УЯЗВИМОСТИ ПРИЛОЖЕНИЙ ФИНАНСОВОЙ ОТРАСЛИ

2016

POSITIVE TECHNOLOGIES

Оглавление

Введение

Банки стремятся использовать передовые технологии, чтобы дать своим клиентам возможность удаленно управлять банковскими продуктами. Для получения большинства банковских услуг достаточно оформить карту банка и заключить договор о дистанционном банковском обслуживании (ДБО). Все чаще появляются банки, которые вовсе не предлагают клиентам привычное обслуживание в территориально распределенных филиалах, а оказывают полный спектр услуг удаленно. У такого подхода множество преимуществ: для пользователей это, прежде всего, удобство и скорость получения услуги; для банка — сокращение затрат на содержание филиалов, сокращение штата. Решается проблема очередей, бюрократических проволочек — и, как следствие, сокращается количество недовольных клиентов.

Однако существует и обратная сторона медали — необходимость обеспечивать безопасность и минимизировать риски, связанные с использованием систем ДБО. Это общедоступные веб- и мобильные приложения, и для них характерны все соответствующие уязвимости и угрозы информационной безопасности (в частности, рассматриваемые в классификации Web Application Security Consortium Threat Classification — WASC TC v. 2). К примеру, наиболее опасной угрозой в случае реализации атак на системы ДБО можно назвать хищение денежных средств. Также среди специфических угроз можно выделить несанкционированный доступ к данным платежных карт, персональным данным пользователей и банковской тайне, отказ в обслуживании банковского приложения; есть и другие угрозы, реализация которых может привести к существенным финансовым и репутационным потерям.

Данный отчет содержит статистику, собранную в ходе работ по анализу защищенности систем дистанционного банковского обслуживания, проведенных специалистами компании Positive Technologies в 2015 году. В рамках исследования представлен также сравнительный анализ данных, полученных в 2015 году, с результатами аналогичных исследований 2014 и 2013 годов. Это дает возможность оценить динамику развития современных систем ДБО с точки зрения обеспечения информационной безопасности.

1. Резюме

Все системы ДБО уязвимы

Хотя критически опасных уязвимостей в системах ДБО становится меньше, они по-прежнему встречаются практически в каждом интернет-банкинге. Лишь в 10% систем ДБО не было обнаружено таких недостатков (при этом в них были выявлены как минимум уязвимости средней степени риска).

В половине исследованных систем ДБО (55%) нарушитель может получить контроль над СУБД и доступ к банковской тайне; в каждой четвертой системе — украсть денежные средства банка, обладая пользовательским доступом к клиентскому приложению, и еще в 5% случаев — сделать то же без каких-либо привилегий. Нарушитель может полностью вывести из строя систему ДБО, используя контроль над ОС сервера и другие уязвимости (40% систем).

Покупная система ДБО не дает гарантии защиты

По сравнению с предыдущими годами количество уязвимостей высокой степени риска в системах ДБО, приобретенных у вендоров, снизилось практически вдвое. Однако все такие продукты по-прежнему подвержены критически опасным уязвимостям (например, «Внедрению операторов SQL» и «Внедрению внешних сущностей XML»). Кроме того, системы ДБО, поставляемые специализированными компаниями, в среднем содержат в 1,5—2 раза больше уязвимостей, чем системы собственной разработки.

Введенные в эксплуатацию системы не менее уязвимы, чем тестовые

В каждой системе ДБО, находящейся на стадии разработки, существенно больше уязвимостей, чем в продуктивных системах (в основном это недостатки среднего и низкого уровня опасности). Однако почти половина всех уязвимостей систем ДБО, уже находящихся в эксплуатации, — критически опасные (40%). По этому показателю они даже хуже тестовых.

Проблемы реализации механизмов защиты по-прежнему актуальны

Предсказуемый формат идентификаторов характерен для всех систем ДБО, при этом возможность сменить идентификатор есть только у пользователей 60% систем.

Двухфакторная аутентификация при входе в личный кабинет и проведении транзакций позволяет существенно снизить риски хищения денежных средств со счетов пользователей, однако по-прежнему велика доля систем ДБО, где такие механизмы не предусмотрены вовсе (24%) либо реализованы некорректно (29%). Уязвима почти каждая вторая система собственной разработки (45%), и даже в системах ДБО, купленных у вендоров, довольно часто встречаются такие недостатки (33%).

