POSITIVE TECHNOLOGIES

СТАТИСТИКА УЯЗВИМОСТЕЙ ФИНАНСОВЫХ ПРИЛОЖЕНИЙ

2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Банки неизменно остаются одной из главных целей атак злоумышленников. К счастью, финансовые организации это отлично понимают и не хотят терять ни клиентов, ни деньги из-за кибератак. Для минимизации рисков компании самостоятельно или с привлечением сторонних экспертов проводят анализ защищенности используемых систем дистанционного банковского обслуживания (ДБО). Это позволяет выявить уязвимости общедоступных веб- и мобильных приложений и принять необходимые меры для их устранения.

Ежегодно мы анализируем общий уровень защищенности банковских систем на основании данных, собранных в ходе работ по анализу защищенности систем ДБО. Данный отчет содержит статистику и результаты анализа интернет- и мобильных банков, проведенного специалистами компании Positive Technologies в 2017 году.

Выводы, сделанные по результатам этого исследования, могут не отражать актуальное состояние защищенности информационных систем не вошедших в выборку организаций. Наша цель — обратить внимание специалистов по ИБ отрасли на наиболее актуальные проблемы и помочь им своевременно выявить и устранить уязвимости.

РЕЗЮМЕ

Мы наблюдаем повышение уровня защищенности финансовых приложений. С каждым годом снижается доля систем ДБО, в которых обнаруживаются критически опасные уязвимости. Так, в 2015 году уязвимости высокого уровня риска содержались в 90% систем, в 2016 году — в 71%, а в 2017 — в 56% проанализированных систем. Компании принимают меры по защите приложений и в первую очередь стремятся устранить критически опасные уязвимости.

В этом году финансовые приложения, построенные на готовых вендорских решениях, содержали меньше критически опасных уязвимостей, чем те, что банки разработали самостоятельно. Это говорит о том, что вендоры стали больше внимания уделять вопросам безопасности, в то время как банкам по-прежнему не хватает в штате опытных разработчиков и грамотно выстроенного процесса безопасной разработки.

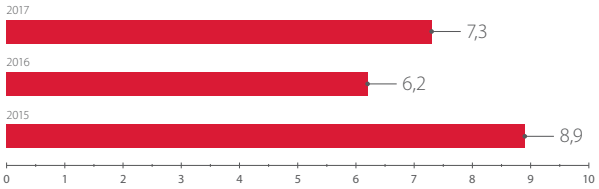
В 2017 году большинство проанализированных систем (61%) находились в промышленной эксплуатации и были доступны клиентам. Среднее количество уязвимостей в продуктивных приложениях, как и в предыдущие годы, превысило аналогичный показатель в тестовых системах. Однако в среднем число критически опасных уязвимостей отличалось незначительно: по 1,7 уязвимости на одну продуктивную систему против 1,6 на тестовую.

В трети онлайн-банков отсутствовали критически опасные уязвимости, в то время как в 2016 году уязвимости высокого уровня риска присутствовали во всех финансовых веб-приложениях, кроме одного. Главной угрозой вследствие эксплуатации уязвимостей стал для онлайн-банков доступ к сведениям, составляющим банковскую тайну клиентов, и личной информации. Выявленные уязвимости в 94% онлайн-банков могли быть использованы злоумышленниками именно для этой цели.

В 8% мобильных банков общий уровень защищенности был оценен как «приемлемый», поскольку в этих приложениях отсутствовали серьезные уязвимости. iOS-приложения вновь оказались защищены лучше, чем их аналоги для Android. Доля уязвимостей высокого уровня риска в iOS-приложениях составила всего 25%, в то время как в Android-приложениях она занимает 56%.

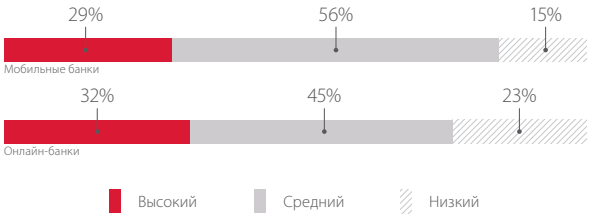
По сравнению с 2016 годом в 2017-м отмечается повышение уровня защищенности финансовых приложений за счет снижения уровня риска выявленных уязвимостей

Среднее количество уязвимостей, приходящееся на одну систему, немного выросло



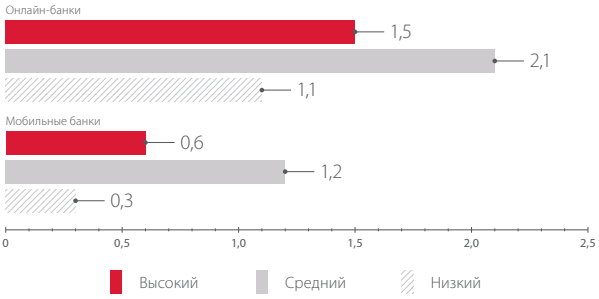
Среднее число уязвимостей в одном приложении

Уровень риска выявленных уязвимостей снизился



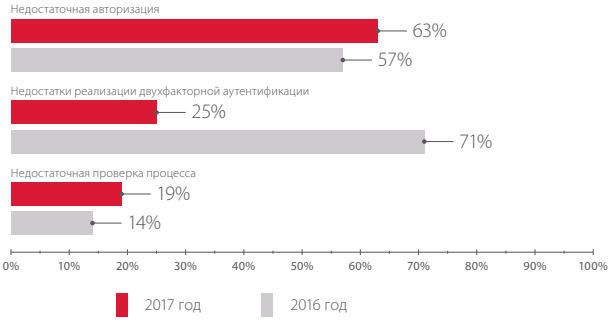
Доли уязвимостей различного уровня риска

