

POSITIVE TECHNOLOGIES

Уязвимости онлайн-банков

2019



Содержание

Введение.....	2
Резюме.....	2
Тенденции.....	2
Общая статистика.....	3
Сравнение приложений собственной разработки и поставляемых вендорами.....	6
Сравнение продуктивных и тестовых приложений.....	8
Выводы	10



Введение

Данный аналитический отчет основан на статистике, полученной экспертами Positive Technologies в 2018 году в ходе работ по анализу защищенности веб-приложений для дистанционного банковского обслуживания (онлайн-банков). Исследование направлено на демонстрацию наиболее распространенных проблем безопасности онлайн-банков и сравнение уровня защищенности таких систем с уровнем 2017 года.

Сделанные выводы могут не отражать актуальное состояние защищенности информационных систем в других организациях. Анализ проведен с целью обратить внимание специалистов по ИБ в финансовой отрасли на наиболее актуальные проблемы и помочь им своевременно выявить и устранить уязвимости.

Резюме

Большинство онлайн-банков содержат критически опасные уязвимости. Как следствие, низкий или крайне низкий уровень защищенности имеют 61% исследованных онлайн-банков.

Все онлайн-банки под угрозой. В каждом исследованном онлайн-банке обнаружены уязвимости, которые могут привести к серьезным последствиям. Например, в 54% приложений возможны проведение мошеннических операций и кража денежных средств.

Механизмы двухфакторной аутентификации недостаточно надежны. Недостатки реализации таких механизмов обнаружены в 77% онлайн-банков.

Покупные решения менее уязвимы. В среднем решения, предлагаемые вендорами, содержат в 3 раза меньше уязвимостей, чем системы, разработанные банками самостоятельно.

Продуктивные системы так же уязвимы, как и тестовые. Оба типа систем в большинстве случаев содержат как минимум одну критически опасную уязвимость.

Тенденции

Уверенное сокращение доли уязвимостей высокого уровня риска. В 2016 году для онлайн-банков этот показатель достигал 36%, в 2017 он снизился до 32%. В 2018 году доля критически опасных уязвимостей составляет лишь 15%.

Теряет свою актуальность критически опасная уязвимость «Недостаточная аутентификация». Доля онлайн-банков, в которых можно совершать важные действия без ввода учетных данных, уменьшалась с каждым годом, и в 2018 году мы наконец не зафиксировали ни одного приложения, где оставалась бы данная проблема. Однако по-прежнему во многих системах операции повышенной важности совершаются без дополнительного (второго) фактора аутентификации.

Личная информация клиентов и банковская тайна под угрозой в каждом исследованном онлайн-банке. Из года в год мы наблюдаем рост доли систем, в которых есть риск несанкционированного доступа к личным данным клиентов и банковской тайне. В 2018 году этот показатель достиг предельного значения: все исследованные онлайн-банки оказались подвержены указанной угрозе.



Общая статистика



В каждом онлайн-банке есть угроза несанкционированного доступа к личной информации клиентов и банковской тайне, а в 54% онлайн-банков возможны мошеннические операции и кража денежных средств



Корректно реализуйте протокол OAuth2. Придерживайтесь общих рекомендаций по безопасности RFC 6749. Для защиты от подмены значения redirect_uri используйте белые списки

Несанкционированный доступ к личной информации клиентов, а в некоторых случаях — и к банковской тайне, например к выпискам по счету или платежным поручениям других пользователей, — может быть получен в результате эксплуатации множества различных уязвимостей. Каждый исследованный в 2018 году онлайн-банк содержал хотя бы одну уязвимость, приводящую к таким последствиям. В частности, угроза актуальна для приложений, в которых существуют недостатки механизмов аутентификации и авторизации. Например, разработчики онлайн-банков нередко допускают ошибки при реализации технологии единого входа (single sign-on, SSO) на базе протокола OAuth2, что может привести к передаче учетных данных по незащищенному протоколу и перехвату сессии злоумышленником.

