков

Во всех онлайн-банках присутствовали уязвимости среднего уровня риска. Такие уязвимости, как «Недостаточная защита сессий» и «Межсайтовое выполнение сценариев», позволяют совершать атаки на клиентов банков (например, перехватывать значения Cookie или похищать учетные данные). Они вошли в топ-10 самых распространенных уязвимостей в этом году для всех веб-приложений, а не только для онлайн-банков, что было наглядно продемонстрировано в нашем исследовании уязвимостей веб-приложений за 2016 год[2].

Некорректная реализация механизма CAPTCHA (например, когда приложение позволяет использовать сессию CAPTCHA повторно) равносильна отсутствию данного механизма и позволяет злоумышленнику осуществить атаку, направленную на подбор учетных данных пользователей.

В 2016 году для всех финансовых приложений был отмечен рост числа критически опасных уязвимостей, связанных с недостатками механизмов аутентификации. Особенно заметно это в части онлайн-банков, при анализе защищенности которых было установлено, что 71% приложений имеют недостатки в реализации двухфакторной аутентификации.

Недостатки реализации двухфакторной аутентификации

В 2015 году мы уже отмечали, что данная проблема стала наиболее распространенной среди всех недостатков механизмов аутентификации, но доля уязвимых систем тогда составила лишь 33% в системах ДБО, поставляемых вендорами, и 45% в системах собственной разработки банков.

Двухфакторная аутентификация при входе в личный кабинет присутствовала лишь в 71% финансовых веб-приложений, а подтверждение транзакций одноразовым паролем требовалось и вовсе только в половине систем.

Среди недостатков реализации двухфакторной аутентификации (помимо ее отсутствия) можно отметить следующие:

+ генерация одноразового пароля на стороне клиента;
+ одноразовый пароль не привязан к совершаемой операции;
+ отсутствие ограничения по числу попыток ввода одноразового пароля;
+ отсутствие ограничения на время жизни одноразового пароля.

Когда второй фактор аутентификации (обычно в онлайн-банках это одноразовый код, присылаемый на телефон) отсутствует или реализован некорректно, злоумышленник, получивший (подсмотревший, подобравший) логин и пароль от личного кабинета пользователя, получает доступ к его счетам и может проводить финансовые операции.

Недостаточная защита от подбора аутентификационных данных

Больше половины финансовых веб-приложений не обеспечивают достаточную защиту от подбора аутентификационных данных (идентификаторов и паролей пользователей). Среди недостатков данного типа можно выделить:

+ использование предсказуемых идентификаторов, таких как номер мобильного телефона;
+ использование предсказуемых паролей для входа в систему, таких как дата рождения пользователя, назначенных по умолчанию и без возможности смены;
+ отсутствие либо возможность обхода механизма CAPTCHA;
+ отсутствие временной блокировки учетных записей после нескольких неудачных попыток ввода учетных данных.

Защита аутентификационных данных пользователей должна быть первоочередной мерой по обеспечению безопасности приложения.

2 www.ptsecurity.com/ru-ru/research/analytics/

В 25% исследуемых онлайн-банков одновременно присутствовали и уязвимости, связанные с недостаточной защитой от подбора аутентификационных данных, и недостатки реализации двухфакторной аутентификации. Это значит, что почти в каждом четвертом онлайн-банке злоумышленник мог получить полный контроль над счетами клиентов.

Недостаточная авторизация

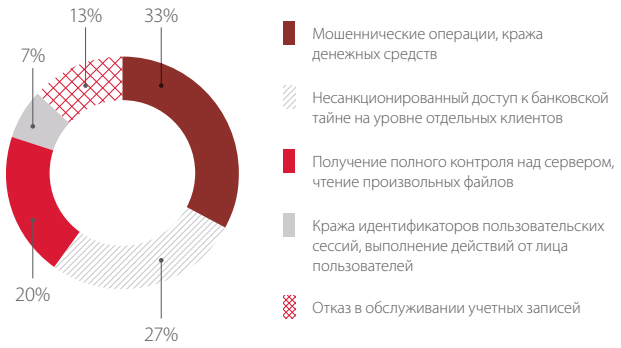
Высокой остается доля приложений, в которых некорректно реализованы механизмы авторизации и разграничения доступа к чувствительной информации (57%). В результате эксплуатации этой уязвимости злоумышленник может проводить атаки на клиентов банков и получать несанкционированный доступ к информации, в том числе составляющей банковскую тайну. Так, в одном из онлайн-банков нарушитель мог узнать график платежей по кредиту, а в другом — остаток денежных средств на счетах других пользователей.