В среднем онлайн-банки содержали больше уязвимостей, чем мобильные финансовые приложения

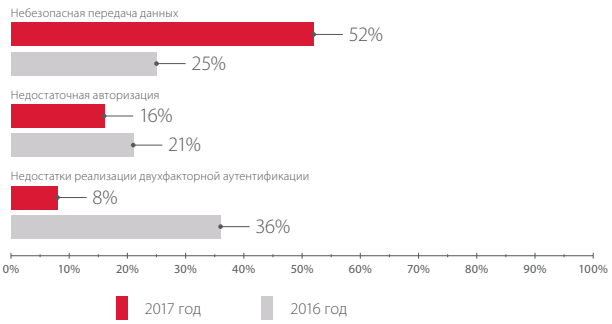


Среднее число уязвимостей различного уровня риска в одном финансовом приложении

Большинство уязвимостей были связаны с недостатками механизмов защиты — идентификации, аутентификации и авторизации



Критически опасные уязвимости онлайн-банков (доля приложений)



Критически опасные уязвимости мобильных банков (доля приложений)

1. ИСХОДНЫЕ ДАННЫЕ

Исходные данные были получены в ходе работ по анализу защищенности, проведенных специалистами компании Positive Technologies в 2017 году. Была рассмотрена 41 система, используемая для проведения финансовых операций.

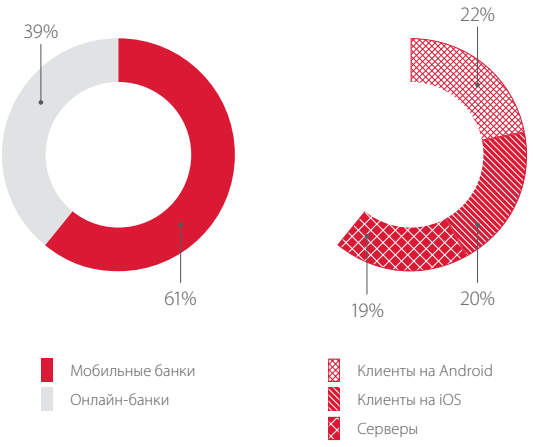
Большинство проанализированных систем ДБО (61%) составили мобильные приложения, среди которых примерно поровну распределились серверные части мобильных приложений и клиенты для мобильных операционных систем Android и iOS.

79% рассмотренных систем использовались для обслуживания физических лиц, 21% — для юридических.

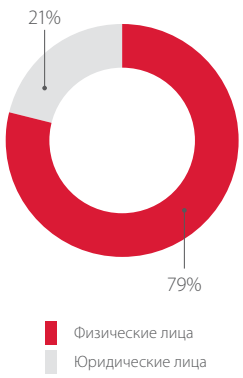
В 2017 году снизилась доля систем, разработанных банками самостоятельно (в 2016 году она составляла 78%, а в 2017 году 68%). Однако ДБО собственной разработки по-прежнему используются чаще систем, развернутых на базе платформ, разработанных известными вендорами. В соответствии с политикой ответственного разглашения информации об уязвимостях в настоящем отчете названия компаний-производителей не указываются.

Для создания систем ДБО собственными силами банки продолжают использовать преимущественно язык программирования Java (46%).

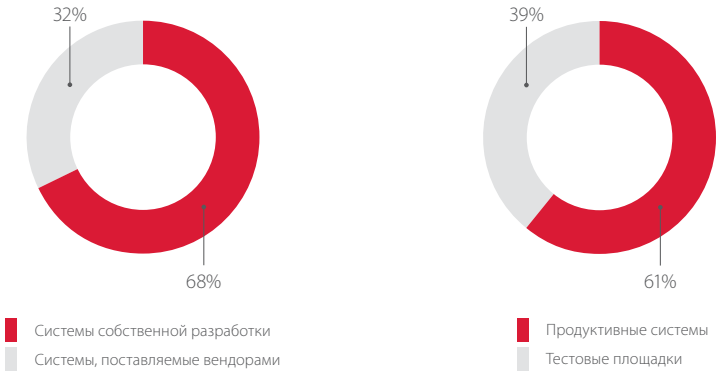
Большинство анализируемых систем представляли собой продуктивные системы, доступные для клиентов (61%); остальные 39% — тестовые стенды, готовые к переводу в промышленную эксплуатацию.



Типы систем ДБО



Сфера обслуживания систем ДБО



Типы систем ДБО по производителю

Соотношение продуктивных и тестовых систем ДБО

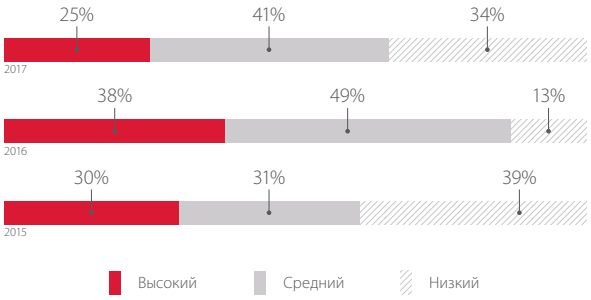
2. НЕДОСТАТКИ ЗАЩИТЫ ФИНАНСОВЫХ ПРИЛОЖЕНИЙ

