СТАТИСТИКА УЯЗВИМОСТЕЙ СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ 2013–2014

POSITIVE TECHNOLOGIES
2015

Оглавление

Введение

В настоящем обзоре представлены обобщенные выводы об уязвимостях систем дистанционного банковского обслуживания (ДБО), обнаруженных в 2013 и 2014 годах при проведении экспертами Positive Technologies работ по анализу защищенности для ряда крупнейших российских банков.

По результатам проведенного исследования можно сделать следующие основные выводы.

Половина систем ДБО имеет низкий уровень защищенности

Среди всех обнаруженных уязвимостей ДБО 44% составили уязвимости высокого уровня риска, 26% — среднего уровня и 30% — низкого.

В 46% систем возможно несанкционированное проведение транзакций на уровне пользователей, при этом в 17% систем кража денежных средств возможна со стороны внешнего злоумышленника, а в 29% случаев — со стороны любого авторизованного пользователя. Кроме того, в 43% случаев возможно получение несанкционированного доступа к СУБД или ОС уязвимых систем. Возможность кражи информации, составляющей банковскую тайну, была выявлена в 89% систем ДБО.

Наиболее распространены уязвимости среднего и низкого уровней риска

Наиболее распространенные уязвимости имеют низкий уровень риска: возможность идентификации используемого программного обеспечения и предсказуемый формат идентификаторов пользователей (каждому из этих недостатков подвержены 57% рассмотренных систем). Вторые по распространенности уязвимости (54%) связаны с возможностью проведения атак на пользователей и имеют средний уровень риска: это недостаточная защита сессий и межсайтовое выполнение сценариев. Тем не менее, как и в 2011—2012 гг., для несанкционированного проведения транзакций на уровне пользователей злоумышленнику зачастую достаточно воспользоваться несколькими уязвимостями среднего и низкого уровней риска. Таким образом, **отсутствие уязвимостей высокой степени риска не означает, что система хорошо защищена.**

Уязвимости высокой степени риска преобладают как в системах ДБО, предлагаемых известными вендорами, так и в системах собственной разработки

Для систем, предоставленных вендорами, каждая вторая уязвимость (49%) имеет высокую степень риска. Для систем собственной разработки доля систем, содержащих уязвимости высокого уровня риска, также значительна и составляет 40%. Кроме того, системы ДБО, поставляемые профессиональными разработчиками, в среднем содержат в 2,5 раза больше уязвимостей на уровне кода приложения, чем системы собственной разработки. Данный факт можно объяснить тем, что при использовании системы, предоставляемой вендором, банк в основном полагается на поставщика продукта в вопросах контроля качества кода. Тем временем сложная архитектура, кроссплатформенность и большое количество функций подобных систем не всегда позволяют вендору обеспечить должный уровень защищенности на уровне кода приложения.

Продуктивные системы более уязвимы, чем тестовые

Согласно проведенному исследованию, в среднем **на одну продуктивную систему приходится почти в два раза больше уязвимостей** всех уровней риска по сравнению с тестовыми системами, находящимися на стадии приемки и ввода в эксплуатацию. В продуктивных системах выявлено больше уязвимостей как в части некорректной конфигурации, так и в части реализации механизмов защиты и на уровне кода приложения. Такие результаты подчеркивают не только необходимость анализа защищенности системы ДБО перед вводом в эксплуатацию, но и необходимость регулярного тестирования в процессе эксплуатации.

Все исследованные системы ДБО имели те или иные недостатки в реализации механизмов защиты

76% систем ДБО содержали как минимум один из двух недостатков механизма идентификации пользователей — предсказуемый формат идентификаторов или раскрытие информации о существующих в системе идентификаторах. Кроме того, 58% рассмотренных систем имели недостатки реализации механизма аутентификации: слабую парольную политику, недостаточную

защиту от подбора учетных данных, возможность обхода механизма CAPTCHA или отсутствие обязательной двухфакторной аутентификации при входе в личный кабинет. **79% систем содержали различные недостатки механизма авторизации,** при этом в 42% случаев злоумышленник мог получить несанкционированный доступ к данным пользователей (персональным данным, информации о счетах, платежах и т. п.), в 8% исследованных систем атакующий при наличии доступа в личный кабинет мог без прохождения дополнительных проверок сменить пароль пользователя или отключить использование одноразовых паролей; наконец, в 13% систем ДБО нарушитель мог напрямую осуществлять банковские операции от лица других пользователей системы ДБО.

1. Исходные данные

В рамках проведенного исследования было рассмотрено 28 систем дистанционного банковского обслуживания, анализ защищенности которых проводился специалистами Positive Technologies в течение 2013 и 2014 гг. В обзор вошли только системы ДБО, для которых проводился наиболее полный анализ с учетом логики функционирования системы. Так, в данном исследовании не рассматриваются системы ДБО на стадии разработки, для которых проводился только поиск уязвимостей на уровне кода веб-приложения без анализа возможностей несанкционированного проведения транзакций. Кроме того, для обеспечения адекватности статистических данных об идентичных системах ДБО, выпущенных одним и тем же вендором, в исследование включалось только по одной системе соответствующего типа.

Рассмотренные системы ДБО относятся к различным сферам обслуживания. Большинство исследованных систем предназначены для обслуживания физических лиц (77%).

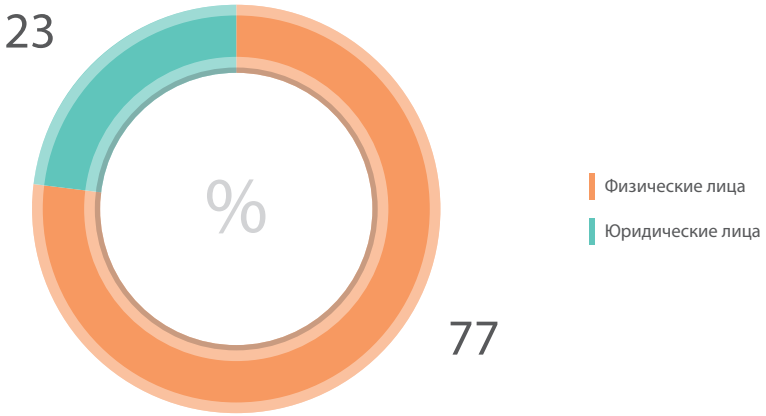

Рис. 1. Распределение систем ДБО по сферам обслуживания

Две трети исследованных систем ДБО (67%) представляли собой приложения собственной разработки банков. Остальные системы были развернуты на базе платформ, созданных известными вендорами. В ходе анализа защищенности систем, разработанных вендорами, было выявлено большое количество критических уязвимостей. В соответствии с политикой ответственного разглашения информации об уязвимостях названия компаний-производителей не указываются.

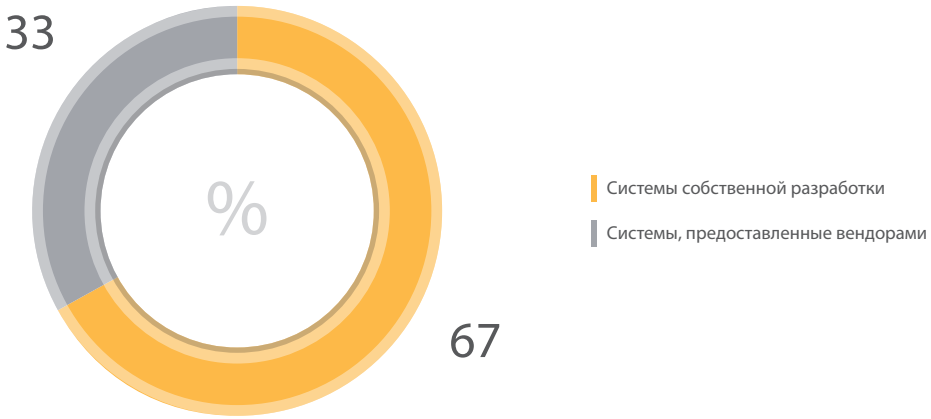

Рис. 2. Типы исследованных систем

Для создания систем ДБО собственной разработки банки использовали Java, C# и PHP. При создании одной из систем использовались два средства разработки — C# и Java. Статистика использования различных средств разработки представлена на рис. 3.

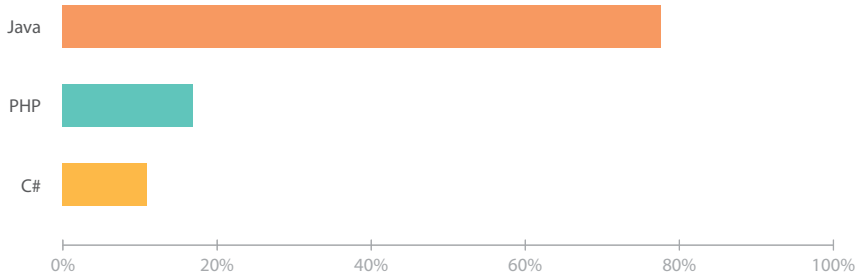

Рис. 3. Средства разработки (доля систем ДБО, %)

В число исследуемых систем ДБО вошли мобильные системы, представленные серверной и клиентской частью, доля которых составила 54%.

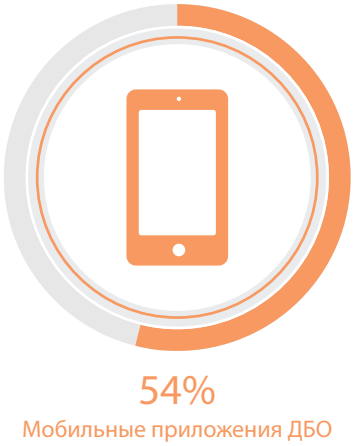

Рис. 4. Доля мобильных приложений в числе систем ДБО

Системы, предоставленные банками для анализа защищенности, находились на различных стадиях разработки. Большинство систем ДБО находились в промышленной эксплуатации и были доступны для клиентов (74%). Четверть ресурсов представляли собой тестовые стенды, готовые к переводу в промышленную эксплуатацию.

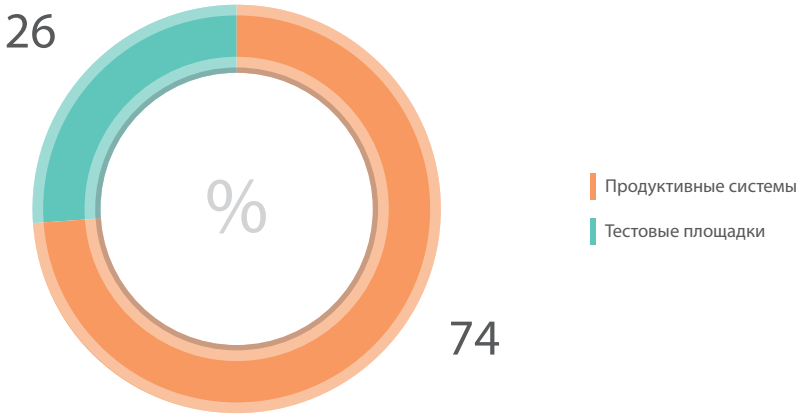

Рис. 5. Распределение систем ДБО по сферам обслуживания

Большая часть систем ДБО разработки известных вендоров находилась в промышленной эксплуатации (77%).

2. Общие результаты работ

2.1. Наиболее распространенные уязвимости и связанные с ними угрозы

При анализе защищенности систем ДБО в 2013—2014 гг. были выявлены уязвимости различного уровня риска. Почти половина уязвимостей — высокого уровня риска (44%). Примерно одинаковое количество уязвимостей имеют среднюю и низкую степень риска (26% и 30% соответственно).

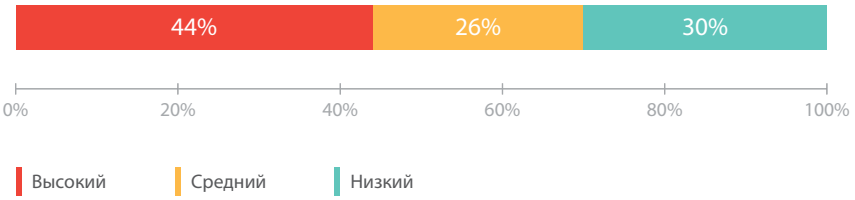

Рис. 6. Распределение уязвимостей по степени риска

В целом уязвимости высокого уровня риска были выявлены в 78% исследованных систем. Распределение систем по максимальной степени риска обнаруженных уязвимостей представлено на рис. 7.

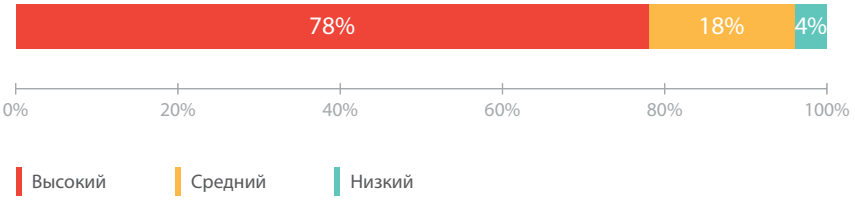

Рис. 7. Распределение систем по максимальной степени риска обнаруженных уязвимостей

Большая часть уязвимостей (42%) связана с ошибками реализации механизмов защиты систем ДБО, заложенных разработчиками. В частности, к данной категории относятся недостатки механизмов идентификации, аутентификации и авторизации. На втором месте по распространенности (36%) — уязвимости, связанные с ошибками в коде приложений, в частности внедрение операторов SQL и межсайтовое выполнение сценариев. Остальные уязвимости (22%) связаны с недостатками конфигурации систем ДБО. Статистика по категориям обнаруженных уязвимостей приведена на рис. 8.