Кроме того, каждая третья система ДБО (35%) не обеспечивает достаточную защиту сессии от перехвата и последующего использования злоумышленником.

Системы для iOS тоже уязвимы

Треть уязвимостей, обнаруженных в мобильных системах ДБО для iOS, характеризуются высокой степенью риска. Эти недостатки связаны с хранением и передачей важных данных в открытом виде. Аналогичные уязвимости были обнаружены и в системах ДБО под Android.

Мобильные системы ДБО, созданные для работы под управлением iOS, по-прежнему обладают более высоким уровнем защищенности, чем Android-системы (там 75% систем подвержены критически опасным уязвимостям!), однако гарантировать безопасность их использования уже не приходится.

2. Исходные данные

В рамках проведенного исследования было рассмотрено 20 систем ДБО, анализ защищенности которых проводился специалистами Positive Technologies в 2015 году. Вошли в исследование также несколько финансовых сервисов, разработанных на языке 1С, в отношении которых проводились аналогичные работы и для которых характерны те же угрозы ИБ, что и для систем дистанционного банковского обслуживания. В обзор вошли только те системы, для которых проводился наиболее полный анализ с учетом логики их функционирования. Так, не рассматриваются системы на стадии разработки, для которых проводился только поиск уязвимостей на уровне кода веб-приложения без анализа возможностей несанкционированного проведения транзакций.

Большинство исследованных систем предназначены для обслуживания физических лиц (75%).

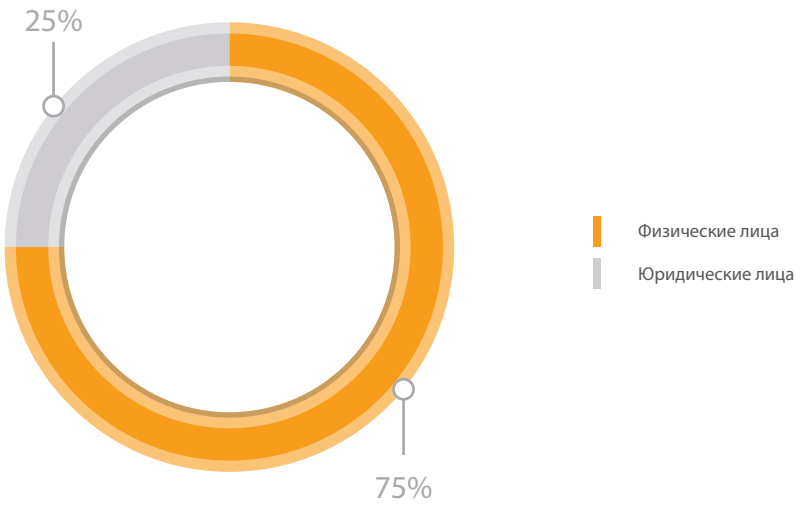

Рис. 1. Системы ДБО по сферам обслуживания клиентов

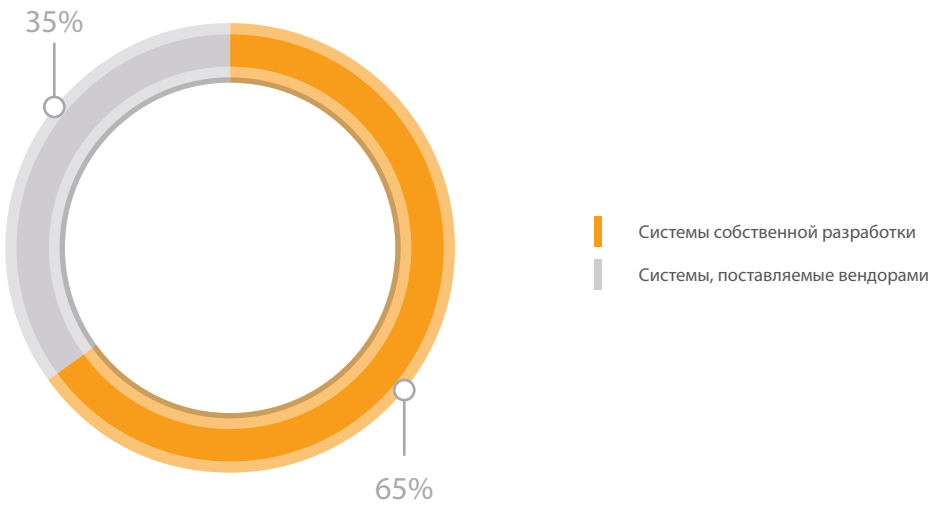

Рис. 2. Типы систем

Две трети исследованных систем ДБО (65%) представляли собой приложения собственной разработки банков. Остальные системы были развернуты 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 собственной разработки банков в подавляющем большинстве случаев использовался язык программирования Java и лишь в 8% систем — технология 1С.