2.1. Общая статистика

В каждом из рассмотренных приложений были выявлены недостатки безопасности

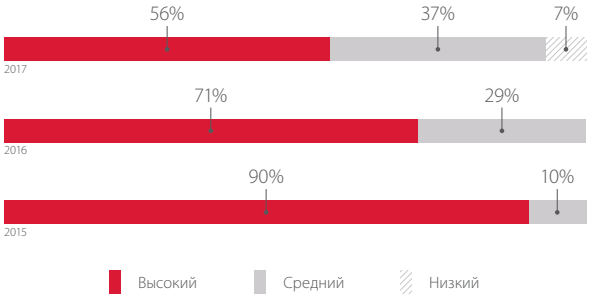
В среднем в 2017 году на каждую систему ДБО приходилось по 7 уязвимостей, что больше прошлогоднего показателя, когда на каждое финансовое приложение приходилось только 6 недостатков. Однако мы видим, что существенно изменилось распределение уязвимостей по уровню риска. А именно, снизились доли уязвимостей высокого (на 7%) и среднего уровня риска (на 8%). Кроме того, лишь в половине (56%) проанализированных систем ДБО присутствовали уязвимости высокого уровня риска. Этот показатель снижается из года в год (в 2015 году уязвимости высокого уровня риска содержались в 90% систем, а в 2016 году в 71%): компании принимают меры по защите приложений и в первую очередь стремятся закрыть критически опасные для системы уязвимости.

В 2017 году снизились доли уязвимостей высокого и среднего уровней риска

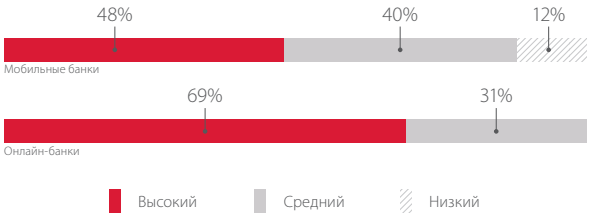


Уязвимости различного уровня риска

Уровень защищенности финансовых приложений медленно, но верно растет

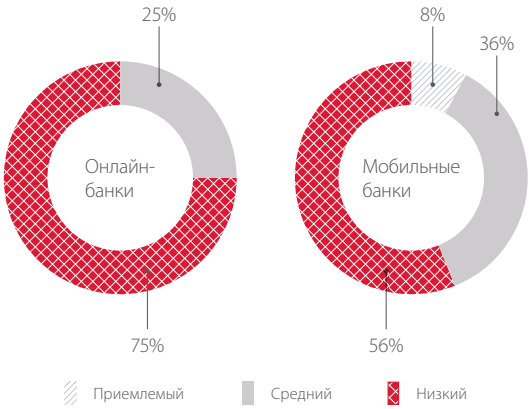


Доли финансовых приложений по максимальному уровню риска уязвимостей



Доли онлайн- и мобильных банков по максимальному уровню риска уязвимостей

Мобильные приложения стали безопасней. Уровень защищенности 8% таких систем был оценен как приемлемый. В 2016 году 93% мобильных банков имели низкий уровень защиты



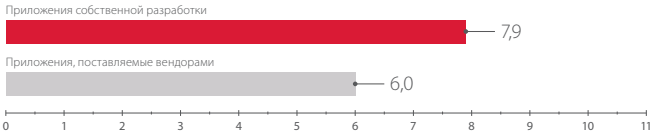
Доли приложений по уровню защищенности

2.2. Сравнение приложений собственной разработки и поставляемых вендорами

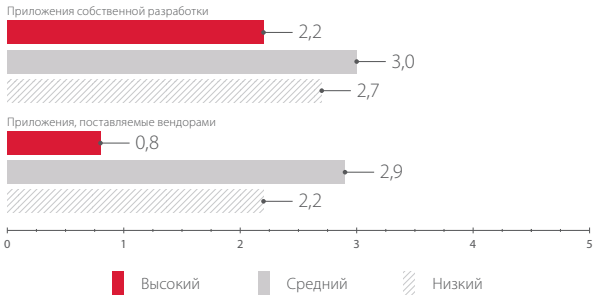
68% рассмотренных систем были разработаны финансовыми организациями самостоятельно

В предыдущие годы мы говорили о том, что системы собственной разработки банков лучше защищены. Действительно, в 2016 году приложения, разработанные банками, содержали в два раза меньше уязвимостей, чем системы, развернутые на готовых платформах. Но в 2017 году ситуация изменилась: количество уязвимостей в приложениях, поставляемых профессиональными вендорами, значительно снизилось, в то время, как выросло количество недостатков в системах ДБО, разработанных банками самостоятельно. Причем в финансовых приложениях, поставляемых вендорами, в среднем оказалось значительно меньше уязвимостей высокого уровня риска, чем в системах собственной разработки банков. Большинство недостатков систем ДБО собственной разработки банков были связаны с уязвимостями кода. Это говорит о том, что банкам, создавшим штат разработчиков, необходимо больше внимания уделить обучению программистов вопросам информационной безопасности и выстраиванию процесса безопасной разработки.