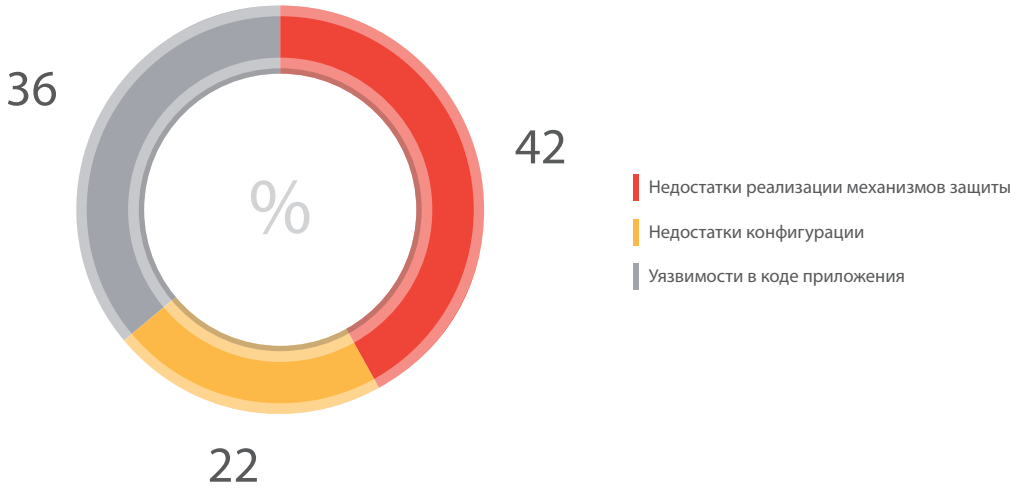

Рис. 8. Общие категории уязвимостей

В 2013—2014 гг. в системах ДБО не было выявлено уязвимостей, связанных с отсутствием актуальных обновлений безопасности, однако это не означает, что во всех исследованных системах установка обновлений осуществлялась своевременно. Для большинства систем анализ защищенности проводился с использованием методов черного и серого ящика, то есть с привилегиями, идентичными привилегиям потенциального злоумышленника. В связи с этим обнаружение уязвимостей осуществлялось только в рамках возможностей соответствующего типа нарушителя, при этом в действительности в системах могли присутствовать устаревшие версии ПО, уязвимости в которых доступны для других категорий злоумышленников.

Наиболее часто в системах ДБО встречались уязвимости, связанные с возможностью идентификации используемого программного обеспечения и с предсказуемыми форматами идентификаторов пользователей. Каждый из этих недостатков был обнаружен в 57% исследованных систем.

Более чем в половине систем (54%) были обнаружены ошибки в программном коде типа «Межсайтовое выполнение сценариев». Если при наличии этой уязвимости в системе клиент банка перейдет по специально сформированной вредоносной ссылке, атакующий может получить доступ к системе ДБО с привилегиями данного клиента.

Кроме того, распространены уязвимости, позволяющие реализовать атаки на сессии пользователей: они также встретились в 54% систем. Это уязвимости, связанные с некорректным завершением сессий пользователей, некорректной настройкой cookie-параметров, возможностью параллельной работы нескольких сессий для одного пользователя, отсутствием привязки сессии к IP-адресу клиента и др. При успешной атаке злоумышленник может получить доступ к личному кабинету с привилегиями пользователя.

В число наиболее распространенных вошла уязвимость высокой степени риска «Внедрение внешних сущностей XML», которая была обнаружена в 46% систем. Она возникает вследствие недостаточной обработки данных, поступающих от пользователя. В результате эксплуатации такой уязвимости злоумышленник может получить содержимое файлов, хранящихся на уязвимом сервере, данные об открытых сетевых портах узла, вызвать отказ в обслуживании всей системы ДБО, — а также, в ряде случаев, обратиться к произвольному узлу от лица уязвимого сервера и развить атаку.

Итоговый рейтинг десяти наиболее часто встречающихся уязвимостей систем ДБО представлен на рис. 9.

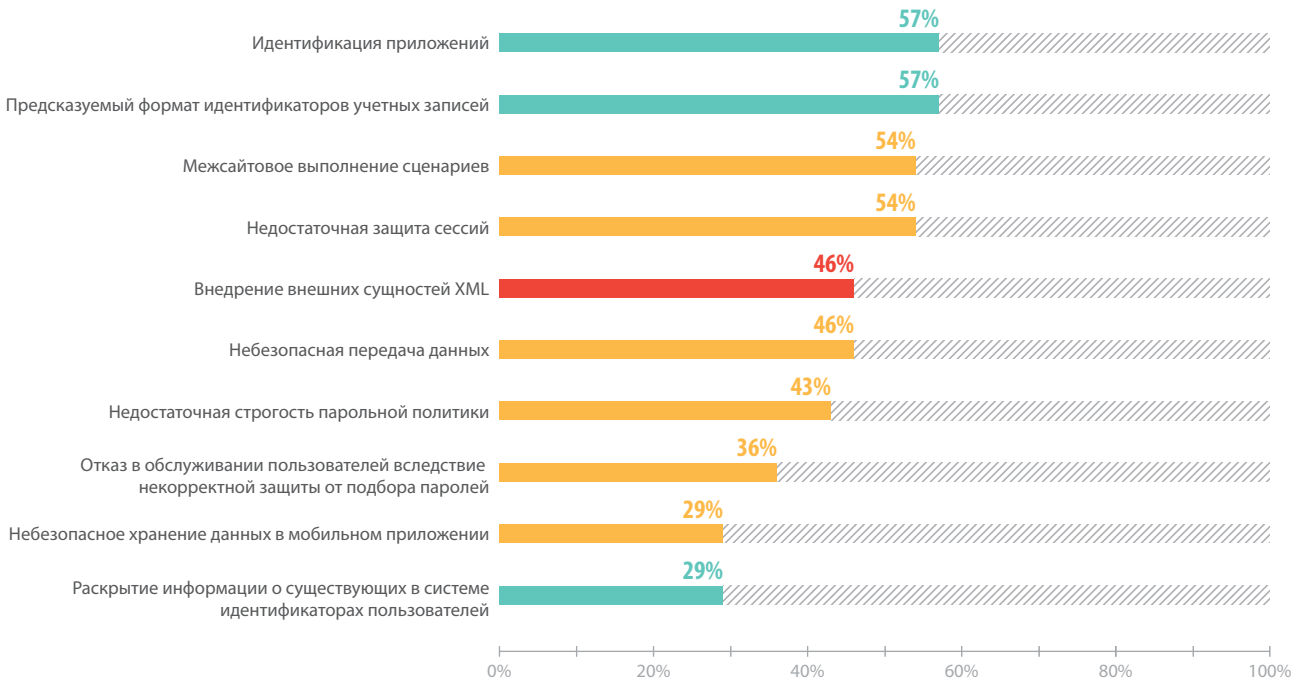

Рис. 9. Рейтинг самых распространенных уязвимостей систем ДБО (доля уязвимых систем)

Большинство самых распространенных уязвимостей имеет средний или низкий уровень риска. Тем не менее комбинация недостатков защищенности и особенностей функционирования конкретных систем ДБО может привести к реализации серьезных угроз безопасности и, как следствие, к финансовому и репутационному ущербу.

Совокупность уязвимостей, выявленных в ходе анализа, потенциально может привести к реализации различных угроз безопасности. Данные о наиболее опасных угрозах безопасности, которые могли быть реализованы в отношении исследованных систем, представлены на рис. 10 (подробно см. разд. 3).

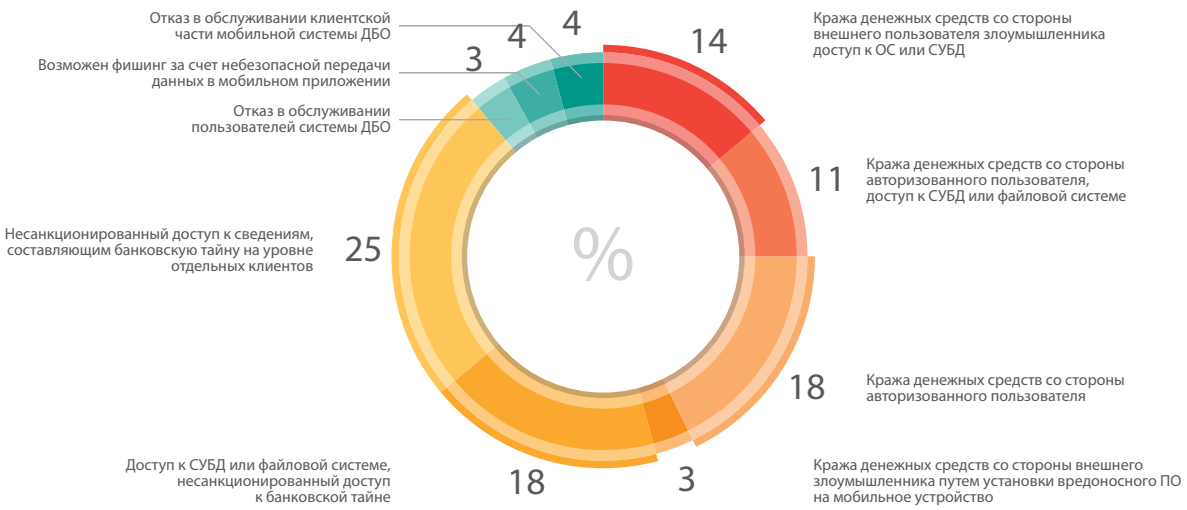

Рис. 10. Реализуемые угрозы ИБ систем ДБО

В отношении исследованных систем ДБО могут быть реализованы серьезные угрозы безопасности, такие как кража денежных средств со стороны внешнего злоумышленника (17%) и кража денежных средств со стороны авторизованного пользователя в результате атак на округление, несанкционированного доступа к операциям произвольного пользователя и эксплуатации других уязвимостей (29%). Кроме того, в 43% случаев возможен доступ к СУБД или ОС уязвимых систем ДБО. Так, в одной из рассмотренных мобильных систем ДБО оказалось возможным выполнение команд ОС как на уровне клиентского устройства на базе Android, так и на уровне сервера, при этом подобные атаки были доступны любому внешнему атакующему без привилегий в системе. Доступ к ОС на сервере системы ДБО может быть использован для вызова отказа в обслуживании, получения важных данных из системы, а также потенциально позволяет развивать атаку вплоть до кражи денежных средств.

Уязвимыми являются как системы собственной разработки, так и системы, созданные профессиональными вендорами. Возможность реализации указанных угроз безопасности была обнаружена в системах ДБО вне зависимости от их стадии разработки: уязвимы и тестовые, и находящиеся в эксплуатации системы. Стоит отметить, что возможность доступа к личным кабинетам пользователей и несанкционированного проведения транзакций может быть получена путем эксплуатации совокупности уязвимостей средней и низкой степени риска. Отсутствие уязвимостей высокой степени риска не гарантирует, что система защищена от серьезных угроз безопасности.

2.2. Уязвимости систем ДБО для физических и юридических лиц

В данном разделе приведены результаты исследования защищенности систем, предназначенных для обслуживания физических и юридических лиц.

В обоих рассматриваемых типах систем преобладают уязвимости, обусловленные недостатками реализации механизмов защиты, которые составляют 42% от общего числа уязвимостей в системах для физических лиц и 47% — в системах для юридических лиц. Второе место по распространенности как в системах для физических лиц, так и в системах для юридических лиц занимают ошибки в программном коде приложений (36% и 39% соответственно). Доли уязвимостей различного типа различаются для двух сфер обслуживания незначительно.

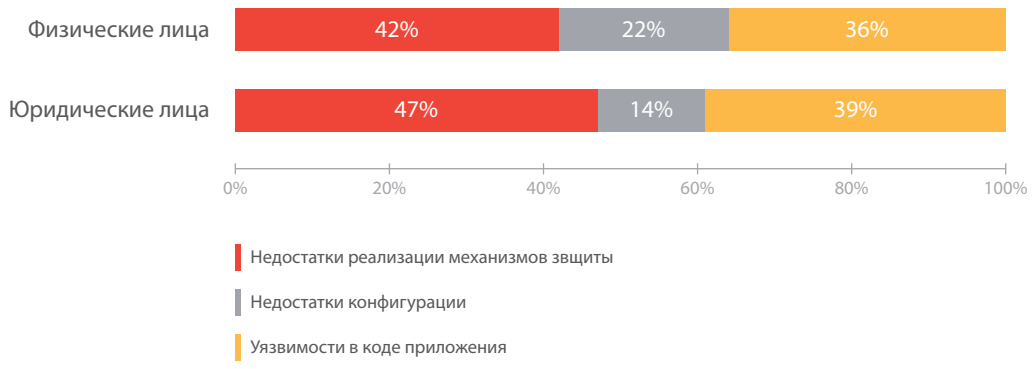

Рис. 11. Типы уязвимостей в системах различного назначения (указаны доли уязвимостей)

Доли уязвимостей различной степени опасности в системах для физических и юридических лиц также различаются незначительно (см. рис. 12).