Нарушение логики работы

Ошибки, допущенные при проектировании приложения, привели к тому, что в каждом третьем онлайн-банке злоумышленник может провести атаки на логику работы. Довольно распространенной является проблема, связанная с округлением при переводе денежных средств между счетами. Например, при переводе с одного счета на другой 1,0009 рубля происходит неверная конвертация в пользу клиента и на счет поступает 1,001 рубля. Конечно, много на таком переводе не заработать, но и транзакцию такую можно провести не один раз.

Угрозы информационной безопасности онлайн-банков

Выявленные уязвимости в веб-приложениях могут нести значительные репутационные и финансовые потери для банков и их клиентов. Эксплуатация уязвимостей может привести к таким ощутимым последствиям, как, например, кража денежных средств в результате проведения мошеннических операций в 33% веб-приложений. В 27% веб-приложений злоумышленник может получить доступ к сведениям, составляющим банковскую тайну, на уровне отдельных клиентов, например к информации об остатках денежных средств на счетах, о графиках платежей по кредитам.



Возможные последствия атак на онлайн-банки

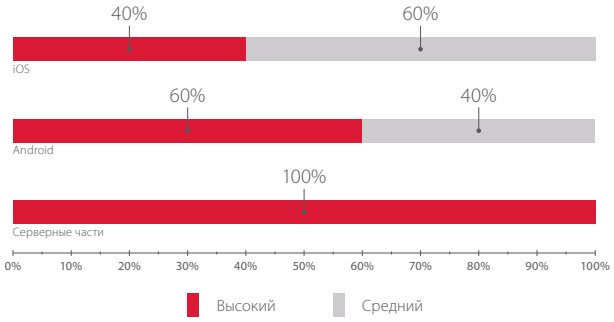
4. УЯЗВИМОСТИ И УГРОЗЫ МОБИЛЬНЫХ БАНКОВ

В 64% мобильных банков была выявлена хотя бы одна критически опасная уязвимость. В среднем на каждое приложение пришлось по 0,9 уязвимости высокого уровня риска.

Уровень риска выявленных уязвимостей

Уровень защищенности iOS приложений по-прежнему выше, чем у Android.

Серверные части мобильных банков оказались наиболее подвержены критически опасным уязвимостям.



Доля мобильных банков по максимальному уровню риска уязвимостей

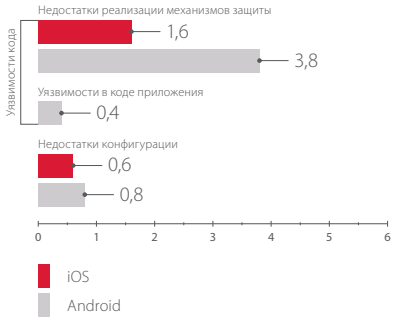
Для всех рассмотренных мобильных банков мы анализировали по два идентичных приложения, разработанных для разных операционных систем — Android и iOS. В некоторых случаях приложение для iOS не содержало уязвимостей, которые были обнаружены в Android-приложении.

Доли уязвимостей разных категорий

Все серверные части мобильных банков содержали критически опасные уязвимости. В каждой из них находились уязвимости, связанные с недостатками авторизации, аутентификации (в том числе двухфакторной).

Примечательно, что в мобильных приложениях, построенных на готовых решениях вендоров, не выявили ни одной уязвимости, связанной с недостатками конфигурации.

iOS-приложения в среднем содержат меньше уязвимостей, чем другие системы.