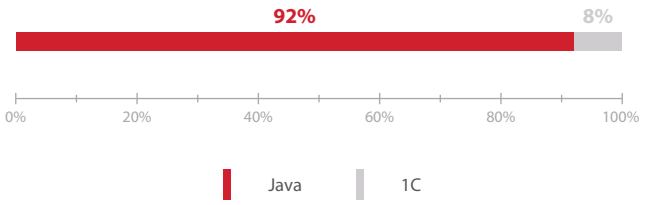

Рис. 3. Средства разработки систем ДБО

В состав исследуемых систем ДБО вошли мобильные системы, представленные серверной и клиентской частью, доля которых составила 35%.

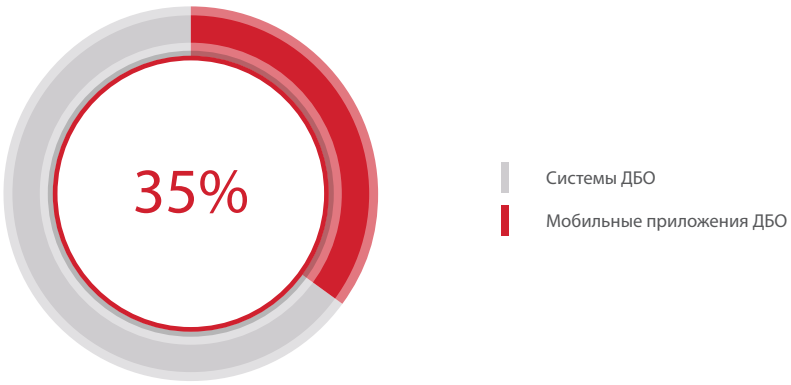

Рис. 4. Доля мобильных приложений среди всех систем ДБО

Анализируемые системы находились на различных стадиях разработки. Большинство были в промышленной эксплуатации, доступны для клиентов (75%). Четверть ресурсов представляли собой тестовые стенды, готовые к переводу в промышленную эксплуатацию.

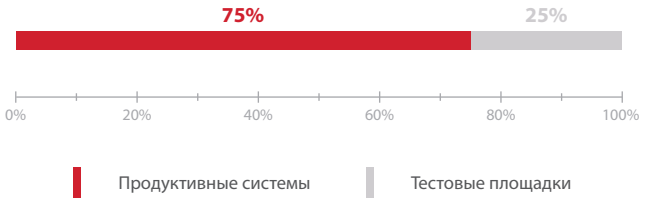

Рис. 5. Соотношение продуктивных и тестовых систем ДБО

Больше половины вендорских систем ДБО находились в промышленной эксплуатации (57%).

3. Общие результаты работ

3.1. Распространенные уязвимости и связанные с ними угрозы

В ходе анализа защищенности систем ДБО в каждом из приложений были выявлены недостатки безопасности. В общей сложности была выявлена 171 уязвимость. Большая часть из них характеризуются низкой степенью риска (39%). Доля уязвимостей высокой степени риска в этом году составила 30%, примерно столько же — средней (31%). В сравнении с результатами 2013—2014 годов доля критически опасных уязвимостей заметно снизилась (на 14%); это положительная тенденция, однако при детальном рассмотрении оказывается, что уровень защищенности систем ДБО в целом остается довольно низким.

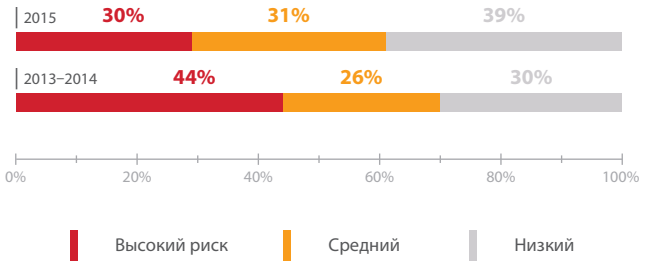

Рис. 6. Уязвимости различной степени риска

В отличие от прошлых лет все исследованные системы ДБО содержали по меньшей мере недостатки среднего уровня риска, при этом практически в каждой из систем (90%) были обнаружены критически опасные уязвимости, что значительно хуже показателей 2013–2014 годов.