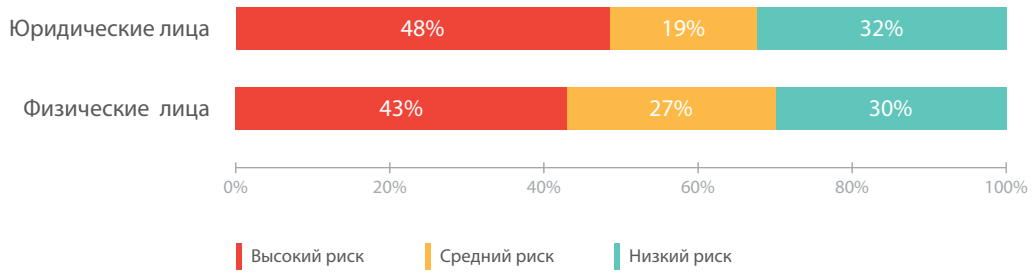

Рис. 12. Распределение уязвимостей в различных системах по степени риска

Все исследованные системы содержали ошибки безопасности. При этом все системы ДБО для юридических лиц оказались подвержены критическим уязвимостям. Доли систем для физических и юридических лиц, подверженных уязвимостям различного уровня риска, представлены на рис. 13 (указана максимальная степень риска обнаруженных уязвимостей).

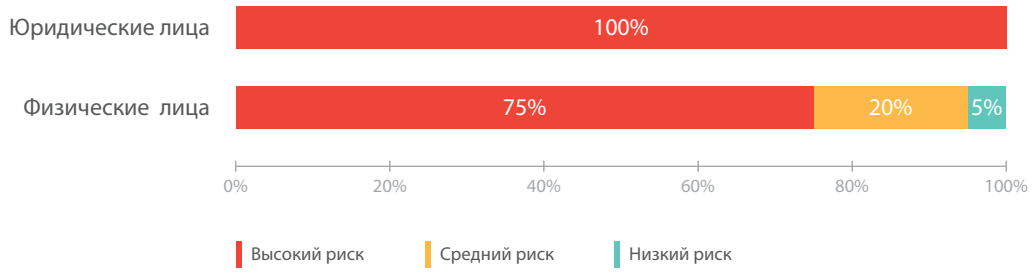

Рис. 13. Распределение систем различного назначения по максимальной степени риска уязвимостей

Для каждого из уровней риска среднее количество уязвимостей на одну систему в системах ДБО для физических лиц оказалось выше по сравнению с системами для юридических лиц. В частности, в системах для физических лиц в среднем почти в два раза больше уязвимостей среднего уровня риска (5,2 против 3 в системах для юридических лиц).

Рис. 14. Среднее число уязвимостей различного уровня риска в одной системе

Во всех исследованных системах для юридических лиц были выявлены уязвимости высокой степени риска. Впрочем, в большинстве систем ДБО для получения доступа к личному кабинету со стороны юридического лица необходимо прохождение процедуры двухфакторной аутентификации с использованием аппаратного токена. В то же время трудно утверждать, что системы ДБО для физических лиц хорошо защищены, поскольку доля таких систем, подверженных критическим уязвимостям, также высока (75%). Кроме того, в системах для физических лиц выше среднее количество уязвимостей на одну систему.

2.3. Уязвимости в системах ДБО собственной разработки и системах профессиональных вендоров

В данном разделе приведены результаты исследования защищенности систем, предоставленных разными категориями разработчиков.

В системах, приобретенных банками у известных вендоров, доля уязвимостей, связанных с ошибками в программном коде, выше, чем в системах собственной разработки банков (48% против 27%). В системах собственной разработки был выявлен больший процент уязвимостей конфигурации по сравнению с платформами, предоставленными вендорами (27% против 14%). Соотношение уязвимостей различного типа для систем собственной разработки и платформ, предоставленных профессиональными вендорами, приведено на рис. 15.

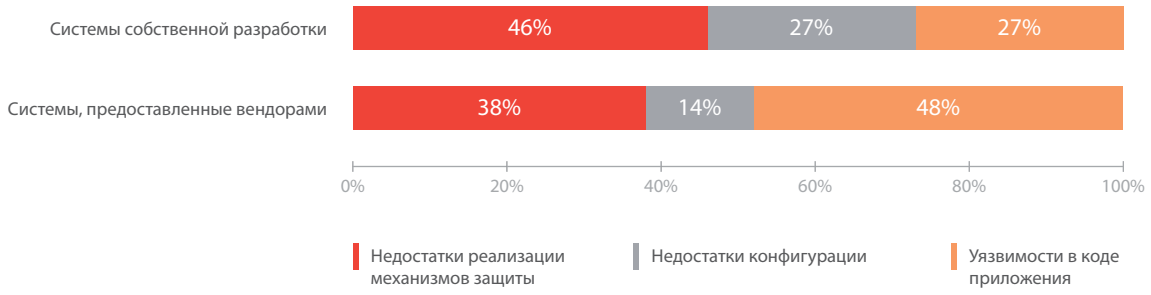

Рис. 15. Доли уязвимостей в системах, предоставленных различными разработчиками

На каждую систему, разработанную известным вендором, в среднем приходится примерно в 2,5 раза больше ошибок в программном коде. Данная тенденция была отмечена также в 2011—2012 гг. и объясняется, вероятнее всего, тем, что при использовании систем, предоставляемых вендором, банк в основном полагается на поставщика в вопросах контроля качества кода. При этом сложная архитектура, кроссплатформенность и большое количество функций систем ДБО не всегда позволяют вендору обеспечить должную защищенность на уровне кода приложения.

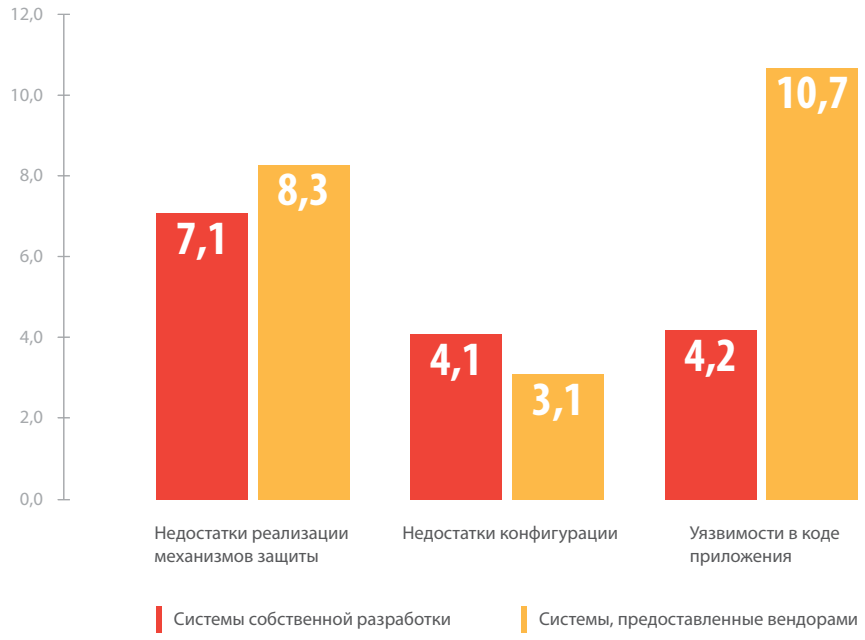

Рис. 16. Среднее число уязвимостей в системах различных разработчиков

Для систем, предоставленных вендорами, каждая вторая уязвимость (49%) имеет высокую степень риска. Для систем собственной разработки большая часть уязвимостей (40%) также характеризуется высоким уровнем риска.

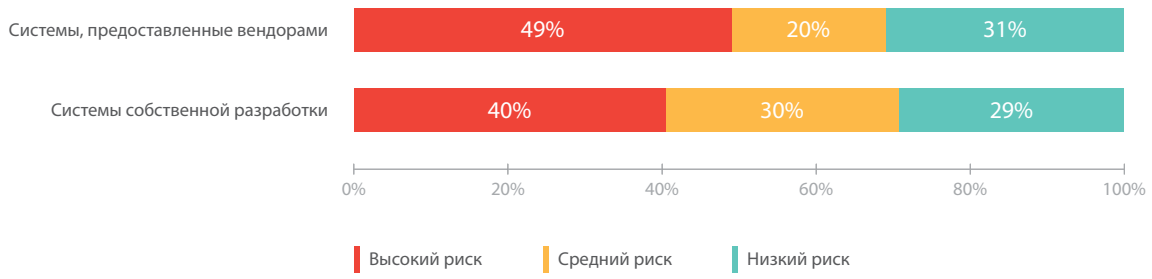

Рис. 17. Распределение уязвимостей по степени риска (доля от общего количества уязвимостей)

Все исследованные системы оказались уязвимы. При этом во всех системах собственной разработки были обнаружены уязвимости средней степени риска и выше. Для платформ, приобретенных у профессиональных вендоров, доля ресурсов, подверженных критическим уязвимостям, незначительно выше (83% против 78% для систем собственной разработки).

На каждую систему, предоставленную вендором, в среднем приходится 10,9 критических уязвимостей, в то время как для систем собственной разработки этот показатель составляет 6,2 (см. рис. 19). Таким образом, системы ДБО, разработанные

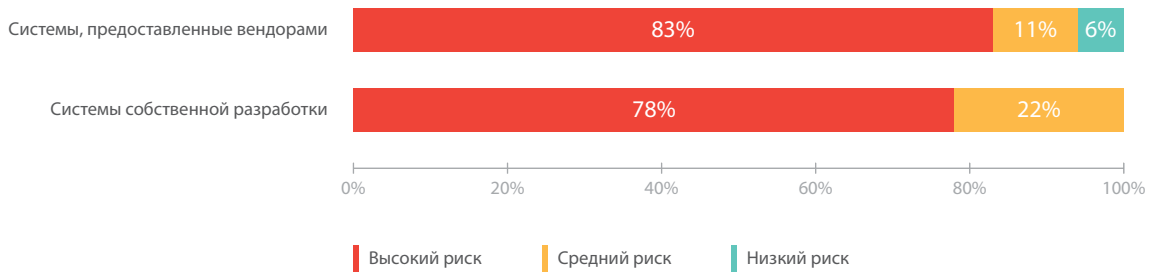

Рис. 18. Распределение систем по максимальной степени риска уязвимостей

сторонними компаниями, в среднем содержат больше уязвимостей, чем приложения собственной разработки банков, поскольку собственные системы ДБО проектируются под конкретную архитектуру и обладают заданной банком функциональностью, что делает их более простыми и, как следствие, менее уязвимыми.

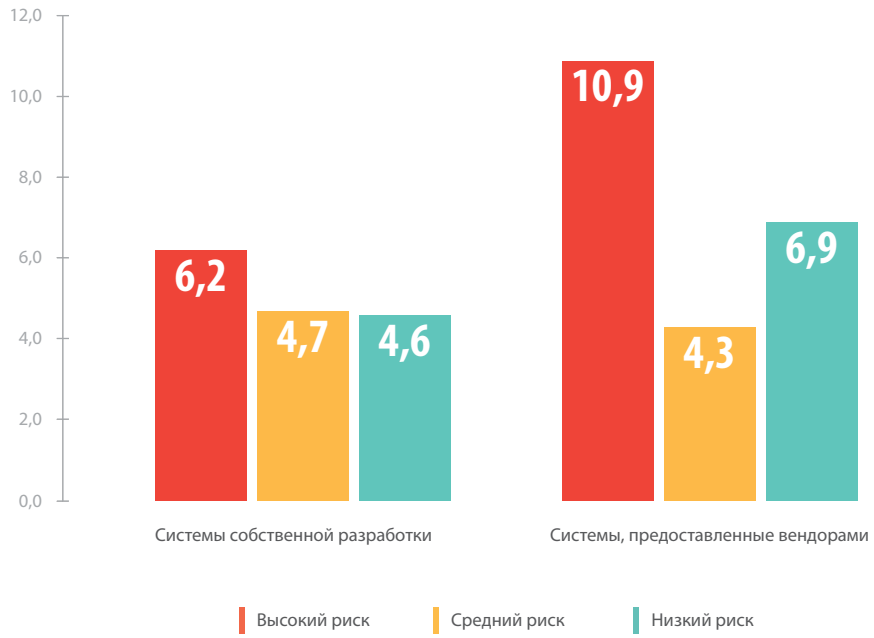

Рис. 19. Среднее количество уязвимостей в системах, предоставленных разными категориями разработчиков

Как и по результатам исследований, проведенных в 2011—2012 гг., можно сделать вывод, что приобретение системы ДБО у профессионального вендора не гарантирует высокого уровня защищенности. Однако переход от покупных систем к собственной разработке сам по себе не означает, что вновь создаваемая система окажется более защищенной. Стоит принять во внимание, что в течение 2013 и 2014 гг. несколько известных поставщиков систем ДБО заявили о внедрении процессов безопасной разработки. Вендоры также ведут работу по устранению уязвимостей, выявленных при анализе защищенности систем ДБО. При этом, во избежание эксплуатации уязвимостей в продуктивных системах ДБО, до выпуска вендором исправлений рекомендуется использовать превентивные средства защиты уровня приложения (web application firewalls). Кроме того, рекомендуется проводить анализ защищенности систем ДБО до ввода эксплуатацию, а также регулярно тестировать системы в ходе эксплуатации, вне зависимости от разработчика.