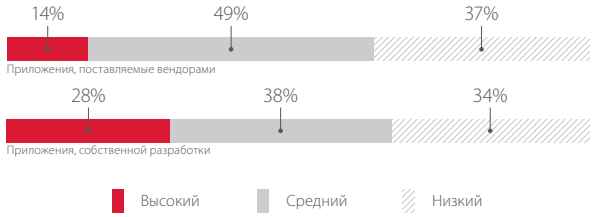
При проектировании типовой системы компания-вендор часто не учитывает нужды конкретного заказчика, что приводит к возникновению недостатков в механизмах защиты, например в аутентификации или авторизации. В таком случае вина ложится не на разработчиков, а на людей, проектировавших систему и разработавших требования для программистов.



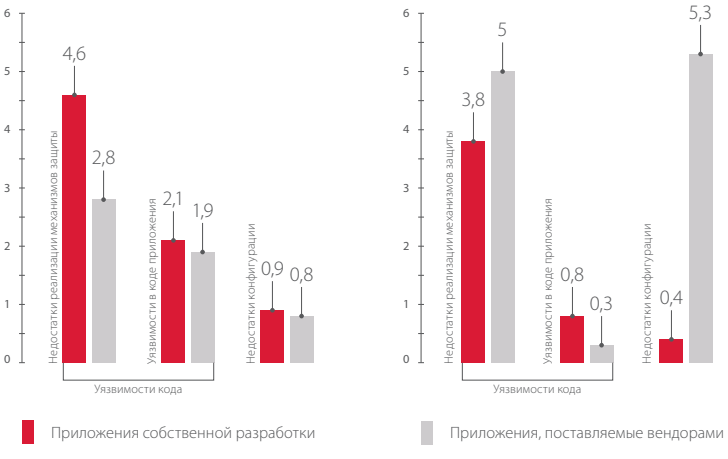
Среднее количество уязвимостей в одном приложении



Среднее количество уязвимостей разного уровня риска в одном приложении



Доли уязвимостей различного уровня риска



Среднее количество уязвимостей в одном приложении (2017)

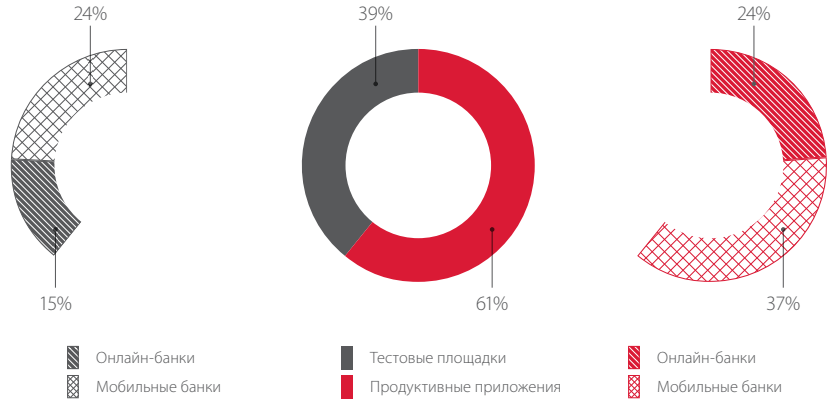
Среднее количество уязвимостей в одном приложении (2016)

2.3. Сравнение тестовых и продуктивных приложений

В 2017 году большинство проанализированных систем (61%) находились в промышленной эксплуатации и были доступны клиентам. Проведение анализа защищенности финансового приложения до ввода в эксплуатацию позволяет своевременно принять меры по его улучшению и предусмотреть все возможные угрозы безопасности без риска, что злоумышленник обнаружит эти недостатки раньше, чем будут приняты меры. (Ведь система еще не доступна клиентам.) Однако для

функционирующей системы ДБО не менее важно регулярно проводить анализ защищенности: в приложение могут внедряться новые функции, исправляться ошибки, что может привнести в систему новые уязвимости.

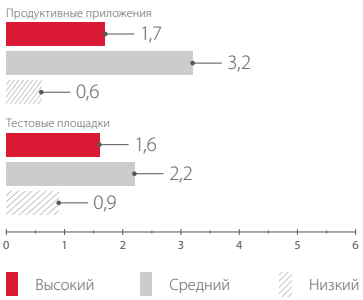
В продуктивных системах было выявлено **в два раза больше уязвимостей**, чем в тестовых



Доли тестовых и продуктивных финансовых приложений

Среднее количество уязвимостей в продуктивных приложениях, как и в предыдущие годы, превысило аналогичный показатель в тестовых системах. Наибольшее количество уязвимостей как в тестовых, так и продуктивных системах относились к уязвимостям кода. Количество этих уязвимостей, как правило, можно минимизировать, если при разработке системы придерживаться практик безопасного программирования SSDLC. А для своевременного выявления таких уязвимостей необходимо проводить регулярные проверки качества кода, например путем его анализа методом белого ящика (в том числе — с использованием автоматизированных средств).