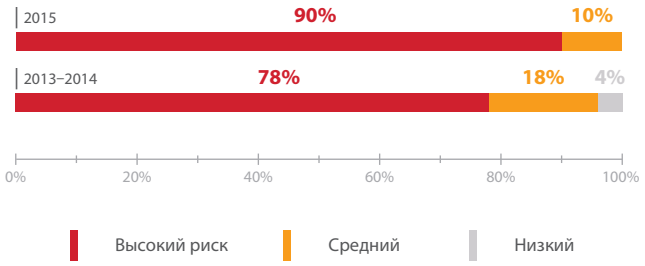

Рис. 7. Доли систем по максимальной степени риска уязвимостей

Распределение уязвимостей по категориям практически совпадает с результатами предыдущих лет: большая часть уязвимостей (36%) связана с ошибками в реализации механизмов защиты, заложенных разработчиками (в 2013–2014 годах их доля составляла 42%). К этой категории относятся, в частности, недостатки механизмов идентификации, аутентификации и авторизации. Не изменилась в 2015 году доля уязвимостей, связанных с ошибками в коде приложений, таких как «Внедрение внешних сущностей XML», «Межсайтовое выполнение сценариев» (в 2013–2014 годах она составляла 36%). Прочие уязвимости систем ДБО связаны с недостатками конфигурации (ранее их доля составляла 22%, теперь 27%).

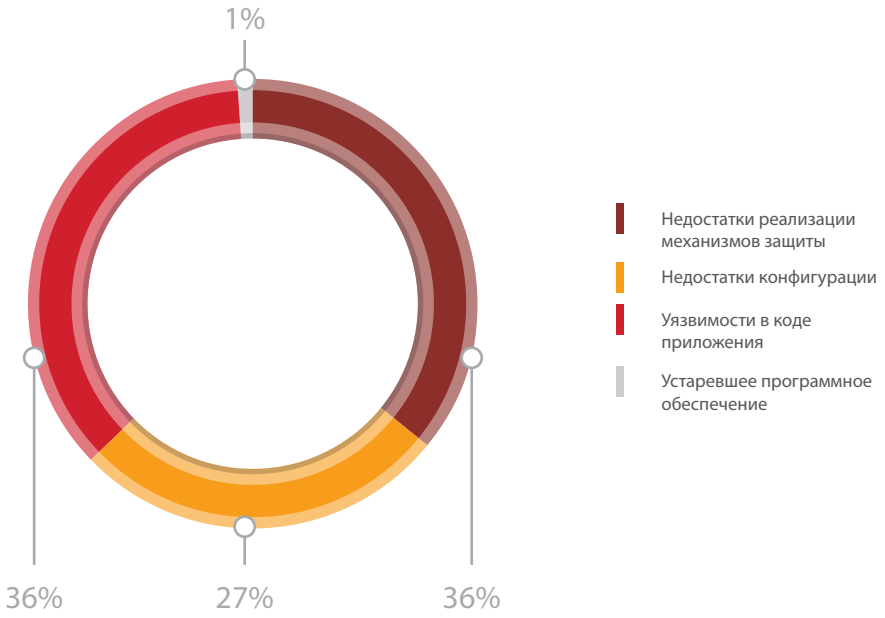

Рис. 8. Уязвимости по категориям

В отличие от предыдущих лет в двух исследованных системах ДБО была выявлена уязвимость, связанная с отсутствием актуальных обновлений безопасности (CVE-2015-1635). Эта уязвимость возникла из-за ошибок в компоненте HTTP.sys, реализующем стек протокола HTTP, и ей подвержены ОС семейства Windows. Подробнее уязвимость описана в бюллетене безопасности компании Microsoft MS15-034, опубликованном 14 апреля 2015 года. Эксплуатация уязвимости осуществляется при помощи специального HTTP-запроса и может привести к отказу в обслуживании атакуемой системы или выполнению произвольного кода.