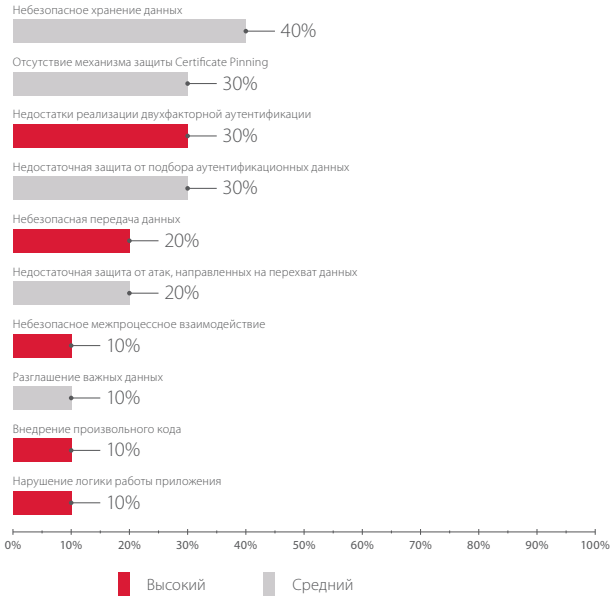


Среднее число уязвимостей разных категорий в мобильных банках

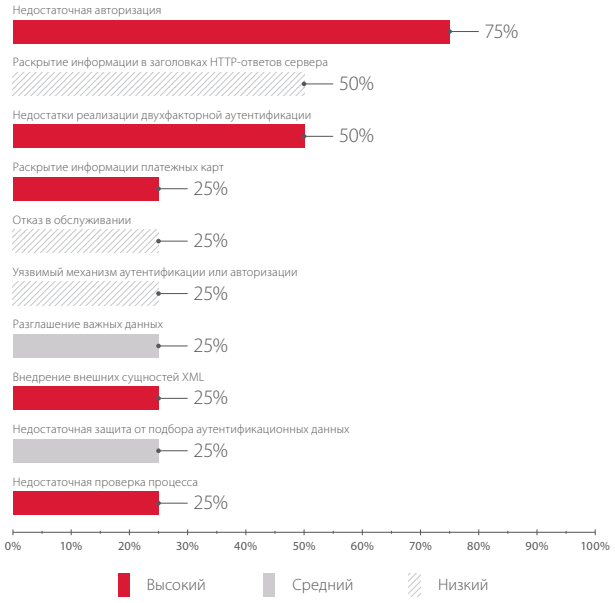
Среднее число уязвимостей в серверных частях мобильных банков

Как уже отмечалось ранее, недостатки механизмов защиты также относятся к уязвимостям в коде, но мы рассматриваем их отдельно, поскольку они появляются в системе еще на этапе проектирования.

В итоге таким уязвимостям, как «Недостаточная защита от атак, направленных на перехват данных», «Небезопасная передача данных», оказались подвержены только мобильные банки собственной разработки.



Топ-10 уязвимостей клиентских частей мобильных банков



Топ-10 уязвимостей серверных частей мобильных банков

Как и в прошлом году, в клиентах мобильных приложений часто встречались уязвимости, связанные с небезопасным хранением и (или) передачей данных. Эти две уязвимости можно оценить как высоким, так и средним уровнем риска в зависимости от реализуемой угрозы в конкретном проекте. Отсутствие механизма защиты Certificate Pinning для проверки подлинности сертификата сервера также позволяет злоумышленнику перехватить и изменить передаваемые данные. В одном из рассмотренных мобильных банков эта уязвимость позволяла полностью скомпрометировать одноразовые пароли, а в другом — перехватить учетные данные и получить доступ к аккаунту пользователя.

Для серверных частей мобильных приложений наиболее остро стоит проблема недостаточной авторизации. Эта уязвимость позволяет злоумышленнику получить доступ к чувствительной информации, хранящейся на сервере.

Недостатки реализации двухфакторной аутентификации

30% мобильных приложений для iOS и Android содержали недостатки в реализации двухфакторной аутентификации.

Двухфакторность, используемая во всех рассмотренных приложениях, состояла из:

1. фактора знания (это традиционные логин и пароль, которые предъявлял пользователь для входа в личный кабинет приложения);
2. фактора владения (это смартфон, на который приходил одноразовый код — one-time password).

Для удобства пользователей некоторые разработчики финансовых приложений упрощают процесс аутентификации и при этом ограничивают функциональность мобильного банка.