2.4. Уязвимости тестовых и продуктивных систем ДБО

В данном разделе приведены результаты исследования уровня защищенности тестовых и продуктивных систем ДБО.

Для тестовых систем выше доли уязвимостей, возникших вследствие недостатков реализации механизмов защиты и некорректной конфигурации.

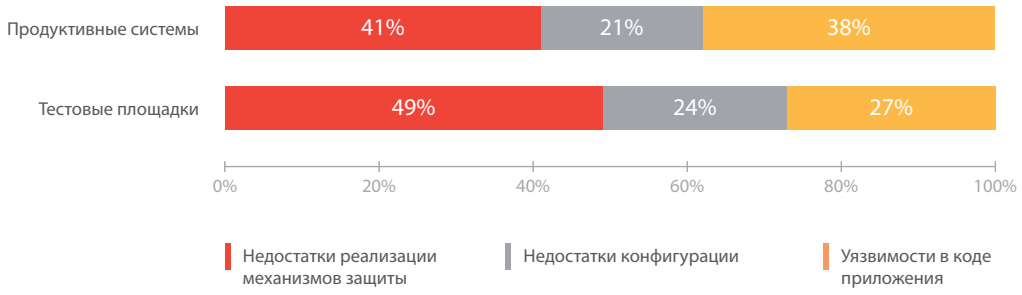

Рис. 20. Доля уязвимостей различного вида в тестовых и продуктивных системах

Среднее количество уязвимостей на одну систему выше для систем, находящихся в эксплуатации, вне зависимости от категории недостатков (см. рис. 21). Данный факт также был отмечен в исследовании, проведенном в 2011—2012 гг. Это можно объяснить тем, что при вводе систем ДБО в эксплуатацию банки уделяют больше внимания выявлению уязвимостей. Для уже функционирующих систем анализ защищенности проводится нерегулярно, и при выявлении уязвимостей сложность реализации уже функционирующих систем не всегда позволяет оперативно вносить изменения в приложения. Кроме того, в ряде случаев условия анализа защищенности в тестовой среде не позволяют полноценно провести некоторые из проверок, например выявить ошибки логики работы приложения, проявляющиеся при взаимодействии с другими банковскими системами, находящимися в стадии промышленной эксплуатации и недоступными на момент тестирования.

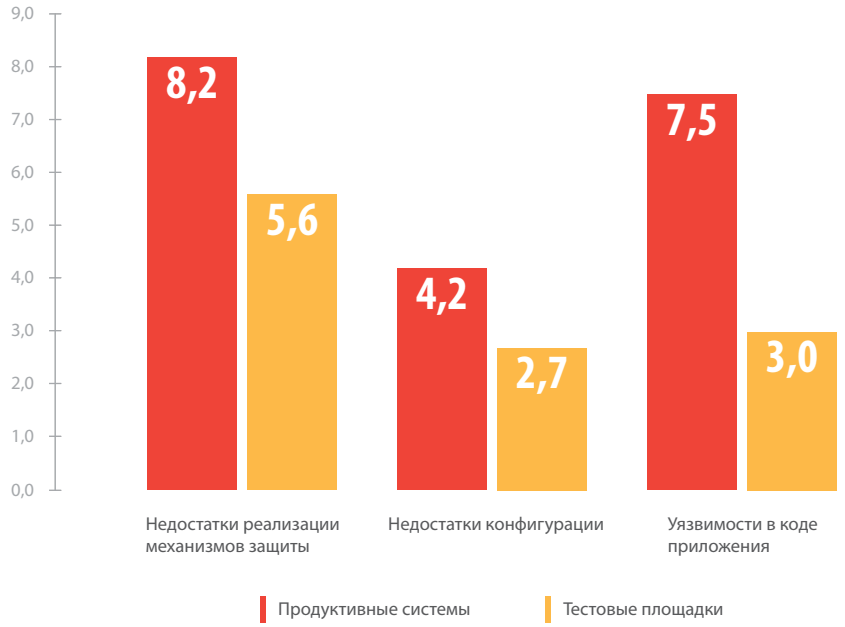

Рис. 21. Среднее количество различных уязвимостей в тестовых и продуктивных системах

Соотношение уязвимостей различного уровня риска для тестовых и продуктивных систем оказалось одинаковым (рис. 22).

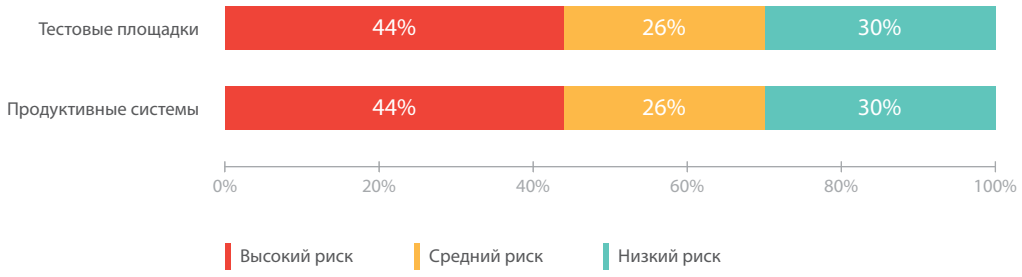

Рис. 22. Уязвимости различного уровня риска в тестовых и продуктивных системах

Все тестовые системы ДБО содержали уязвимости как минимум средней степени риска. 85% продуктивных приложений содержали критические уязвимости (см. рис 23). Подобная ситуация в области защищенности систем ДБО, уже находящихся в эксплуатации, наглядно свидетельствует о необходимости внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений (secure SDLC).

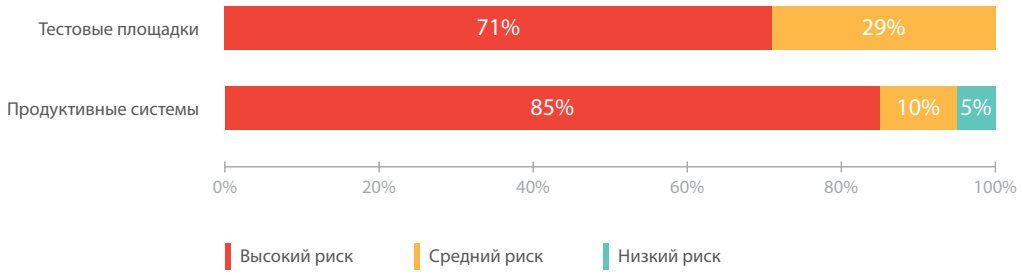

Рис. 23. Распределение тестовых и продуктивных систем по максимальной степени риска

Приведенные выше выводы подтверждаются соотношением среднего количества уязвимостей различного уровня риска для двух рассматриваемых категорий систем (см. рис. 24). Среднее число уязвимостей каждого из уровней риска на одну систему выше для систем, находящихся на стадии эксплуатации.

Результаты проведенного исследования говорят не только о необходимости проведения анализа защищенности системы ДБО перед вводом в эксплуатацию, но и о необходимости проведения регулярного тестирования в процессе ее эксплуатации.

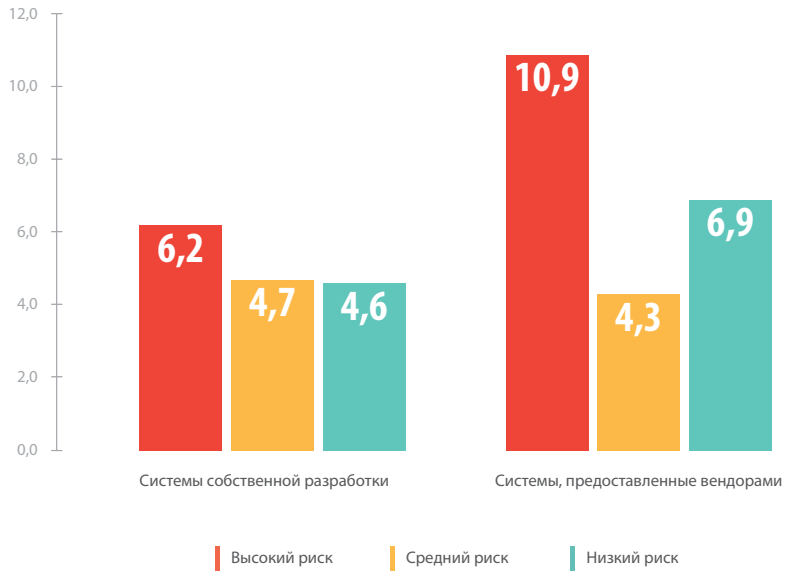

Рис. 24. Среднее количество уязвимостей различного уровня риска в тестовых и продуктивных системах

3. Обзор наиболее опасных уязвимостей

В данном разделе приведен обзор уязвимостей высокой степени риска, которые были обнаружены в большинстве рассмотренных систем ДБО. Перечень наиболее распространенных критических уязвимостей с указанием доли подверженных им систем представлен на рис. 25.

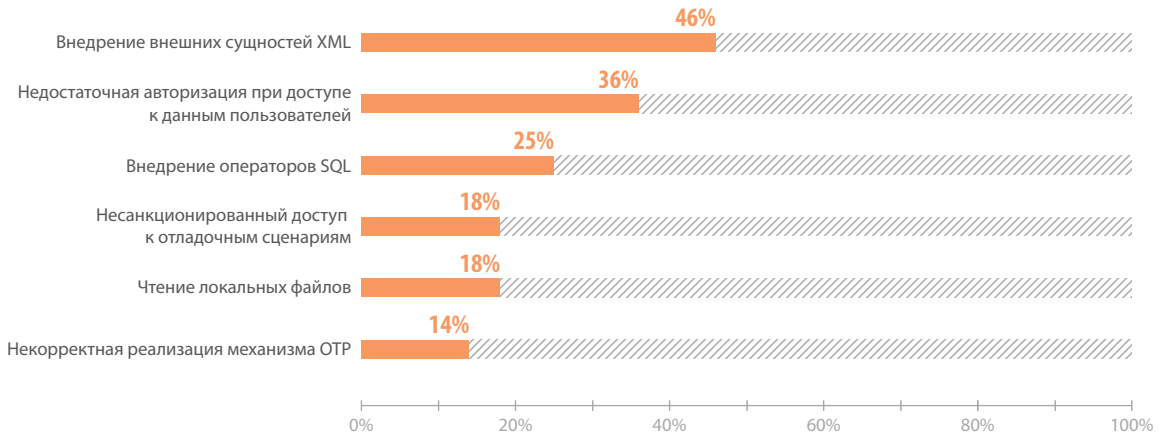

Рис. 25. Наиболее распространенные уязвимости высокой степени риска

Подробное описание самых распространенных критических уязвимостей в системах ДБО приведено ниже.

3.1. Внедрение внешних сущностей XML

«Внедрение внешних сущностей XML» — уязвимость, позволяющая злоумышленнику получить содержимое файлов, расположенных на атакуемом сервере. Уязвимость обусловлена недостаточной проверкой приложением данных, поступающих от пользователя: это позволяет злоумышленнику осуществлять атаку, направленную на изменение логики запроса посредством внедрения произвольного XML-кода. Кроме того, данная уязвимость позволяет злоумышленнику выполнять SMB- и HTTP-запросы в локальной сети атакуемого сервера. Это может привести к разглашению важных данных, получению злоумышленником исходных кодов веб-приложения, файлов конфигурации и другой чувствительной информации о системе.

В результате эксплуатации данной уязвимости в одной из исследованных систем ДБО специалисты Positive Technologies получили доступ к конфигурационному файлу, в котором в открытом виде хранились учетные записи пользователей СУБД, адреса внутренних ресурсов, идентификаторы пользователей системы ДБО и названия файлов журналирования. Кроме того, в результате атаки был получен исходный код сценариев приложения, который позволил выявить другие уязвимости высокой степени риска, такие как «Подключение локальных файлов». Таким образом, внешний злоумышленник потенциально мог развивать атаку вплоть до выполнения произвольных команд ОС и получения полного контроля над сервером.

3.2. Недостаточная авторизация при доступе к данным пользователей

Эта уязвимость связана с недостатками механизма авторизации пользователей. В ряде систем ДБО (36%) проверка пользовательских привилегий реализована некорректно или отсутствует, вследствие чего злоумышленник может получить доступ к некоторым сценариям и файлам, обратившись к ним напрямую. В зависимости от специфики и набора функций системы злоумышленник может получить несанкционированный доступ к такой информации, как:

- персональные данные пользователей системы ДБО;
- информация о транзакциях и платежных картах пользователей;
- файлы, загруженные в систему ДБО произвольными пользователями;

- информация о сертификатах различных пользователей системы ДБО;
- специфические данные о клиентах (счета, шаблоны платежей).

В ходе анализа защищенности одной из систем ДБО для юридических лиц было обнаружено, что имена файлов, загружаемых пользователями в приложение, являются предсказуемыми: злоумышленник мог путем перебора получить доступ ко всем пользовательским файлам (в частности, к файлам, содержащим важные данные клиентов банка — оферты, договоры и проч.).