Среднее число уязвимостей разных типов

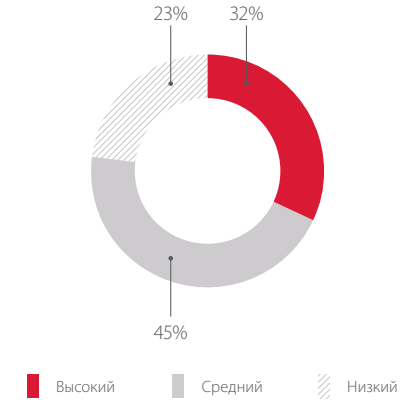


Среднее число уязвимостей разного уровня риска в тестовых и продуктивных системах

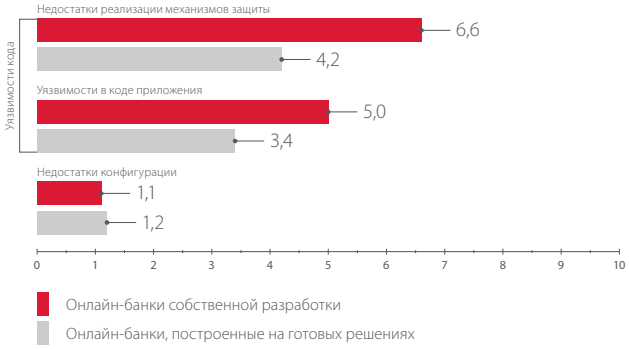
3. УЯЗВИМОСТИ И УГРОЗЫ ОНЛАЙН-БАНКОВ

В 2017 году мы наблюдали повышение уровня защищенности анализируемых систем ДБО — как онлайн-банков, так и мобильных приложений

Так, в 31% финансовых веб-приложений не было обнаружено ни одной критически опасной уязвимости, в то время как в 2016 году уязвимости высокого уровня риска присутствовали во всех онлайн-банках, кроме одного. В среднем на каждое веб-приложение пришлось по 1,3 уязвимости высокого уровня риска, что вновь лучше показателей прошлого года, когда на каждую подобную систему приходилось по 2,1 уязвимости (а в 2015 году было и вовсе по 4,2). Это объясняется тем, что некоторые банки уже ранее проводили анализ защищенности систем ДБО и устраняли выявленные уязвимости, а в 2017 году обратились к специалистам Positive Technologies повторно.



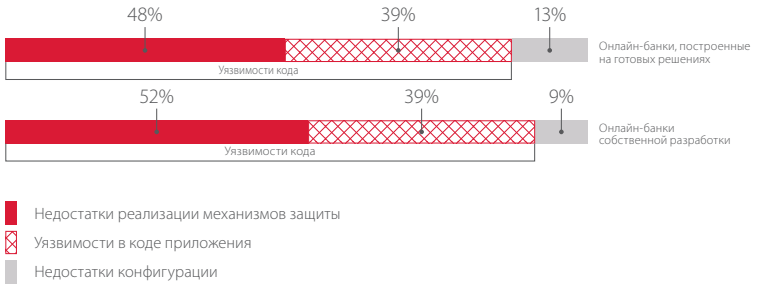
Доли уязвимостей онлайн-банков различного уровня риска



Среднее число уязвимостей разных типов в финансовых веб-приложениях

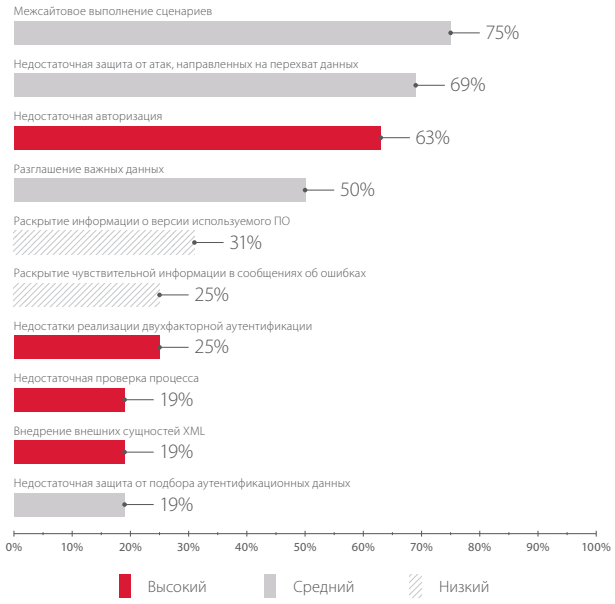
Распределение уязвимостей разных типов в онлайн-банках собственной разработки и веб-приложениях, построенных на готовых решениях, в 2017 году оказалось схожим. Веб-приложения собственной разработки содержали на 4% больше недостатков реализации механизмов защиты (таких как «Недостаточная авторизация», «Недостаточная аутентификация», «Недостатки парольной политики»), а онлайн-банки, построенные на готовых решениях, — на 4% больше недостатков конфигурации (например, «Небезопасная конфигурация заголовков HTTP-сервера»).

100% онлайн-банков имели недостатки реализации механизмов защиты



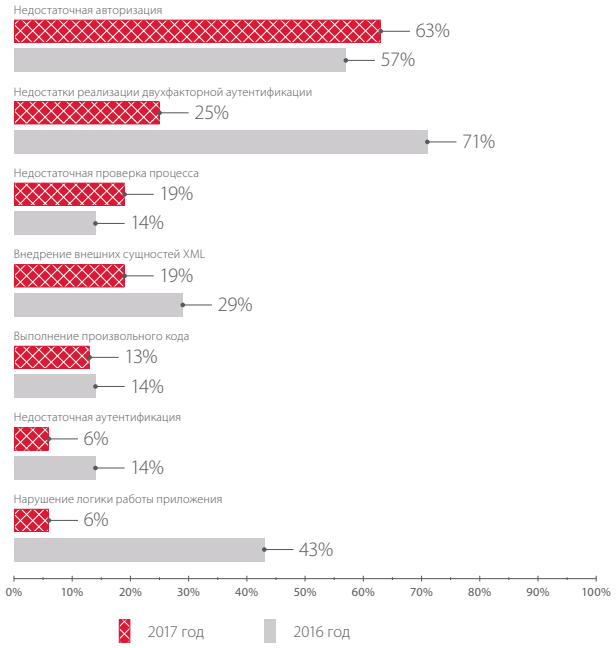
Доли уязвимостей разных типов

Перечень наиболее распространенных уязвимостей год от года меняется незначительно. Наиболее распространенными в 2017 году оказались уязвимости «Межсайтовое выполнение сценариев» и «Недостаточная защита от атак, направленных на перехват данных», которые позволяют совершать атаки на клиентов банков (например, перехватывать значения cookie или похищать учетные данные). Больше половины онлайн-банков (63%) содержали уязвимость высокого уровня риска «Недостаточная авторизация», которая позволяет злоумышленнику получить несанкционированный доступ к функциям веб-приложения, не предназначенным для данного уровня пользователя.