В одном мобильном приложении в качестве первого фактора аутентификации использовалась связка «номер мобильного телефона + дата рождения». Однако данная информация не является секретом и может быть получена злоумышленником из открытых источников (например, из социальных сетей). Более того, дату рождения и номер телефона невозможно сменить при компрометации, в отличие от традиционных логина и пароля. В данном случае двухфакторная аутентификация сводилась к однофакторной, а ее безопасность зависела только от одноразового пароля, который в ряде случаев не обеспечивает должной защиты:

+ телефон, на который приходит одноразовый пароль, утерян или украден;
+ в роли злоумышленника выступает знакомый жертвы, который имеет физический доступ к телефону (даже кратковременный);
+ одноразовый пароль никак не привязан к совершаемому действию. Злоумышленник, имеющий доступ к приложению или имеющий возможность подключить атакуемого к поддельной базовой станции, может сгенерировать множество одноразовых паролей на будущее, изменяя время на смартфоне.

Недостаточная защита от подбора аутентификационных данных

Нередко для доступа в мобильный банк достаточно ввести четырехзначный код. Если же в приложении при этом отсутствует защита от подбора (ограничение по количеству попыток ввода), то злоумышленнику требуется лишь перебрать 10 000 вариантов, а с использованием специального ПО это не занимает много времени.

В одном приложении у злоумышленника была возможность сделать выводы о корректности введенного логина по времени ответа сервера, поскольку в зависимости от того, правильно ли введен логин, время ответа отличалось.

Еще одна уязвимость, связанная с недостаточной защитой от подбора аутентификационных данных, заключалась в том, что ответ сервера содержал только информацию о результате сравнения введенного кода с тем, что хранился на сервере, при этом серверная часть не возвращала новый идентификатор сессии, а клиентская часть использовала идентификатор, сохраненный на устройстве. Другими словами, клиентская часть определяла, верно ли пользователь ввел пин-код, основываясь на ответе сервера, который в свою очередь можно было подменить.

Небезопасная передача данных

Обычно для обмена данными с сервером мобильные приложения используют защищенный протокол HTTPS. Однако в нескольких случаях клиентская часть имела недостаток в реализации функциональности, касающейся установления шифрованного соединения. Так, одно из приложений допускало использование сервером недоверенного самоподписанного сертификата. В случае атаки «человек посередине» злоумышленник мог подменить сертификат сервера и выполнить перехват и подмену передаваемых данных (например, аутентификационных). Установка сертификатов на устройство жертвы не требовалась, и атакующему было достаточно только контролировать канал передачи данных.

Недостаточная авторизация

При разработке одного из рассмотренных мобильных приложений была допущена следующая ошибка: получив (украв) смартфон и не зная ни логина, ни пароля клиента мобильного банка, злоумышленник мог получить доступ к минимальной функциональности приложения, включающей доступ к информации о банковских картах, оплате услуг и настройкам автоплатежей.

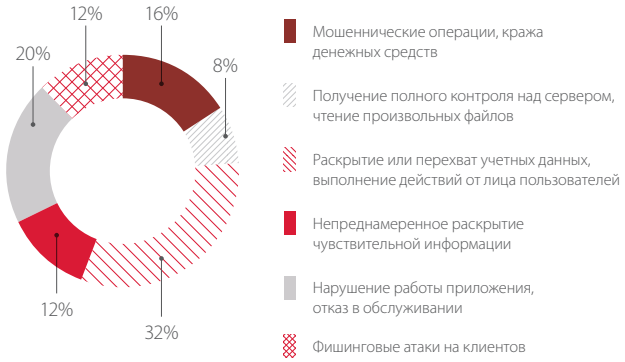
Для этого было достаточно на экране ввода пин-кода нажать на кнопку «назад», после чего злоумышленник попадал на экран аутентификации в мобильном-банке по паре логин-пароль. При этом текущий пользователь оставался авторизован в системе и ему была доступна описанная функциональность.

Угрозы информационной безопасности финансовых мобильных приложений

В 32% рассмотренных мобильных банков эксплуатация выявленных уязвимостей позволяла злоумышленникам расшифровать, перехватить, подобрать учетные данные для доступа в приложение или же и вовсе обойти процесс аутентификации, в результате чего получить доступ к мобильному приложению от лица легитимного пользователя и возможность совершать различные операции.