3.3. Внедрение операторов SQL

Эксплуатация уязвимости осуществляется путем внедрения операторов SQL и отслеживания изменений в получаемом содержимом страницы. Уязвимость обусловлена недостаточной проверкой приложением данных, поступающих от пользователя: она позволяет злоумышленнику осуществлять атаку, направленную на изменение логики запроса к базе данных. В зависимости от специфики и функциональности системы ДБО злоумышленник мог осуществлять следующие несанкционированные действия:

- определять версии используемых СУБД;
- получать идентификаторы и пароли пользователей;
- получать одноразовые пароли;
- создавать и изменять данные платежных поручений.

В некоторых исследованных системах в результате эксплуатации уязвимостей типа «Внедрение операторов SQL» были получены идентификаторы и значения хеш-функций паролей пользователей системы ДБО. В ряде случаев на базе полученных хешей специалисты смогли подобрать пароли пользователей. Кроме того, при эксплуатации данной уязвимости полученные привилегии в ряде случаев позволяют развить атаку вплоть до исполнения команд ОС и полной компрометации систем.

4. Недостатки механизмов идентификации

76% исследованных систем ДБО содержали по меньшей мере один из следующих недостатков механизма идентификации пользователей:

- предсказуемый формат идентификаторов учетных записей;
- раскрытие информации о существующих в системе идентификаторах пользователей.

Данные недостатки предоставляют злоумышленнику возможность составить список зарегистрированных идентификаторов пользователей и провести атаки, направленные на получение доступа к системе ДБО от имени пользователя (например, подбор пароля). Несмотря на низкий уровень риска подобных уязвимостей, возможность получения злоумышленником данных об идентификаторах в совокупности с выявленными недостатками механизмов аутентификации, авторизации и защиты транзакций (см. разд. 5 и 6) может сыграть существенную роль в получении несанкционированного доступа к личным кабинетам пользователей и последующем проведении транзакций.

Кроме того, в половине исследованных систем используется блокировка учетных записей пользователей после определенного числа попыток неправильного ввода пароля. Знание идентификаторов зачастую может позволить злоумышленнику провести атаку, направленную на отказ в обслуживании пользователей системы ДБО.

Данные о подобных недостатках в системах различных разработчиков даны на рис. 26.

4.1. Предсказуемый формат идентификаторов

Наиболее распространенным недостатком механизмов идентификации исследованных систем ДБО является предсказуемость формата идентификатора учетной записи. Большинство рассматриваемых систем (64%) подвержены данной уязвимости (см. рис. 27).

Рис. 26. Доли систем, подверженных уязвимостям механизмов идентификации

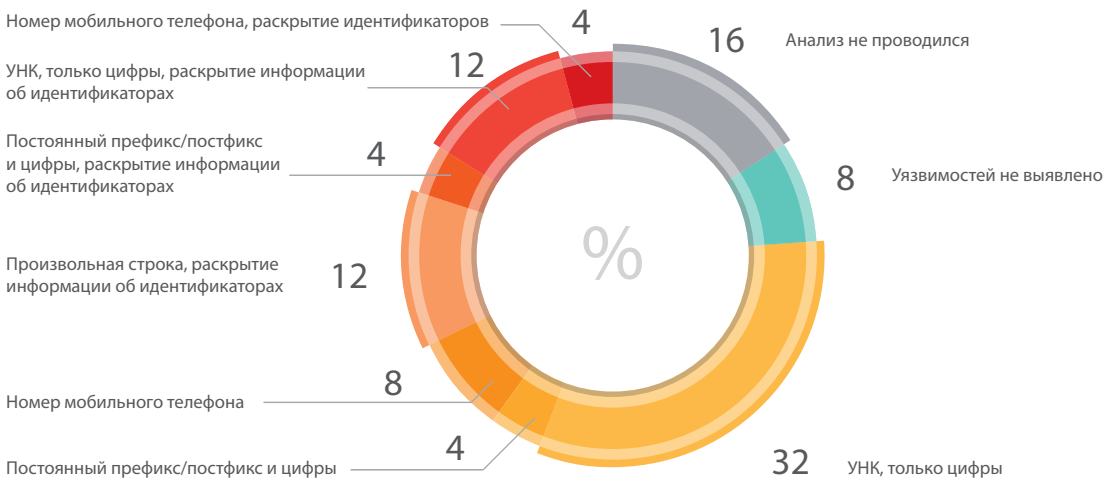

Рис. 27. Недостатки механизмов идентификации (доля систем)

Формат идентификаторов систем ДБО зачастую позволяет злоумышленнику, знающему несколько существующих в системе идентификаторов, предсказать другие существующие в системе идентификаторы, вычислив механизм их формирования системой. Наиболее распространенные форматы предсказуемых идентификаторов это:

- идентификаторы, состоящие из случайного набора цифр (например, 6321970) — встретились в 44% рассмотренных систем;
- идентификаторы, представляющие собой телефонный номер пользователя (например, 89012345678) — встретились в 12% рассмотренных систем;
- идентификаторы, состоящие из набора цифр и постоянного префикса или постфикса (например, usr1378, 1231254YP) — встретились в 8% рассмотренных систем.

Зачастую в качестве цифрового идентификатора используется уникальный номер клиента (УНК), который при этом может иметь небольшую длину (в рассмотренных системах ДБО длина УНК составляла от 5 до 9 символов). Идентификаторы подобного формата могут быть легко подобраны злоумышленником.

На рис. 27 приведена итоговая статистика использования различных уязвимых форматов идентификаторов в системах ДБО. Анализ формата идентификаторов не проводился для 16% систем ДБО: они находились на стадии разработки, в связи с чем окончательный формат идентификаторов учетных записей еще не был утвержден.

Для того чтобы избежать описанного выше недостатка рекомендуется добавлять к идентификаторам символы, которые генерируются случайным образом, например: 1234567-Tn4, 1234568-h2S. Это существенно повысит сложность реализации атак методом прямого перебора (brute force). В случае использования идентификаторов, которые могут задаваться пользователями произвольно, рекомендуется запрещать пользователям использование в качестве идентификатора распространенных словарных комбинаций.

4.2. Раскрытие информации об идентификаторах

Еще один распространенный тип недостатков механизмов идентификации — раскрытие информации о существующих в системе учетных записях: этой уязвимости подвержено 32% исследованных систем. Раскрытие информации возникает вследствие того, что уязвимая система возвращает различные ответы в зависимости от существования введенного идентификатора. Часто уязвимость встречается в сценариях регистрации новых пользователей или смены пароля, когда система ДБО выдает различный результат для зарегистрированных и незарегистрированных пользователей.

Стоит отметить, что в 20% случаев системы содержали оба недостатка: как раскрытие информации об идентификаторах, так и предсказуемый формат идентификаторов.

5. Недостатки механизмов аутентификации

В данном разделе приведен обзор уязвимостей, связанных с недостатками механизмов аутентификации систем ДБО. При анализе не учитывалась система, в которой аутентификация пользователей происходила на стороннем ресурсе, не вошедшем в границы проведения работ.

В большинстве рассмотренных систем (71%) использовалась обязательная двухфакторная аутентификация пользователей, требующая дополнительного предъявления аппаратного токена или ввода одноразового пароля. В 8% исследованных систем двухфакторная аутентификация не являлась обязательной: пользователь мог отключить ее при входе в личный кабинет. В остальных системах ДБО аутентификация осуществлялась на основании идентификатора и пароля пользователя.

Выявленные уязвимости механизмов аутентификации систем ДБО относятся преимущественно к следующим основным категориям:

- возможность обхода механизма CAPTCHA;
- отсутствие обязательной двухфакторной аутентификации при доступе в личный кабинет (при отсутствии таковой на этапе проведения транзакций);
- недостатки парольной политики;
- недостаточная защита от подбора учетных данных (brute force).

Уязвимости механизмов аутентификации, связанные с недостаточной защитой учетных данных от подбора и недостаточной строгостью парольной политики, являются наиболее распространенными недостатками данного типа.

Данные о недостатках механизмов аутентификации представлены на рис. 28.

5.1. Недостатки парольной политики

Среди недостатков парольной политики наиболее распространенными являются следующие:

- недостаточное ограничение длины пароля: возможен выбор пароля длиной менее 8 символов (в 38% рассмотренных систем минимальная длина пароля составляла 4 или 6 символов);

Рис. 28. Доля систем с ошибками в механизмах аутентификации

- некорректная реализация или отсутствие проверки на использование словарных паролей (в 25% систем допускается установка простых паролей, таких как «11111111» или «123123»);
- возможность задания пароля, который уже использовался ранее (данный недостаток был обнаружен в 8% систем).

Подобные недостатки в совокупности с недостаточной защитой от атак, направленных на подбор пароля, а также отсутствием двухфакторной аутентификации при входе в систему делают возможными атаки на пользователей, приводящие к несанкционированному доступу к личным кабинетам клиентов банков. Поскольку аутентификация является первым барьером для доступа к системе, рекомендуется внимательно относиться к парольной политике, исключая возможность использования коротких и словарных паролей, особенно в случае если для доступа к личному кабинету клиента достаточно обладать только идентификатором и паролем.

В случае отсутствия двухфакторной аутентификации при входе в систему ДБО минимальная рекомендуемая длина пароля пользователя составляет 8 символов, в пароле должны присутствовать символы верхнего и нижнего регистра, цифры и спецсимволы. Кроме того, следует запретить использовать в качестве паролей словарные значения (например, P@ssw0rd). Срок действия пароля должен быть ограничен, при этом пользователь не должен иметь возможность выбрать новый пароль, совпадающий с последними из предыдущих.

На рис. 29 представлено отношение числа систем, содержащих различные недостатки парольной политики, к общему количеству исследуемых.

5.2. Недостаточная защита от подбора учетных данных пользователей

Подбор учетных данных оказался возможен в 17% исследованных систем. В качестве защитной меры от атак, направленных на подбор пароля, зачастую используется механизм временной или постоянной блокировки учетных записей после нескольких неудачных попыток ввода пароля, однако данный механизм не позволяет защититься в полной мере. В случае когда парольная политика разрешает использование словарных паролей, при отсутствии двухфакторной аутентификации злоумышленник может провести атаку, направленную на подбор учетных записей по заданному словарному паролю.

Следует отметить, что одна из систем оказалась уязвима к подбору учетных данных — несмотря на наличие двухфакторной аутентификации, поскольку возможность ввода одноразового пароля (OTP) для доступа в личный кабинет предоставлялась только тем пользователям, которые ввели корректный идентификатор и пароль.

В случае отсутствия двухфакторной аутентификации при входе в систему для защиты от подбора паролей пользователей рекомендуется использовать технологию Completely Automatic Public Turing test to tell Computers and Humans Apart (CAPTCHA).

Рис. 29. Основные недостатки механизмов аутентификации (доля систем)

Данный механизм запрашивает у пользователя ввод отображенной на экране информации при частых попытках ввода неверных учетных данных, что позволяет повысить затраты злоумышленника на подбор идентификаторов и паролей пользователей.

Использование технологии CAPTCHA в совокупности со строгой парольной политикой позволяет существенно повысить стойкость системы к подбору учетных данных при отсутствии двухфакторной аутентификации. При реализации блокировки рекомендуется учитывать такие факторы, как временной промежуток между последовательными попытками входа, IP-адрес источника, факты подбора не только паролей, но и идентификаторов.

5.3. Отсутствие двухфакторной аутентификации при входе в личный кабинет

В ряде рассмотренных систем (29% от общего числа) для доступа к личному кабинету пользователь должен предъявить только идентификатор и пароль. При этом использование строгой парольной политики и эффективной защиты от подбора учетных данных в комбинации с двухфакторной аутентификацией на этапе проведения транзакций, как правило, позволяет обеспечить приемлемый уровень безопасности.

Однако для некоторых систем (8%) было установлено, что дополнительная проверка принадлежности учетных данных легитимному пользователю не осуществляется ни на стадии входа в кабинет, ни на стадии проведения транзакции. В данном случае отсутствие двухфакторной аутентификации при входе в личный кабинет рассматривалось как уязвимость, поскольку подобная реализация механизмов защиты создает повышенные риски для системы ДБО.

В общем случае даже для систем, в которых отсутствуют недостатки, связанные со слабой парольной политикой и недостаточной защитой учетных данных, а также реализована двухфакторная аутентификация на этапе проведения транзакций, рекомендуется рассмотреть возможность перехода к двухфакторной аутентификации при входе в личный кабинет. Данная мера позволит снизить риски несанкционированного доступа к персональным данным пользователей, информации о счетах, получателях платежей и другим важным данным. Кроме того, при наличии пользовательского доступа злоумышленник получает возможность развивать атаку не только в направлении обхода авторизации и проведения транзакций от имени пользователя, но и с целью выявления и эксплуатации недостатков серверных компонентов системы (например, уязвимостей типа «Внедрение внешних сущностей XML» и «Внедрение операторов SQL»).