Самые распространенные уязвимости онлайн-банков (доля систем)

В 2017 году для всех финансовых приложений было отмечено снижение числа практически всех критически опасных уязвимостей. Наибольшее количество уязвимостей высокого уровня риска в онлайн-банках (63%) было связано с некорректной реализацией механизма авторизации. 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 получить доступ к панели управления веб-сервером и изменять системные параметры, а в другом — узнать остаток денежных средств на счетах других пользователей.



Критически опасные уязвимости (доля онлайн-банков)

Среди других критически опасных уязвимостей онлайн-банков стоит отметить значительное снижение доли недостатков реализации двухфакторной аутентификации. В 2017 году эта уязвимость встретилась в четверти онлайн-банков вместо 71%, которые были в 2016 году. В большинстве уязвимых систем отсутствовала защита от подбора одноразового пароля, а именно не ограничивалось количество попыток ввода или время жизни одноразового пароля. Отметим, что на черном рынке киберпреступники могут «оформить подписку» и получать детализацию входящих СМС для любого номера телефона, а значит — могут отслеживать одноразовые пароли для совершения операций в онлайн-банке. Банкам стоит задуматься о дополнительных мерах для защиты пользовательских транзакций.

Выявленные уязвимости в финансовых веб-приложениях могут обернуться значительными репутационными и финансовыми потерями для банков и их клиентов. Эксплуатация уязвимостей может привести к таким ощутимым последствиям, как, например, кража денежных средств в результате проведения мошеннических операций, — в половине веб-приложений. В 94% проанализированных веб-приложений злоумышленник мог получить доступ к личной информации клиентов, а иногда и сведениям, составляющим банковскую тайну, например к данным банковских карт, информации об остатках денежных средств на счетах, к графикам платежей по кредитам. В трети веб-приложений (31%) могло быть нарушено обслуживание отдельных учетных записей клиентов, а в 13% — работа самого онлайн-банка.

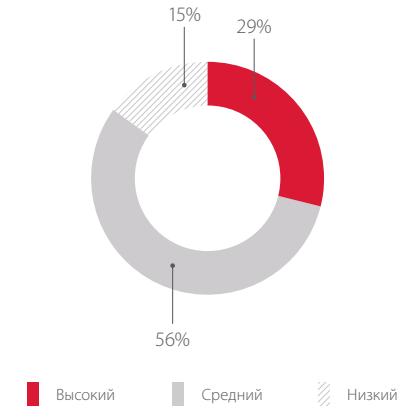
Возможные последствия атак на онлайн-банки (доля уязвимых приложений)

4. УЯЗВИМОСТИ И УГРОЗЫ МОБИЛЬНЫХ БАНКОВ

В 8% мобильных банков общий уровень защищенности был оценен как «приемлемый», поскольку в этих приложениях отсутствовали серьезные уязвимости

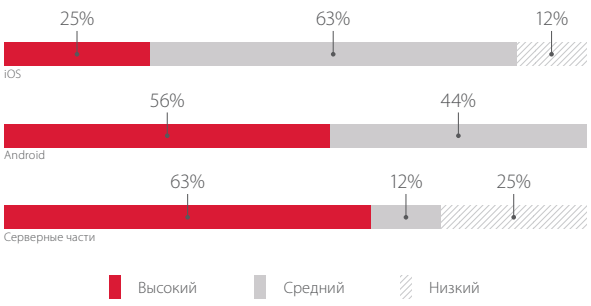
В 48% мобильных банков была выявлена хотя бы одна критически опасная уязвимость. В среднем на каждое мобильное приложение пришлось по 0,64 уязвимости высокого уровня риска, что ниже аналогичного показателя по проанализированным онлайн-банкам.

В сравнении с показателями 2016 года снизились и доли уязвимостей высокого (29% вместо 32% в 2016 году) и среднего уровня риска (56% вместо 60%). Соответственно, увеличилась доля уязвимостей низкого уровня риска; компании стремятся в первую очередь принимать меры для устранения критически опасных уязвимостей.