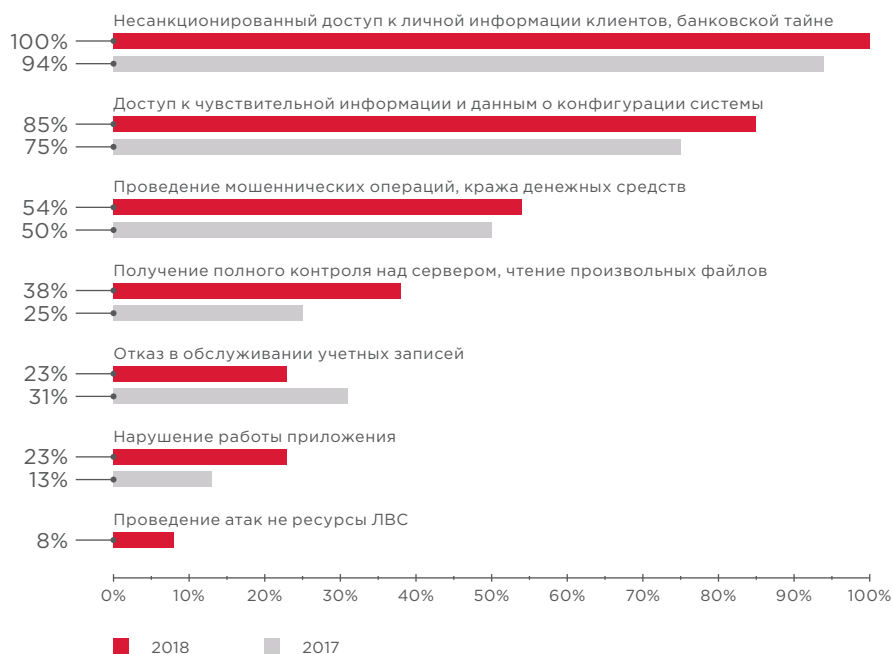


Рисунок 1. Возможные последствия атак на онлайн-банки (доля приложений)



Введите минимально допустимую сумму денежных средств при конвертации валюты. Тщательно проверяйте формулу расчета итоговой суммы

Мошеннические операции и кража денежных средств чаще всего возможны из-за ошибок в логике работы онлайн-банка. Например, многократное повторение так называемых атак на округление суммы денежных средств при конвертации валюты может привести к ощутимым для банка финансовым потерям. Уязвимость широко известна и существует из-за погрешности в округлении при конвертации из одной валюты в другую и обратно.



Не используйте сериализованные объекты при передаче в параметрах, которые могут быть легко подделаны злоумышленником, либо используйте цифровую подпись таких объектов с проверкой на серверной стороне

Наряду с критически опасными уязвимостями (например, такими как «Выполнение произвольного кода» или «Десериализация недоверенных данных») наши специалисты в некоторых случаях выявляли на сервере онлайн-банка интерфейс с адресом внутренней сети банка; зная этот адрес, злоумышленник может развивать атаки на корпоративную инфраструктуру.



61% онлайн-банков
имеет низкий или крайне низкий
уровень защищенности

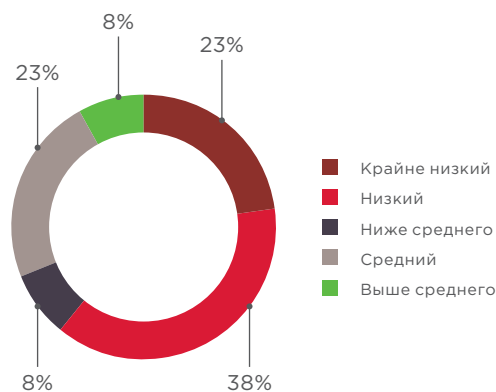
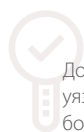


Рисунок 2. Уровень защищенности онлайн-банков (доля систем)



Доля критически опасных
уязвимостей сократилась
более чем в два раза
по сравнению с 2017 годом

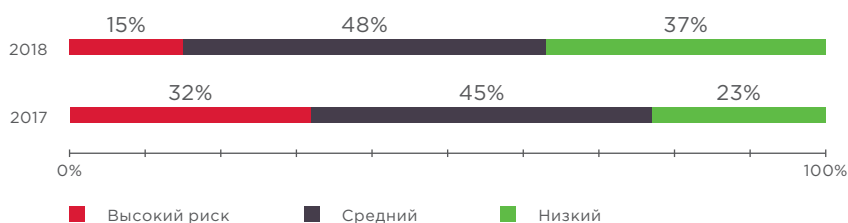


Рисунок 3. Доли уязвимостей различного уровня риска



Среднее число уязвимостей
в одном онлайн-банке
выросло почти в два раза
по сравнению с 2017 годом, однако
среднее число критически опасных
уязвимостей в одной системе
практически не изменилось