6. Недостатки механизмов авторизации и защиты транзакций

В рассмотренных системах авторизация пользователей реализуется на базе механизма формирования сессии пользователя. В некоторых системах помимо идентификатора сессии для авторизации используются дополнительные параметры, такие как уникальный токен запроса. Во всех исследованных системах идентификатор сессии обладал достаточной энтропией, что делает подбор идентификатора затруднительным. Однако в ряде систем сессия была недостаточно защищена от перехвата и последующего использования злоумышленником:

- в 46% случаев отсутствовала привязка сессии к IP-адресу и браузеру клиента;
- в 21% систем была возможна параллельная работа с одной учетной записью;
- в одной из рассмотренных систем ДБО не было ограничено время сессии.

Кроме того, для cookie-параметров, содержащих идентификатор сессии и другие важные данные, зачастую не были установлены свойства secure и HTTPOnly, что делало возможным проведение атак на сессии пользователей (см. разд. 8). При этом во многих системах данные передавались незащищенным образом и могли быть перехвачены злоумышленником.

Для защиты процесса проведения транзакций в большинстве рассмотренных систем применялась двухфакторная аутентификация с использованием одноразовых паролей (one time passwords, OTP). Однако для ряда систем двухфакторная аутентификация на этапе подтверждения транзакций отсутствовала.

Наиболее распространенными серьезными недостатками механизмов защиты транзакций систем ДБО, согласно проведенному исследованию, являются:

- недостаточная авторизация (уязвимости данного типа были обнаружены в 71% систем ДБО), в том числе при доступе к данным пользователей (см. разд. 3.2), к отладочным сценариям, при отключении пароля или OTP, при доступе к операциям произвольного пользователя в приложении (в том числе — к функциям проведения транзакций);
- некорректная реализация механизма OTP, вследствие которой злоумышленник может проводить несколько транзакций по одному одноразовому паролю или перехватить значение OTP (подобные уязвимости были обнаружены в 17% систем ДБО);
- отсутствие двухфакторной аутентификации на этапе проведения транзакций (данная уязвимость была обнаружена в 13% систем ДБО).

Данные о недостатках защиты транзакций представлены на рис. 30 и 31.

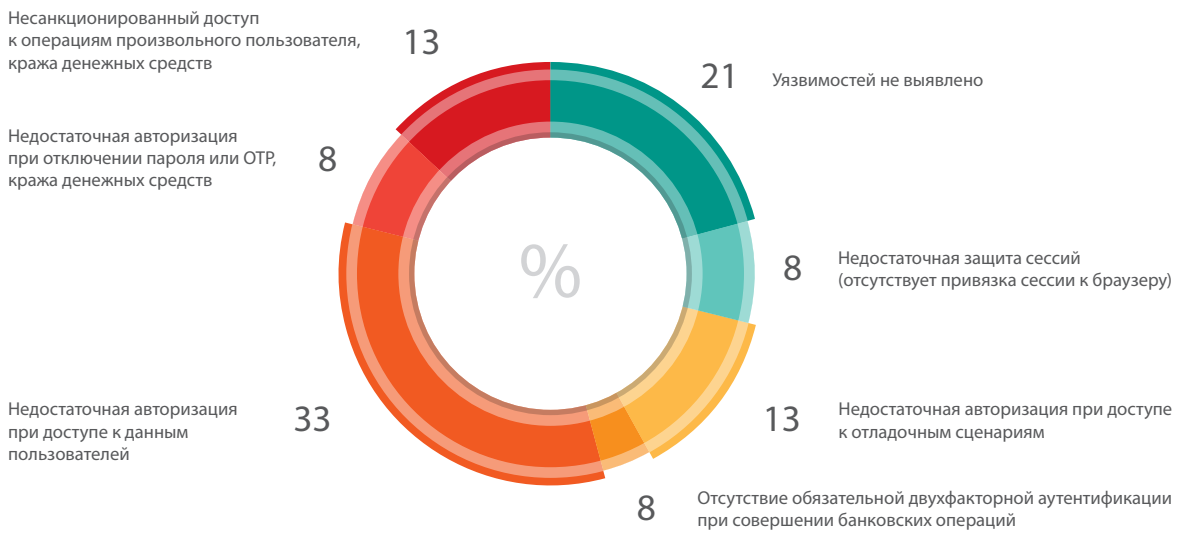

Рис.30. Наиболее значительные недостатки механизмов авторизации (доли уязвимых систем, %)

Рис. 31. Недостатки механизмов авторизации систем ДБО различных видов разработки

Большинство уязвимостей авторизации характерны в первую очередь для систем, поставляемых вендорами. Исключение составляют недостатки, возникшие вследствие недостаточной проверки прав доступа при совершении критически важных операций: к ним относится возможность сменить пароль или отключить механизм OTP путем отправки специально сформированного запроса к приложению без дополнительного предъявления пароля.

6.1. Недостаточная авторизация

Уязвимости, связанные с недостаточной авторизацией пользователей, были обнаружены в 71% исследованных систем, причем в 54% исследованных систем в результате эксплуатации уязвимостей данного типа злоумышленник получает доступ к сведениям, составляющим банковскую тайну, а в 25% случаев – доступ к проведению банковских операций от лица произвольных пользователей.

К данному типу уязвимостей относятся следующие:

- недостаточная авторизация при доступе к данным пользователей, таким как информация о счетах, шаблоны платежей (см. разд. 3.2): данная уязвимость была выявлена в 36% исследованных систем ДБО;
- недостаточная авторизация при доступе к отладочным сценариям (18% систем);
- несанкционированный доступ к операциям произвольного пользователя (13% систем), в результате которого авторизованный пользователь может задать чужую платежную карту для совершения платежа, переименовать чужую карту и совершать прочие мошеннические действия от имени других пользователей системы;
- недостаточная авторизация при отключении пароля или OTP (8% систем), заключающаяся в возможности посредством специально сформированного запроса сменить пароль или отключить механизм OTP без дополнительной проверки прав доступа пользователя.

6.2. Отсутствие двухфакторной аутентификации при проведении транзакций

Использование одноразовых паролей при проведении транзакций позволяет обеспечить защиту от несанкционированного доступа. Однако в 13% рассмотренных систем двухфакторная аутентификация на этапе проведения банковских операций отсутствовала. При этом в 8% систем двухфакторная аутентификация отсутствовала не только при проведении транзакций, но и при входе в личный кабинет. Таким образом, злоумышленник получал возможность беспрепятственно осуществлять транзакции при получении доступа с правами пользователя (например, в результате подбора учетных данных или перехвата сессии).

7. Уязвимости на уровне кода веб-приложений

7.1. Общая статистика уязвимостей в коде приложений

В данном разделе приведен обзор уязвимостей, обусловленных ошибками в программном коде систем ДБО.

Большинство исследованных систем подвержены уязвимостям на уровне кода приложений (82%). Данный показатель не изменился по сравнению с 2011—2012 гг. При этом все ресурсы, подверженные недостаткам данного типа, содержат уязвимости как минимум средней степени риска. Большинство исследованных систем (68%) содержат ошибки в программном коде, уровень риска которых оценивается как высокий.

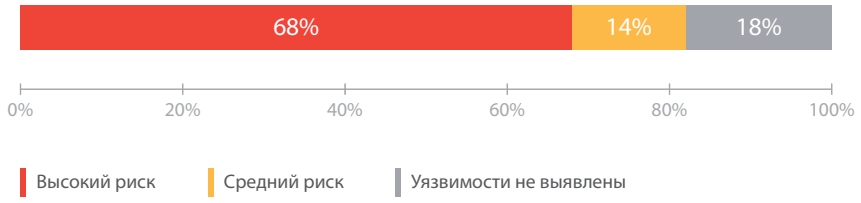

Рис. 32. Распределение систем по максимальной степени риска уязвимостей на уровне кода приложений

Доли систем, подверженных уязвимостям уровня кода веб-приложений различной степени риска, представлены на рис. 33.

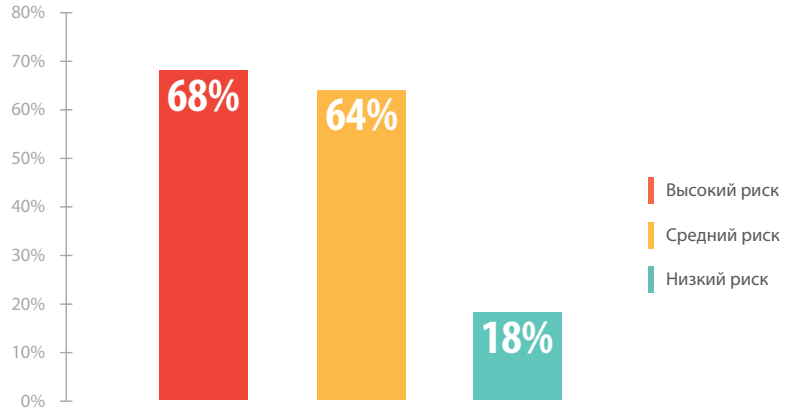

Рис. 33. Доли систем с уязвимостями уровня кода приложений

43% ошибок в программном коде приложений имеют высокий уровень риска. К данной категории относится самая распространенная из опасных уязвимостей систем ДБО — «Внедрение внешних сущностей XML» (см. разд. 3.1). Более половины уязвимостей на уровне кода (52%) имеют средний уровень риска.

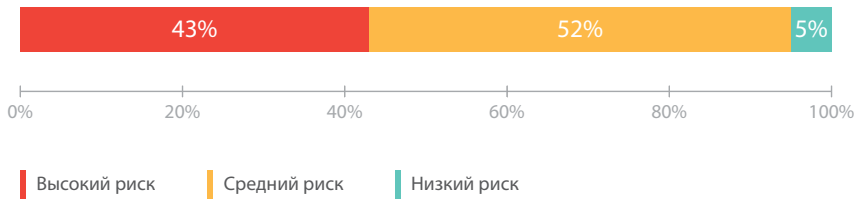

Рис. 34. Распределение уязвимостей на уровне кода приложений по степени риска

Среднее количество ошибок в программном коде, приходящееся на одну систему, дано на рис. 35.

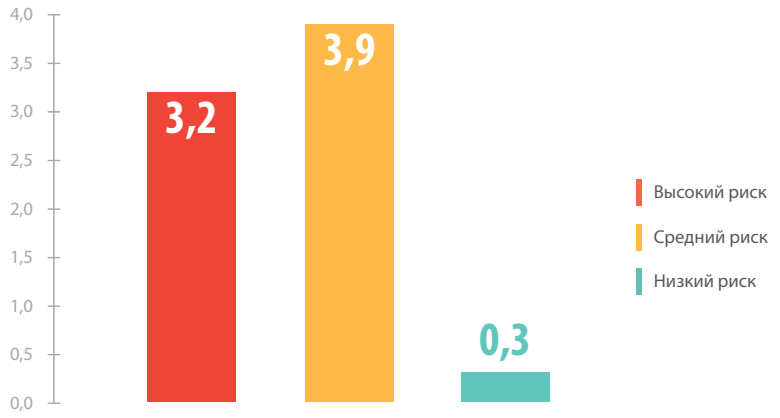

Рис. 35. Среднее число уязвимостей кода приложений в системе

7.2. Уязвимости веб-приложений в системах собственной разработки и в системах, поставляемых вендорами

Как упоминалось ранее, системы, поставляемые известными вендорами, содержат большее количество уязвимостей в программном коде (см. разд. 2.3). Кроме того, для данной категории систем более половины (56%) выявленных уязвимостей имеют высокий уровень риска (см. рис. 36).

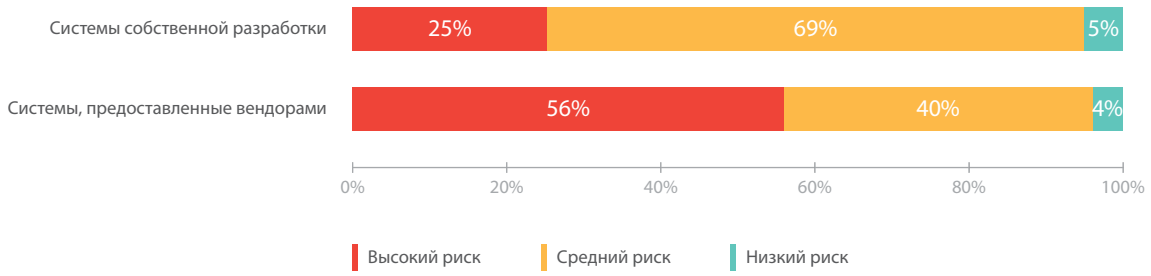

Рис. 36. Доля ошибок в программном коде в зависимости от категории разработчика

В среднем в каждой системе ДБО, поставляемой вендором, содержится около 6 критических уязвимостей на уровне кода приложения. Системы собственной разработки содержат почти в 6 раз меньше подобных ошибок, имеющих высокую степень риска.

7.3. Наиболее распространенные уязвимости уровня веб-приложения

Перечень наиболее распространенных уязвимостей уровня кода приложения, а также соответствующие доли уязвимых систем ДБО представлены на рис. 38.

Множественные уязвимости типа «Межсайтовое выполнение сценариев» были обнаружены более чем в половине исследованных систем ДБО (54% от общего числа). В 2011—2012 гг. данная уязвимость также встречалась в большинстве исследованных ресурсов. Таким образом, каждая вторая система позволяет проводить атаки на клиентов.