Были выявлены сценарии, когда злоумышленник, имеющий доступ к приложению или имеющий возможность подключить атакуемого к поддельной базовой станции, мог сгенерировать множество одноразовых паролей на будущее, изменяя время на смартфоне. А внедрившись

в сессию атакуемого с помощью межсайтового выполнения сценариев или атаки «человек посередине», нарушитель мог подделать реквизиты совершаемых операций и использовать перехваченные (сгенерированные) коды для проведения мошеннических операций на сумму до 5000 евро.



Возможные последствия атак на мобильные банки

Реализация атак на мобильные банки в 2016 году могла нанести серьезный ущерб как самим банкам, так и их клиентам, поскольку большинство этих атак связаны:

+ с проведением мошеннических операций;
+ получением полного контроля над серверной частью приложения;
+ выполнением действий от лица легитимного пользователя.

5. УЯЗВИМОСТИ И УГРОЗЫ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

Автоматизированные банковские системы — это особенный класс финансовых приложений, так как они применяются непосредственно в банках и для банков. Именно на АБС построена вся банковская деятельность: расчетно-кассовые операции и обслуживание клиентов (например, открытие счетов и выдача кредитов), операции на денежном и валютном рынках, сделки на биржевом рынке ценных бумаг и многое другое.

В 2016 году мы выделили следующие критически опасные уязвимости, характерные для АБС:

+ недостаточная авторизация;
+ недостаточная аутентификация;
+ внедрение внешних сущностей XML.

Две трети уязвимостей, выявленных в АБС, были критически опасными, а остальным мы присвоили средний уровень опасности.

Уровень риска найденных уязвимостей

Так, в одной АБС был получен административный доступ к серверу, а это означает, что потенциальный злоумышленник мог, оставаясь незамеченным, проводить любые мошеннические операции, связанные с деньгами, например заводить новые счета и указывать на них любое количество денег или же подменять платежные поручения, отправляемые в Центробанк. Обнаружить такую атаку, вероятней всего, получится лишь тогда, когда сумма перевода превысит сумму, имеющуюся на корреспондентском счете банка.

В начале 2016 года сразу два российских банка (Русский международный банк[3] и Металлинвестбанк[4]) понесли серьезный ущерб от атак на АБС, в общей сложности составивший более 1 млрд рублей.

Анализируя инциденты, произошедшие в 2016 году, мы отмечали, что целевые атаки на банки во многих случаях были направлены именно на подмену платежных поручений. Этот вектор атак сложно реализуем, поскольку АБС недоступны внешнему злоумышленнику, но и приводит к самым серьезным последствиям.

ЗАКЛЮЧЕНИЕ

Как показывает исследование, уровень защищенности финансовых приложений остается низким. В 2016 году отмечается уменьшение количества уязвимостей, выявленных в финансовых приложениях, однако их уровень риска повысился.

Основные проблемы в защите онлайн-банков и мобильных банков связаны с недостатками реализации механизмов защиты. Большинства уязвимостей этой категории можно избежать еще на этапе проектирования приложений и разработки технических заданий для программистов, если учесть все нюансы, связанные с реализацией механизмов аутентификации (в том числе двухфакторной) и авторизации.

Уязвимостей в коде можно также избежать еще на стадии разработки. Для этого необходимо придерживаться практик безопасного программирования (SSDLC) и уделять пристальное внимание тестированию механизмов защиты.

Для снижения рисков, связанных с эксплуатацией уязвимостей в любых финансовых приложениях, рекомендуется регулярно проводить анализ защищенности приложения на всех этапах, от разработки до эксплуатации, и оперативно устранять все выявленные уязвимости. Как показывает практика, наиболее эффективным методом выявления уязвимостей веб-приложения является анализ его исходного кода, в том числе автоматизированными средствами.

3 www.rbc.ru/finances/04/05/2016/5729c0169a794742dcc6551f
4 www.vedomosti.ru/finance/articles/2016/03/09/632749-hakeram-korscheta

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». 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.

POSITIVE TECHNOLOGIES

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