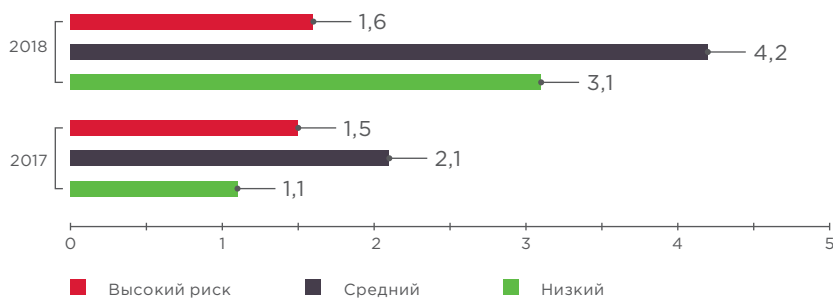


Рисунок 4. Среднее число уязвимостей в одном онлайн-банке



Используйте механизм OTP
для всех критически важных дей-
ствий в системе. Одноразовые
пароли должны иметь ограни-
ченный срок жизни (не более
2 минут) и быть привязаны к вы-
полняемой операции с помощью
дополнительного случайного
параметра, соответствующего
идентификатору операции

Остановимся подробно на некоторых уязвимостях, которые были обнаружены нашими экспертами. В 2018 году ни в одном исследованном онлайн-банке не была выявлена уязвимость «Недостаточная аутентификация», а «Недостаточная авторизация» встречалась гораздо реже, чем годом ранее. На первое место вышли ошибки в реализации механизмов двухфакторной аутентификации. Например, в некоторых онлайн-банках не применяются одноразовые пароли (one-time password, OTP) для критически важных действий (аутентификация, смена учетных данных и др.) или пароли имеют слишком большой срок действия. На наш взгляд, это связано с тем, что банки стремятся найти баланс между безопасностью и удобством использования, ведь необходимость много раз вводить одноразовые пароли в течение одного сеанса работы может вызывать недовольство у пользователей. Например, благодаря удобству применения и возможности сэкономить на SMS-сообщениях для OTP в системах ДБО сегодня часто используют механизмы адаптивной аутентификации, в частности риск-ориентированную модель аутентификации (risk-based authentication). В то же время отказ даже от части мер безопасности в пользу удобства повышает риск совершения мошеннических операций. Так, если нет необходимости подтверждать операцию с помощью одноразового пароля, злоумышленнику больше не требуется доступ к мобильному телефону жертвы, а слишком большой срок действия пароля повышает шанс его успешного подбора.



В 2018 году до 31% выросла (с 6% в 2017 году) доля атак, в результате которых злоумышленник может повлиять на бизнес-логику системы. Вероятно, это связано с ростом числа уязвимостей в коде приложений, разработанных банками самостоятельно. Как будет показано далее (рис. 11), в 2018 году доля таких уязвимостей достигла 59%, в то время как в прошлом году она составляла 39%.