Важно отметить, что столь малая доля систем ДБО, подверженных уязвимостям данной категории, не означает, что для всех остальных исследованных систем осуществлялась своевременная установка обновлений. Для большинства систем анализ защищенности проводился с использованием методов черного и серого ящика, то есть с привилегиями, идентичными привилегиям потенциального злоумышленника. Это означает, что в действительности в системах ДБО могли присутствовать устаревшие версии ПО.

Наиболее часто в системах ДБО встречались уязвимости, позволяющие получить несанкционированный доступ к данным пользователей. К этой категории в основном относятся недостатки авторизации. Таким критически опасным недостаткам подвержены более половины исследованных систем ДБО (55%). Это говорит о недостаточном внимании разработчиков к вопросам реализации механизмов защиты.

На втором месте по распространенности (50%) оказалась уязвимость среднего уровня риска «Недостаточная защита сессии». Сюда относятся некорректное завершение сессий пользователей, некорректная настройка cookie-параметров, возможность параллельной работы с несколькими активными сессиями для одного пользователя, отсутствие привязки сессии к IP-адресу клиента и другие недостатки.

На третьей строчке рейтинга расположился недостаток низкой степени опасности «Идентификация приложений», доля уязвимых систем составила 40% (на 17% ниже, чем в прошлые годы). Стоит отметить, что прежде первые строчки рейтинга занимали именно уязвимости низкого уровня риска.

Четвертую и пятую строчки рейтинга заняли критически опасная уязвимость «Внедрение внешних сущностей XML» и уязвимость среднего уровня риска «Межсайтовое выполнение сценариев».

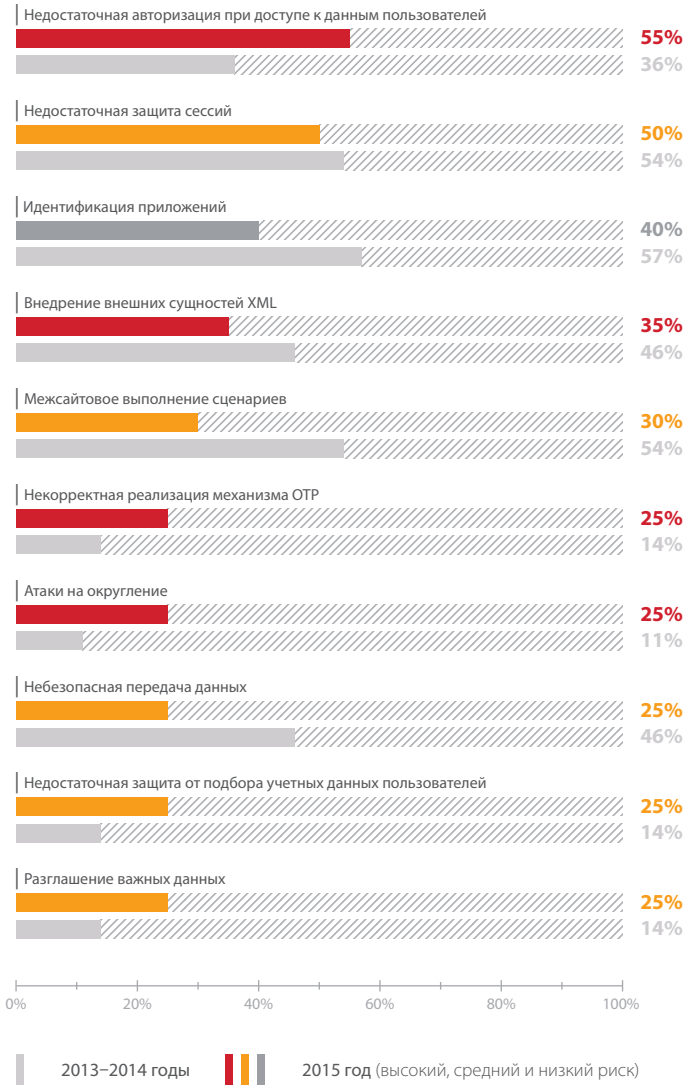

Рис. 9. Наиболее распространенные уязвимости систем ДБО (доля уязвимых систем)

Совокупность различных уязвимостей, выявленных в ходе анализа защищенности, потенциально может привести к реализации ряда угроз информационной безопасности. В рамках исследования были выделены наиболее опасные угрозы, которые могли быть реализованы в отношении систем ДБО.