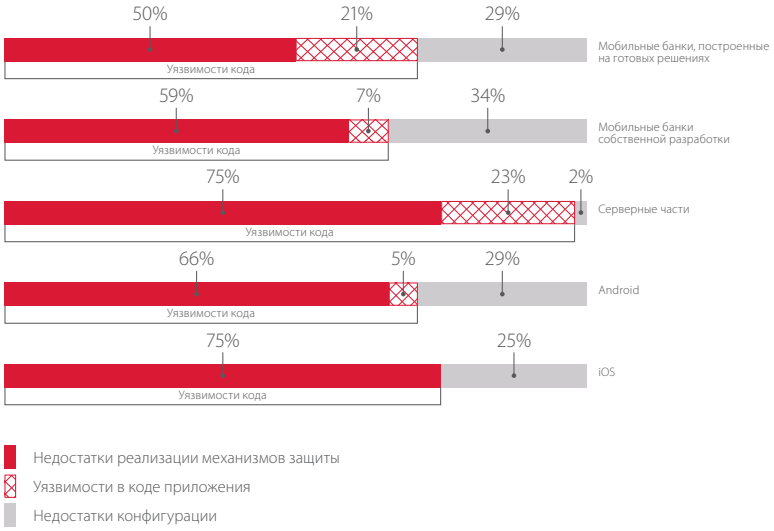
Доли уязвимостей мобильных банков различного уровня риска

Уровень защищенности iOS- приложений вновь оказался выше, чем у Android

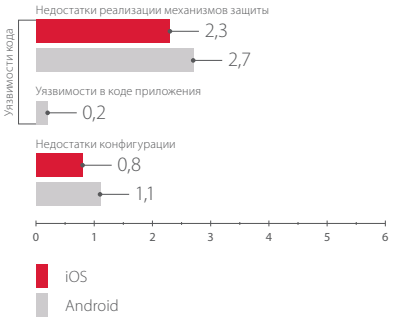


Доли мобильных банков по максимальному уровню риска уязвимостей

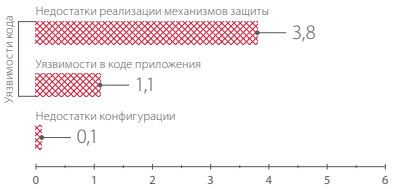
Практически для всех рассмотренных мобильных банков (кроме одного) мы анализировали по два идентичных приложения, разработанных для разных операционных систем, Android и iOS. В некоторых случаях мобильное приложение для iOS не содержало уязвимостей, которые были обнаружены в Android-приложении.



Доли уязвимостей разных типов



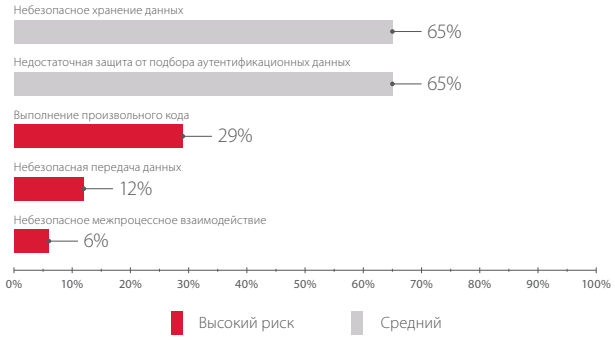
Среднее число уязвимостей в клиентских частях мобильных банков



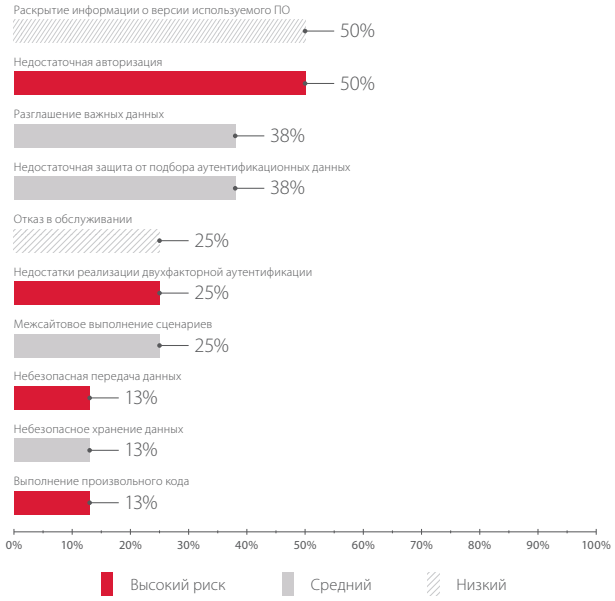
Среднее число уязвимостей в серверных частях мобильных банков

Наибольшее число уязвимостей в мобильных приложениях было связано с недостатками механизмов защиты. Как уже отмечалось, подобные уязвимости относятся к уязвимостям кода, однако мы их рассматриваем отдельно, поскольку возникают они в приложении в другое время. Недостатки механизмов защиты появляются в системе еще на этапе проектирования, в то время как все прочие уязвимости кода возникают уже непосредственно во время разработки.

Примечательно, что в 2017 году уязвимости клиентских частей мобильных приложений не отличались разнообразием, и поэтому мы выделили только пять самых популярных недостатков. Более половины клиентских приложений (65%) содержали уязвимости «Небезопасное хранение данных» или «Недостаточная защита от подбора аутентификационных данных». Эти недостатки могут быть использованы злоумышленниками для получения несанкционированного доступа к учетным данным пользователя и, как следствие, доступа к мобильному банку от лица этого пользователя. Отметим также, что уязвимости, связанные с небезопасным хранением и (или) передачей данных, можно оценить как высоким, так и средним уровнем риска — в зависимости от угрозы, реализуемой в конкретном проекте.



Топ-5 уязвимостей клиентских частей мобильных банков



Топ-10 уязвимостей серверных частей мобильных банков

Для серверных частей мобильных приложений по-прежнему остро стоит проблема недостаточной авторизации. Однако доля уязвимых мобильных банков снизилась с 75%, которые были в 2016 году, до 50%.