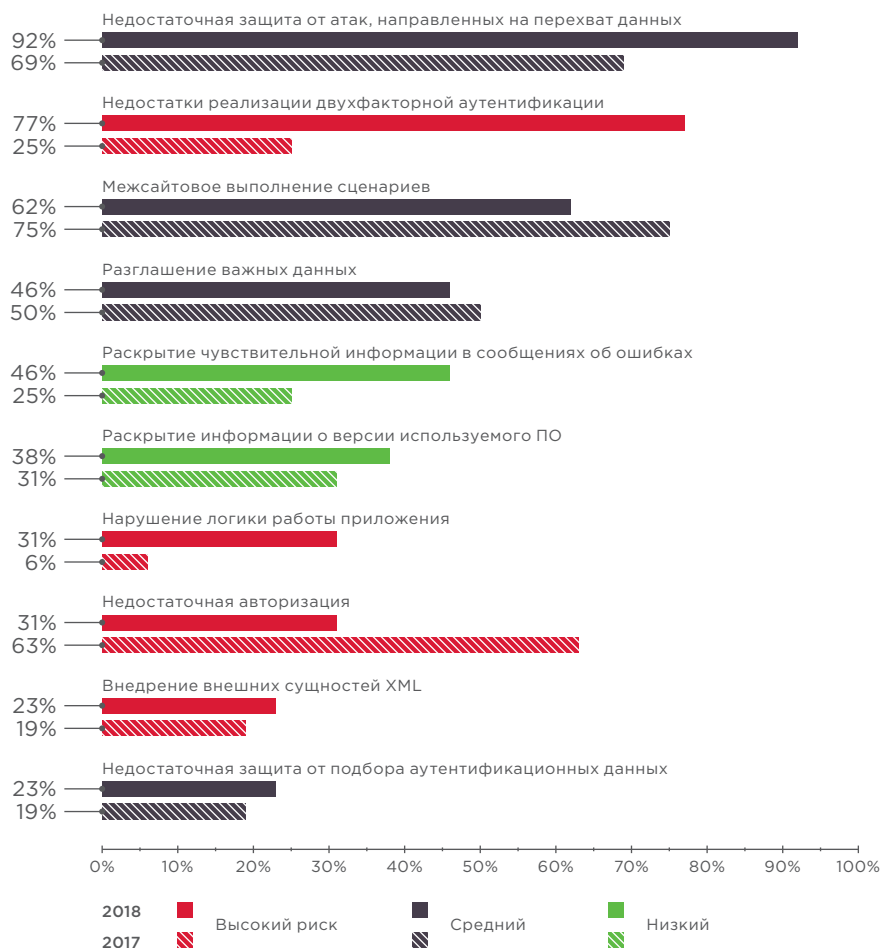


Рисунок 5. Самые распространенные уязвимости онлайн-банков (доля систем)



Если в приложении не используется механизм HSTS, а параметры cookie не защищены флагами Secure и SameSite, злоумышленник может перехватить идентификатор сессии пользователя и получить доступ к его личному кабинету и банковской тайне



Флаг Secure определяет необходимость передачи cookie только по защищенному протоколу HTTPS. Отсутствие флага создает угрозу перехвата cookie. Устранить проблему можно установив значение true для свойства requireSSL. Использование атрибута SameSite в режиме Strict не позволит передавать cookie на сторонние ресурсы и обеспечит защиту от атак типа «Подделка межсайтового запроса»

Для защиты от перехвата чувствительных данных и атак на пользователей современные браузеры поддерживают ряд механизмов, в частности:

- HTTP Strict Transport Security (HSTS) — механизм принудительного соединения посредством защищенного протокола HTTPS. За активацию механизма отвечает заголовок Strict-Transport-Security в HTTP-ответе сервера;
- HTTP Public Key Pinning (HPKP) — технология привязки публичного ключа, запрещающая подключаться к веб-серверу, если злоумышленник подменил SSL-сертификат. За активацию механизма отвечает заголовок Public-Key-Pins;
- Content Security Policy, CSP — механизм обеспечения безопасности, направленный на защиту от атак с внедрением контента, например от «Межсайтового выполнения сценариев». Механизм активируется заголовком Content-Security-Policy;
- X-Content-Type-Options — заголовок, предназначенный для защиты браузера пользователя от атак с использованием подмены типа передаваемого контента MIME;
- X-Frame-Options — заголовок, который позволяет защититься от атак типа «Кликджекинг» (Clickjacking).



Передавайте заголовки Public-Key-Pins и Strict-Transport-Security. Запрещайте пользователям онлайн-банков использовать устаревшие версии браузеров, а также браузеры, в которых есть возможность продолжить работу в случае подделки сертификата

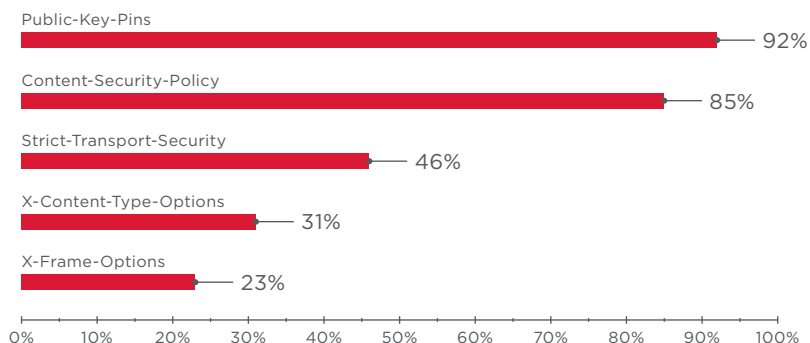


Рисунок 6. Доля приложений, в которых не установлены соответствующие заголовки сервера