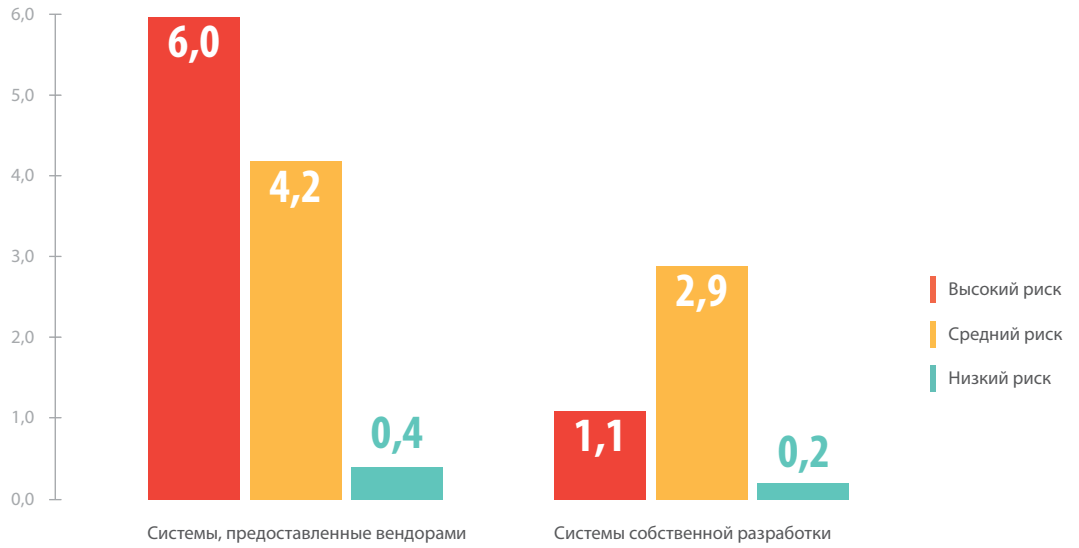

Рис. 37. Среднее число уязвимостей уровня кода приложений на одну систему

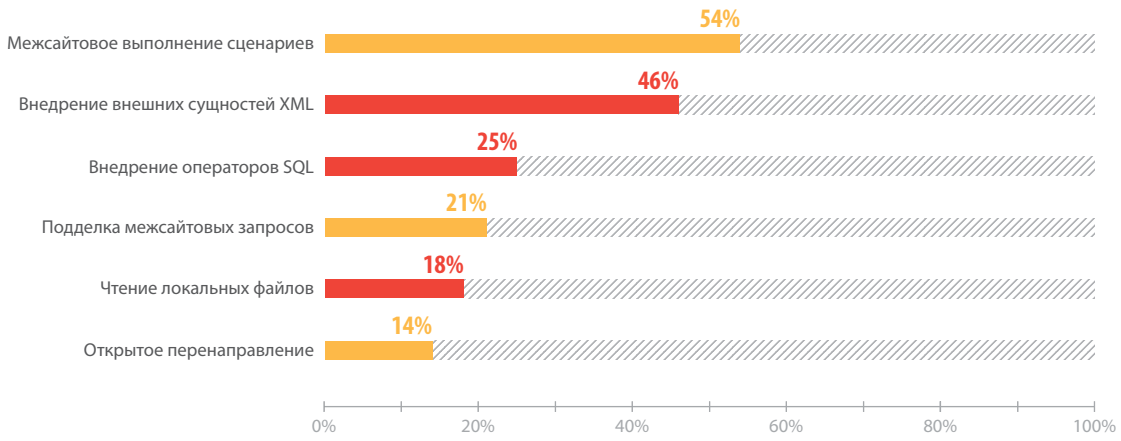

Рис. 38. Доля систем, подверженных наиболее распространенным уязвимостям уровня кода приложения

Стоит отметить, что перечисленные уязвимости, за исключением ошибок типа «Открытое перенаправление», в большей степени характерны для систем, предоставленных вендорами. Доли систем, подверженных различным уязвимостям в коде приложений, в зависимости от категории разработчиков представлены на рис. 39.

Для снижения рисков, связанных с эксплуатацией уязвимостей на уровне веб-приложения, рекомендуется внедрять практики безопасного программирования, регулярно проводить анализ защищенности приложений (желательно с анализом исходного кода) и оперативно устранять выявленные уязвимости в коде. В случае использования систем, поставляемых сторонними вендорами, при невозможности оперативного исправления недостатков рекомендуется использовать превентивные средства защиты уровня приложения.

Рис. 39. Системы с наиболее распространенными уязвимостями уровня кода приложения

8. Недостатки конфигурации

8.1. Общая статистика недостатков конфигурации

В данном разделе приведен обзор уязвимостей систем ДБО, обусловленных недостатками конфигурации.

Недостатки данной категории вызваны некорректной настройкой операционных систем, СУБД, веб-сервера и компонентов веб-приложений. 22% всех обнаруженных уязвимостей относятся к этому типу (см. рис. 8). Большинство уязвимостей данной категории (62% от общего числа) имеют средний уровень риска.

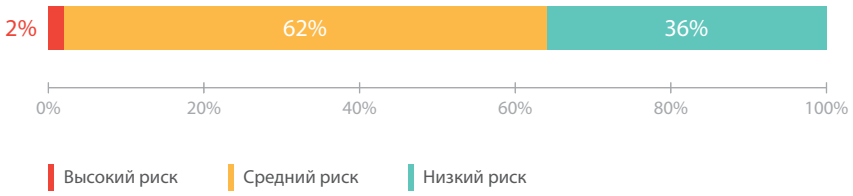

Рис. 40. Распределение выявленных недостатков конфигурации по степени риска

89% рассмотренных систем содержали хотя бы одну уязвимость, связанную с недостатками конфигурирования. При этом 71% систем содержали недостатки среднего уровня риска и выше.

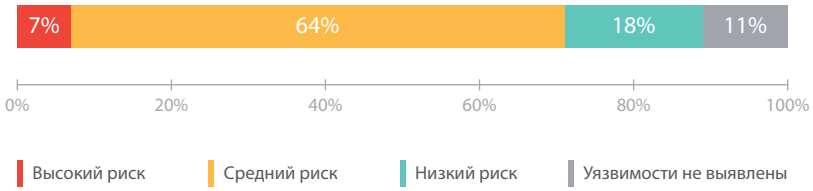

Рис. 41. Доли систем с недостатками конфигурации (по максимальному уровню риска)

Уязвимости высокой степени риска связаны с назначением избыточных привилегий мобильным приложениям ДБО, вследствие которого злоумышленник с помощью вредоносного ПО может совершать исходящие звонки от лица легитимного пользователя, а также выполнять системные команды на устройстве пользователя.

В среднем каждая система ДБО содержит более 4 уязвимостей, связанных с некорректными настройками.

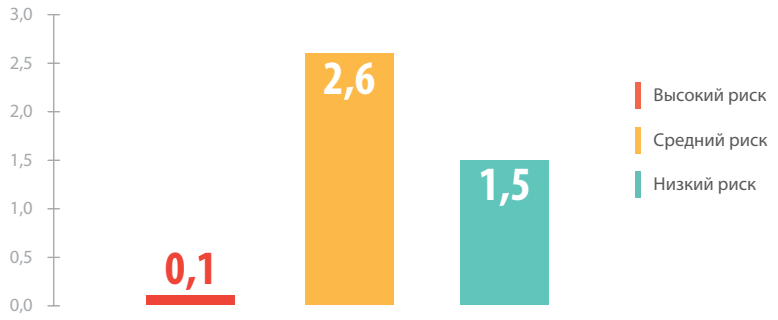

Рис. 42. Среднее количество уязвимостей конфигурации на одну систему

Наиболее распространенными уязвимостями данного типа являются:

- возможность идентификации программного обеспечения (подвержено 57% систем);
- возможность проведения атак на сессию (54% систем);
- небезопасная передача данных (46% систем).

Например, если для cookie-параметра, передающего идентификатор сессии, не устанавливается свойство secure, то браузер может передавать параметр не только по безопасному протоколу HTTPS, но и по протоколу HTTP. При использовании небезопасного протокола передачи данных, а также нестойких алгоритмов шифрования злоумышленник может перехватить пользовательские данные.

8.2. Недостатки конфигурации в системах собственной разработки и в системах, поставляемых вендорами

Для систем, предоставляемых вендорами, почти половина уязвимостей, связанных с недостатками конфигурации, имеет низкий уровень риска (46%). Уязвимости конфигурации высокой степени риска были выявлены только в системах собственной разработки.

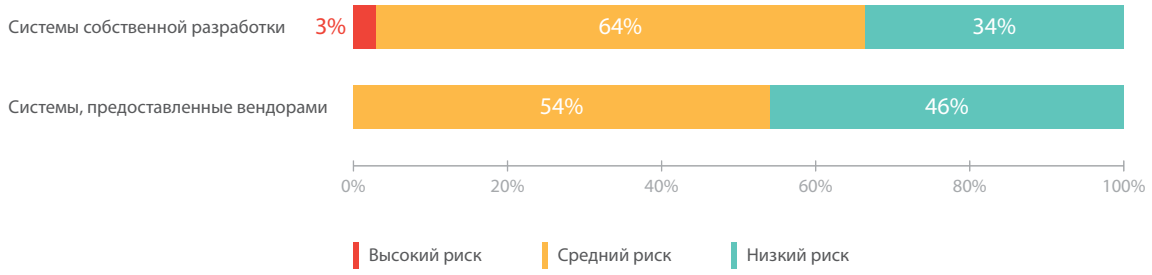

Рис. 43. Распределение недостатков конфигурации по уровням риска

На рис. 44 представлено среднее количество недостатков конфигурации различной степени риска на одну систему для различных категорий разработчиков. Для обоих типов систем это количество невелико, при этом в системах собственной разработки в среднем было выявлено больше уязвимостей.

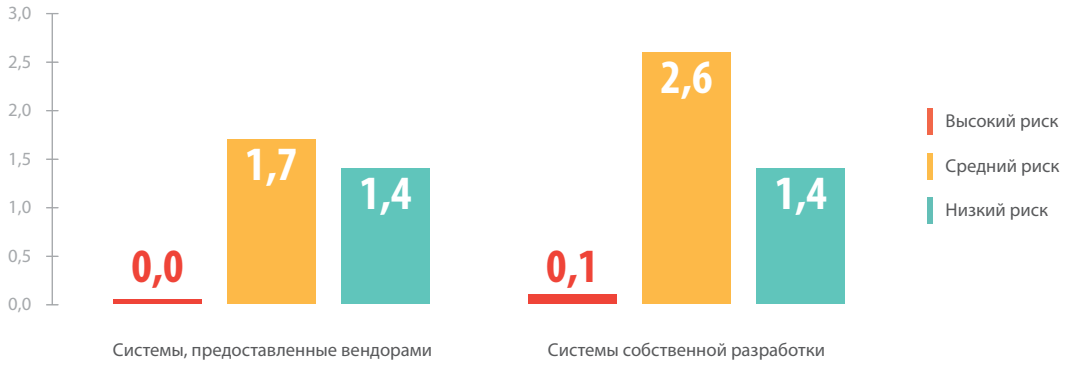

Рис. 44. Среднее число уязвимостей конфигурации на одну систему

9. Другие недостатки

Рассмотренные в рамках проведенного исследования системы ДБО содержат также ряд других существенных недостатков, в том числе недостатков на уровне логики системы.

К примеру, в ряде систем была обнаружена возможность проведения атак на алгоритмы округления. Вследствие некорректного использования алгоритмов округления чисел, злоумышленник может получить большую сумму денег, чем предусмотрено текущим обменным курсом валют.

Пример атаки:

- злоумышленник переводит 0,29 рубля в доллары США. При стоимости одного доллара США в 60 рублей, сумма в 0,29 рубля соответствует 0,00483333333333333333333333333333 доллара США. Такая сумма будет округлена до двух знаков после запятой, т. е. до 0,01 доллара, что соответствует одному центу США;
- злоумышленник переводит 0,01 доллара обратно в рубли. В результате перевода он получит 0,60 рубля. В результате данных операций злоумышленнику будет начислено на счет 0,31 рубля.

В результате автоматизации данной процедуры, с учетом отсутствия ограничений по количеству транзакций в сутки и минимальному размеру транзакции, а также возможности эксплуатации уязвимости типа Race Condition («Состояние гонки») — в ряде случаев злоумышленник мог получать неограниченные суммы денежных средств. Race Condition — атака, направленная на использование ошибок атомарности доступа к разделяемым данным, когда несколько процессов находятся в состоянии гонки (состязания) за один набор данных. Подобная атака позволяет обойти логику системы ДБО, предусмотренную разработчиком, и совершать различные неавторизованные действия, например проводить несколько транзакций по одному и тому же значению одноразового пароля. Такие уязвимости были обнаружены в 11% проанализированных систем.

В ряде систем ДБО не маскируются номера платежных карт (PAN). Данный недостаток является нарушением требований стандарта Payment Card Industry Data Security Standard (PCI DSS) и может быть использован злоумышленниками для реализации атак на пользователя. Отсутствие маскирования PAN было обнаружено в двух системах ДБО.