Так, например, довольно популярной практикой является создание пользователем короткого ПИН-кода для быстрого доступа к финансовому приложению с мобильного устройства. Однако в случае отсутствия привязки ПИН-кода к устройству злоумышленник может получить несанкционированный доступ к мобильному банку. В одном из проанализированных мобильных приложений значение, передаваемое в паре с ПИН-кодом для упрощенной аутентификации, хранилось на устройстве в открытом виде и было неизменно для учетной записи пользователя. В случае утечки данного значения злоумышленник мог подобрать ПИН-код и получить доступ к личному кабинету жертвы со своего мобильного телефона.

Недостатки реализации двухфакторной аутентификации в 2017 году также встречались реже — в четверти серверных частей мобильных приложений (вместо каждой второй в 2016-м).

В 13% мобильных приложений встретилась уязвимость «Выполнение произвольного кода». Эта уязвимость была характерна для серверных частей приложений. **Ее эксплуатация позволяет злоумышленнику получить полный контроль над сервером,** выполнять произвольный код в системе, читать, удалять или изменять файлы на сервере, проводить атаки с целью повышения привилегий в ОС или отказа в обслуживании сервера. Подобные действия нарушителя могут привести к существенным репутационным и финансовым потерям банка.

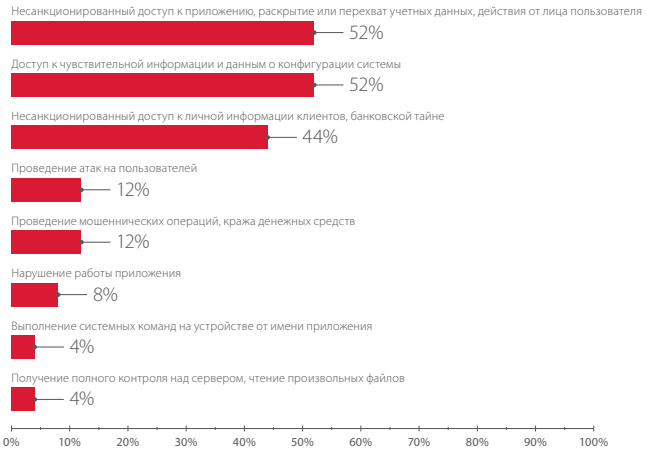
В половине мобильных банков (52%) выявленные уязвимости позволяли злоумышленникам расшифровать, перехватить, подобрать учетные данные для доступа в мобильное приложение или же и вовсе обойти процесс аутентификации, в результате чего получить доступ к мобильному банку от лица легитимного пользователя и возможность совершать различные операции.

Были выявлены сценарии, когда злоумышленник, обладающий физическим доступом к устройству пользователя с root-доступом или включенным режимом отладки, может получить доступ к исходящим сообщениям, идентификатору и паролю пользователя и контроль над мобильным банком.

В 44% проанализированных мобильных банков выявленные недостатки позволяли киберпреступникам получить доступ к банковской информации клиентов. Так, в одном из мобильных приложений вследствие недостатков авторизации на сервере злоумышленник мог получить доступ к таким данным пользователя, как имя, фамилия, денежный баланс, информация по вкладам, кредитам. Это не только может привести к репутационным потерям банка, подобная информация может быть использована в дальнейшем для атаки на клиентов.

Реализация атак на мобильные банки в 2017 году могла нанести серьезный ущерб как самим банкам, так и их клиентам, поскольку большинство этих атак связаны:

+ с выполнением действий от лица легитимного пользователя,
+ доступом к банковским сведениям клиентов,
+ проведением мошеннических операций.



Возможные последствия атак на мобильные банки (доля уязвимых приложений)

ВЫВОДЫ

2017 год подарил надежду, что финансовые приложения когда-нибудь станут безопасными. Мы наблюдали существенное повышение уровня защищенности анализируемых систем ДБО — как онлайн-банков, так и мобильных приложений. Однако текущие недостатки все равно несут серьезные угрозы для банков и их клиентов. Клиенты в первую очередь рискуют своими личными данными и банковской информацией, а банки — денежными средствами.

Как показывают многолетние исследования, главные проблемы в защите онлайн-банков и мобильных банков связаны с уязвимостями кода приложений. Для того чтобы избежать большинства уязвимостей, банкам следует уделять больше внимания вопросам безопасности как на этапе проектирования приложений и разработки технических заданий для программистов, так и на стадии разработки. Необходимо своевременно учесть все нюансы, связанные с реализацией механизмов защиты, придерживаться практик безопасного программирования SSDLC и, конечно, уделять пристальное внимание тестированию самих приложений и их механизмов защиты.

Сегодня практически все банки регулярно (не реже одного раза в год) проводят анализ защищенности приложений. Но не стоит забывать и про анализ исходного кода, особенно если приложение построено на базе готового вендорского решения: в нем могут не учитываться отдельные особенности системы и из-за этого возникать уязвимости. Также стоит отметить, что существенную роль в обеспечении безопасности банковских систем играет не столько выявление уязвимостей, сколько принятие своевременных мер по их нейтрализации. Поэтому после устранения всех выявленных уязвимостей рекомендуется проводить проверку эффективности принятых мер. Исправление уязвимостей может занять продолжительное время и для того, чтобы защититься от кибератак в адрес онлайн-банков и серверных частей мобильных банков, пока разработчики вносят изменения в финансовые приложения, рекомендуется использовать систему превентивного контроля (web application firewall).

О компании

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.

POSITIVE TECHNOLOGIES

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