Сравнение приложений собственной разработки и поставляемых вендорами

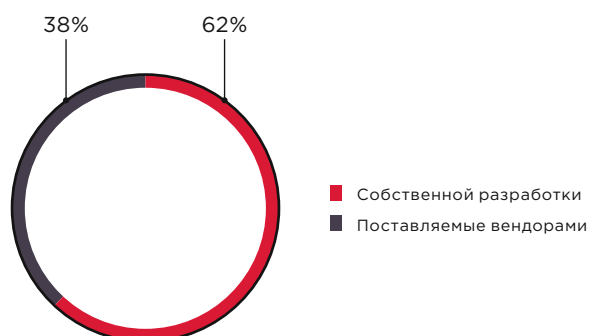


Рисунок 7. Типы онлайн-банков



Системы ДБО, разработанные банками самостоятельно, более уязвимы, чем готовые решения



Среднее число уязвимостей в приложениях собственной разработки в 3 раза больше, чем в системах, предлагаемых вендорами

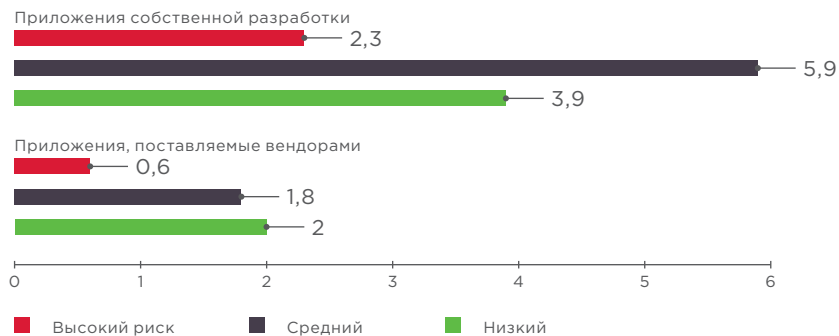


Рисунок 8. Среднее количество уязвимостей в одном приложении

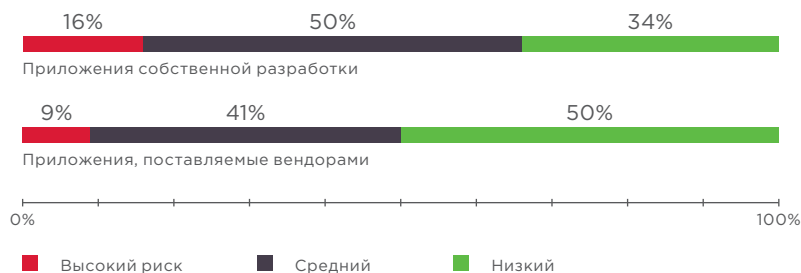


Рисунок 9. Доли уязвимостей различного уровня риска

Все выявленные уязвимости мы разделили на три группы:

- уязвимости в коде веб-приложения (ошибки, которые допустил программист при разработке);
- ошибки реализации механизмов защиты (в отличие от уязвимостей в коде — появляются в системе еще на этапе проектирования);
- недостатки конфигурации.

К первой группе относятся, например, «Межсайтовое выполнение сценариев» и «Внедрение SQL-кода». «Недостаточная защита от подбора учетных данных», «Недостаточная авторизация» — это примеры уязвимостей в механизмах защиты. К числу наиболее распространенных уязвимостей конфигурации относятся раскрытие чувствительных данных в сообщениях об ошибках и версий используемого ПО в заголовках ответов веб-сервера.

Большинство уязвимостей — как в готовых решениях, так и в собственных разработках банков — относятся к уязвимостям кода веб-приложений, но если вендоры чаще допускают ошибки на этапе проектирования, то в собственных решениях банков уязвимости закладываются непосредственно на этапе написания кода.