Атаки типа «Отказ в обслуживании» (DoS) являются одной из наиболее актуальных угроз безопасности. В случае систем ДБО данная атака может быть направлена на нарушение доступности как серверной части системы, так и личного кабинета пользователя. Отказ в обслуживании всей системы ДБО может быть вызван некорректной обработкой поступающих данных, а также может возникать в результате эксплуатации уязвимостей «Внедрение сущностей XML», «Внедрение операторов XPath» и др. Вызов отказа в обслуживании системы ДБО в целом был возможен в половине исследованных ресурсов (52%). С другой

стороны, используя предсказуемость формата идентификатора учетных записей, нарушитель способен осуществить блокировку учетных записей пользователей при многократном вводе неверных данных в поле пароля (данная уязвимость была обнаружена в 41% исследованных систем).

10. Уязвимости клиентского ПО мобильных систем ДБО

В данном разделе приведен обзор уязвимостей клиентского ПО мобильных систем ДБО на базе двух ОС — Android и iOS.

Клиентское ПО для ОС Android более уязвимо по сравнению с приложениями для iOS. В частности, 70% приложений для ОС Android содержат критические уязвимости, в то время как соответствующая доля мобильных систем на базе iOS составляет 50%.

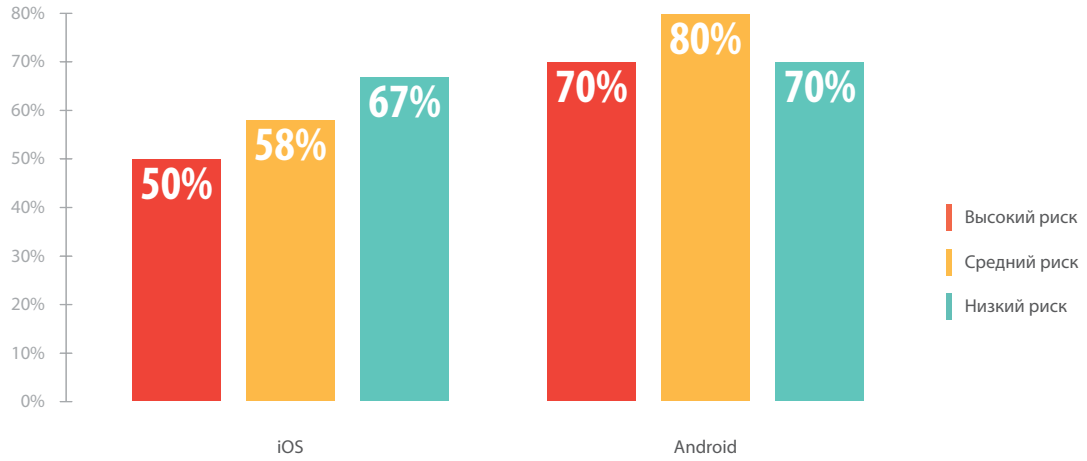

Рис. 45. Доли мобильных клиентов, подверженных уязвимостям различной риска

Большинство исследованных систем содержало уязвимости, при этом уязвимые мобильные системы ДБО на базе Android содержали недостатки как минимум среднего уровня риска. Распределение мобильных систем ДБО по максимальной степени риска обнаруженных уязвимостей представлено на рис. 46.

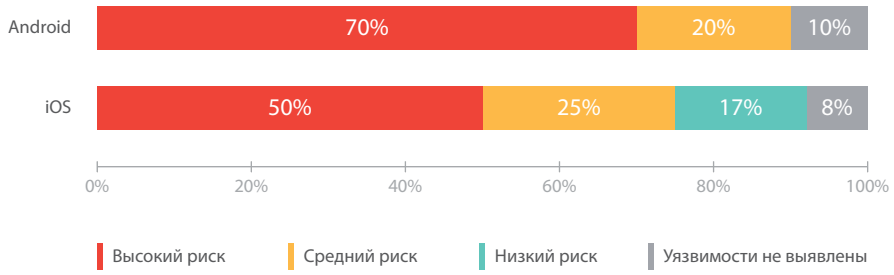

Рис. 46. Распределение мобильных систем по максимальной степени риска

В среднем каждое приложение на базе Android содержит 3,7 уязвимостей, в то время как для iOS-приложения данный показатель равен 2,3.

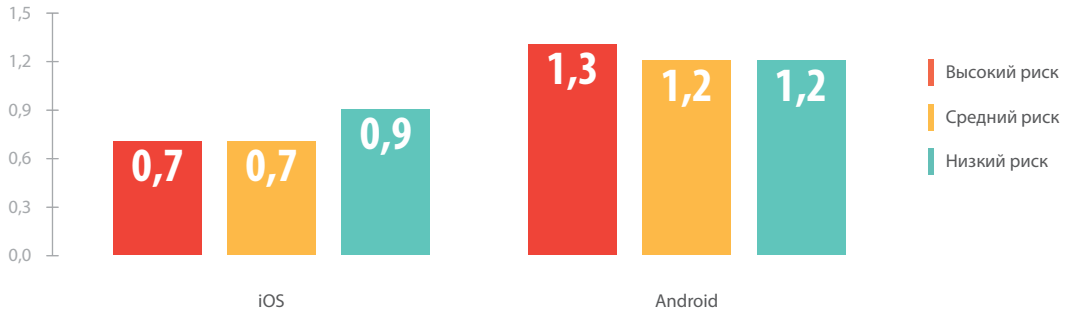

Рис. 47. Среднее количество уязвимостей различного уровня риска в клиентском ПО мобильных систем

Наиболее часто в мобильных системах ДБО встречались уязвимости, связанные с небезопасной передачей данных. Распространены также уязвимости, связанные с возможностью проведения атак на сессии пользователей, а также недостатки, обусловленные небезопасным хранением данных.

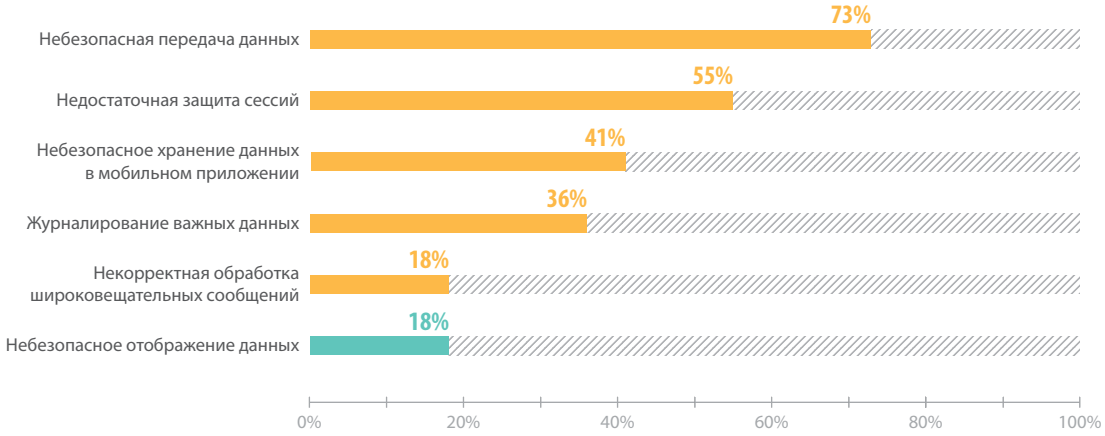

Рис. 48. Наиболее распространенные уязвимости клиентского ПО мобильных систем

Хотя наиболее распространенные уязвимости мобильных систем ДБО имеют среднюю или низкую степень риска, в ряде случаев в совокупности выявленные недостатки позволяли реализовать серьезные угрозы безопасности. Например, одно из исследованных приложений отправляло широковещательное сообщение, содержащее полученное от банка SMS-сообщение (включавшее том числе одноразовый пароль для проведения транзакции), которое могло быть перехвачено сторонним приложением. Кроме того, данное мобильное приложение осуществляло журналирование важных данных, таких как учетная запись пользователя, вследствие чего при успешном заражении устройства вредоносным кодом атакующий мог получить полный доступ к аутентификационным данным и проводить транзакции от лица пользователя мобильного приложения.

10.1. Небезопасная передача данных

Уязвимости мобильных приложений, связанные с небезопасной передачей данных, относятся к следующим основным категориям:

- передача данных по незащищенному протоколу HTTP (36% от общего числа систем);
- возможность добавления на устройстве пользователя самоподписанных сертификатов в список доверенных (7% систем);
- передача важных данных, например пароля пользователя, в открытом виде без использования хеширования (4% систем).

В результате эксплуатации указанных уязвимостей злоумышленник может получить доступ к важным данным, передаваемым приложением, таким как идентификаторы и пароли пользователей, геолокационные данные и к другой важной информации. Например, в случае если пользователь мобильной системы ДБО подключится к публичной беспроводной сети, атакующий может провести атаку типа «человек посередине» (man in the middle) и перехватить передаваемые в открытом виде данные. При автоматизации атаки злоумышленник может вмешаться в процесс проведения транзакций, подменяя реквизиты платежей в режиме реального времени.

Рекомендуется использовать защищенные протоколы передачи данных (SSL или TLS), а также использовать сертификаты, заверенные подписью удостоверяющего центра.

10.2. Недостаточная защита сессий

В исследованных мобильных системах ДБО было выявлено большое количество уязвимостей, позволяющих реализовать атаки на сессии пользователей:

- при выходе из учетной записи приложение не отправляет запрос к серверу для закрытия сессии (32% мобильных приложений);
- предсказуемый формат идентификатора сессии (9% приложений);
- для cookie-параметров не устанавливается свойство «secure», вследствие чего разрешается передавать идентификатор сессии по незащищенному протоколу HTTP (9% приложений);
- по умолчанию отключено автоматическое завершение сессии (5% приложений).

В ходе работ по анализу защищенности нескольких мобильных систем ДБО (9%) специалисты Positive Technologies обнаружили, что идентификаторы сессий представляли собой хеш пароля и криптографическую соль в открытом виде. Данный механизм аутентификации не обеспечивает должной защиты от несанкционированного доступа, поскольку злоумышленник может подобрать значение пароля по хеш-функции с помощью радужных таблиц. Таким образом, при отсутствии двухфакторной аутентификации атакующий мог получить доступ к личному кабинету пользователя и совершать транзакции от его имени.

10.3. Небезопасное хранение данных

Мобильные приложения хранят в файловой системе важные данные в открытом виде. Данная уязвимость была обнаружена в 41% исследованных приложений. К чувствительной информации относятся персональные данные клиентов, идентификаторы и пароли пользователей, идентификаторы сессий, отладочная информация. Кроме того, в ряде случаев (9%) данные записываются в файловую систему с правами не только на чтение, но и на запись, вследствие чего злоумышленник, используя вредоносное ПО, может подменить сохраненные данные произвольными.

Рекомендуется не сохранять важные данные в общедоступных каталогах или использовать шифрование при хранении чувствительной информации.

Заключение

По итогам проведенного исследования можно сделать вывод о том, что уровень защищенности систем ДБО на сегодняшний день остается низким. Уязвимыми являются как системы для юридических, так и для физических лиц, как платформы, поставляемые профессиональными вендорами, так и собственные разработки банков. Кроме того, ситуация с защищенностью систем ДБО, уже находящихся в эксплуатации, наглядно свидетельствует о необходимости внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений. Перед вводом системы ДБО в эксплуатацию необходимо проводить анализ ее защищенности, вне зависимости от разработчика.

Недостатки механизмов аутентификации и авторизации могут привести к реализации различных угроз безопасности вплоть до несанкционированного проведения транзакций и получения полного контроля над системой ДБО. В связи с этим следует уделять особое внимание корректной реализации механизмов защиты, а также обеспечивать контроль качества кода веб-приложения.

Для того чтобы снизить риски, связанные с уязвимостями в системах ДБО, следует внедрять процессы безопасной разработки, обеспечивать всестороннее тестирование безопасности систем при приемке работ, а также использовать средства превентивной защиты типа web application firewall. В частности, для продуктивных систем, приобретаемых у вендоров, межсетевой экран уровня приложения рекомендуется использовать во избежание эксплуатации уязвимостей до выпуска обновления. В качестве основы для внедрения процессов обеспечения информационной безопасности систем ДБО на всех стадиях жизненного цикла могут быть использованы выпущенные в 2014 году РС БР ИББС-2.6-2014 («Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»).

Регулярный и всесторонний контроль защищенности систем ДБО позволит снизить риски реализации угроз безопасности и избежать финансовых и репутационных потерь.

О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована ФСТЭК и ФСБ, продукция сертифицирована Газпромсерт, Минобороны РФ и ФСТЭК. Более 1000 организаций из 30 стран мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, выполнения требований регуляторов и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня по вопросам защиты SCADA- и ERP-систем, крупнейших банков и телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности, а также стала лидером по темпам роста на международном рынке систем управления уязвимостями, согласно исследованиям IDC. Подробнее о компании — на сайте www.ptsecurity.ru

* Отчет IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares (№ 242465), опубликованный в августе 2013 года и основанный на данных о выручке от продаж в 2012 году (для вендоров с выручкой больше 20 млн долл. США).

POSITIVE TECHNOLOGIES

PT-DBO_DS_A4.RUS.0001.01.NOV.05.2015