Подавляющее большинство уязвимостей как у вендоров, так и в собственных разработках относятся к уязвимостям кода

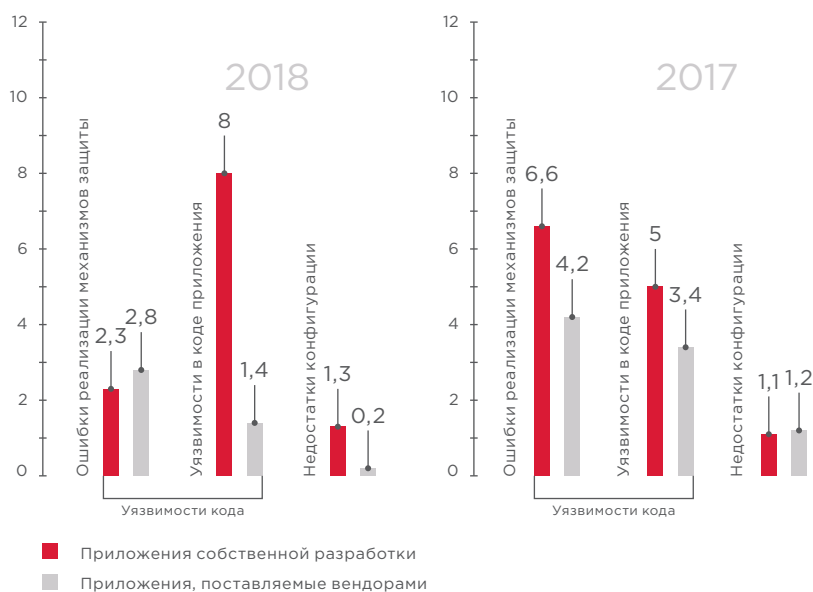


Рисунок 10. Среднее число уязвимостей в одном приложении



Компании — разработчики систем ДБО сосредоточены на реализации функциональных возможностей больше, чем на безопасности. Как следствие, 75% уязвимостей в покупных решениях связаны с недостатками механизмов защиты

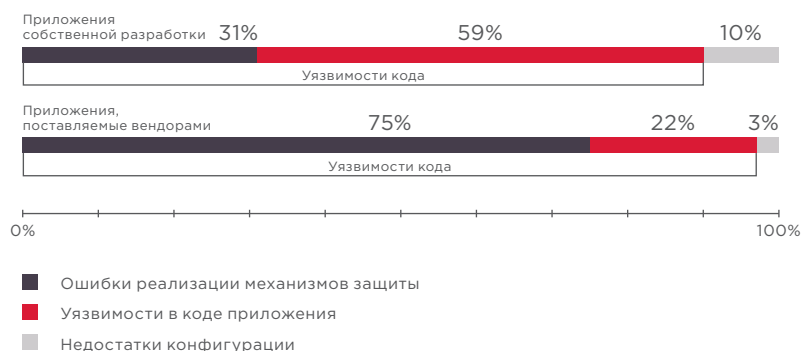


Рисунок 11. Доли уязвимостей разных типов

Сравнение продуктивных и тестовых приложений

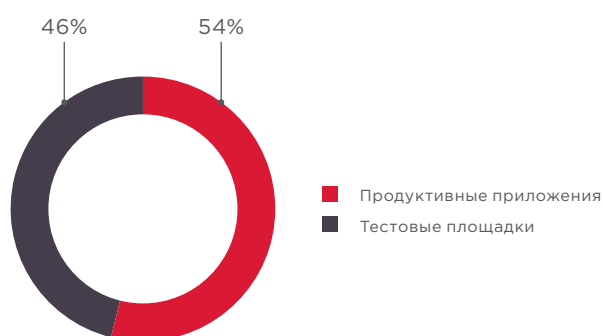


Рисунок 12. Доли продуктивных и тестовых систем



В одной продуктивной системе содержится примерно столько же критически опасных уязвимостей, сколько в одной тестовой



Проводите регулярный анализ защищенности веб-приложений для ДБО на каждом этапе развития продукта. Не стоит забывать, что доступ к исходному коду (тестирование методом белого ящика) повышает эффективность анализа

После тестирования защищенности приложения и устранения всех выявленных уязвимостей проходит время, и возникает необходимость модифицировать или оптимизировать веб-приложение, добавить новые функции. Небольшие изменения в коде, казалось бы, не могут кардинальным образом повлиять на безопасность, поэтому проверки сводятся к функциональному тестированию новых возможностей, а повторный анализ защищенности при этом не проводится. Со временем в продуктивной системе неминуемо появляется значительное число уязвимостей, подчас сопоставимое с тем, которое было обнаружено при первичном тестировании защищенности.

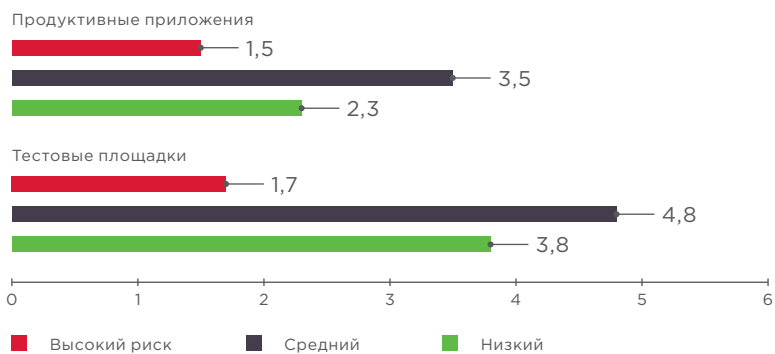


Рисунок 13. Среднее количество уязвимостей в одном приложении

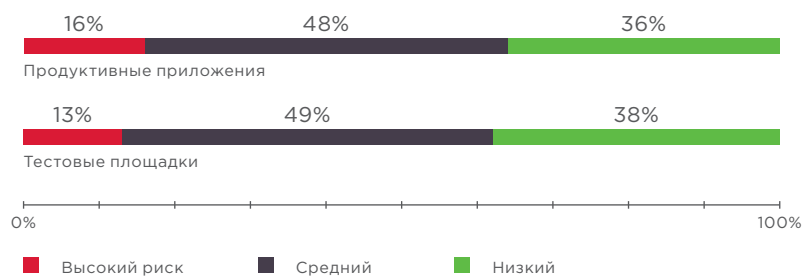


Рисунок 14. Доли уязвимостей различного уровня риска

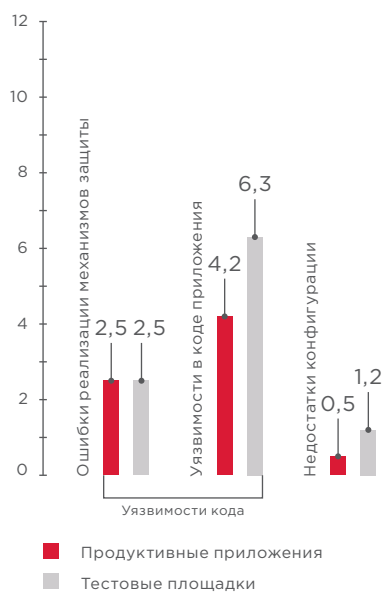


Рисунок 15. Среднее число уязвимостей в одном приложении



Выводы

Главной позитивной тенденцией в безопасности финансовых приложений в 2018 году стало сокращение доли уязвимостей высокого уровня риска. Однако уровень защищенности онлайн-банков остается низким.

Без сомнения, одно из серьезнейших последствий атаки на онлайн-банк — кража денежных средств. В 2018 году такая угроза отмечалась в 54% онлайн-банков. Угроза несанкционированного доступа к информации клиентов и банковской тайне оказалась актуальной для каждого исследованного онлайн-банка, а в отдельных случаях уязвимости позволяли развивать атаку до проникновения в корпоративную инфраструктуру.

Покупные решения для онлайн-банкинга в целом имеют более высокий уровень защищенности, чем приложения, разработанные банками самостоятельно, однако компании-разработчики чаще допускают ошибки в механизмах защиты, сосредоточиваясь на функциональных возможностях своих продуктов.

Изменения, которые вносятся в код, при отсутствии повторной проверки на наличие уязвимостей приводят к тому, что продуктивные системы не менее уязвимы, чем тестовые. Это говорит о необходимости выстраивать процессы безопасности на каждом этапе жизненного цикла онлайн-банка. Методика разработки безопасного программного обеспечения (SSDLC) позволяет избежать множества ошибок, но не исключает необходимости систематически проводить анализ защищенности веб-приложений. Наиболее эффективным методом проверки является метод белого ящика, подразумевающий анализ исходного кода. В качестве превентивной меры рекомендуется использовать межсетевой экран уровня приложений (web application firewall) для предотвращения эксплуатации уязвимостей, возникающих при внесении изменений в программный код.

О компании

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

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

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