В 5% исследованных систем ДБО была выявлена возможность хищения денежных средств пользователя в результате эксплуатации внешним нарушителем комбинации уязвимостей различных категорий (недостаточной защиты сессии и недостатков реализации механизмов двухфакторной аутентификации). В отношении 25% исследованных систем ДБО могут быть реализованы серьезные угрозы безопасности, такие как кража денежных средств со стороны авторизованного пользователя. Нарушитель может использовать, в частности, атаки на округление, несанкционированный доступ к операциям другого

пользователя, а в некоторых случаях внедрение операторов SQL. В результате подобных действий нарушителя банки могут понести существенные финансовые и репутационные потери. Кроме того, в 10% случаев возможен доступ к ОС сервера системы ДБО. В каждом втором проекте (55%) была выявлена возможность осуществления несанкционированного доступа к СУБД, в которых хранятся важные данные (персональные данные пользователей, данные платежных карт, финансовая информация).

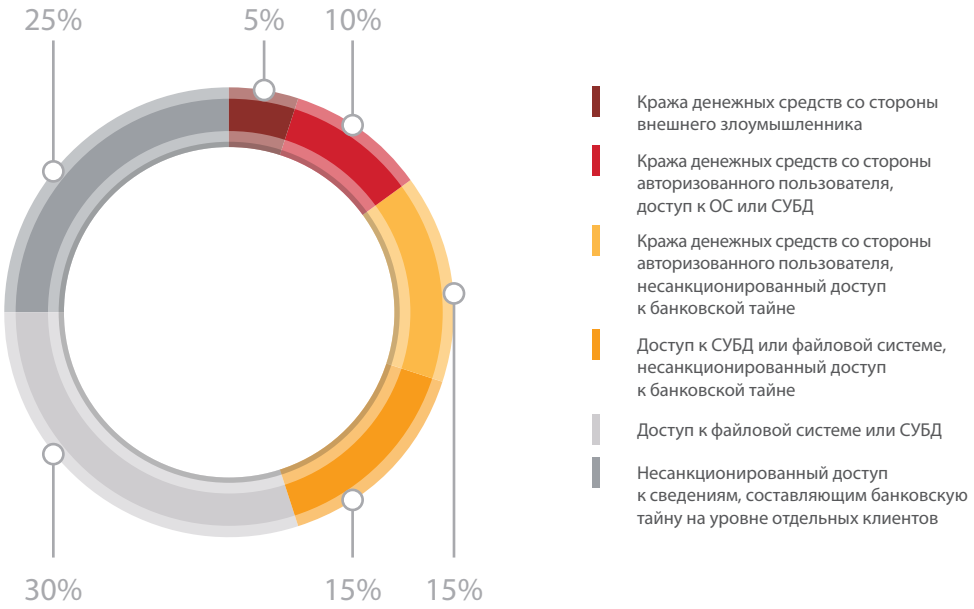

Рис. 10. Угрозы информационной безопасности систем ДБО (доли систем)

Важно отметить, что уязвимыми являются как системы собственной разработки банков, так и системы, приобретенные у крупных вендоров. Кроме того, возможность реализации названных угроз обнаружена в различных системах ДБО вне зависимости от стадии их разработки (продуктивные уязвимы не меньше тестовых).

3.2. Уязвимости систем ДБО для физических и юридических лиц

Для обоих типов систем доля недостатков реализации механизмов защиты относительно невелика: они обнаружены в каждой третьей системе. При этом выявлена тенденция к снижению доли систем для юридических лиц с такими недостатками (с 47 до 31%).

Доли различных систем ДБО, в которых выявлены уязвимости двух других категорий, заметно различаются. Недостатки конфигурации в два раза чаще встречались в системах для физических лиц, при этом уязвимости в коде приложений встречались в таких системах вдвое реже. Использование устаревших версий ПО было выявлено только в системах для юридических лиц.

По сравнению с результатами 2013–2014 годов наблюдается существенное увеличение доли ресурсов, в которых выявлены те или иные недостатки конфигурации систем ДБО для физических лиц (с 22 до 38%).

Рис. 11. Уязвимости различных категорий в системах для физических и юридических лиц (доли систем)

Доли уязвимостей различных уровней риска в системах для физических и юридических лиц отличаются незначительно (см. рис. 12). Заметно снижение доли критически опасных уязвимостей в сравнении с предыдущими годами (на 19% для юридических и на 12% для физических лиц). Возросли, соответственно, доли недостатков среднего и низкого уровней риска.

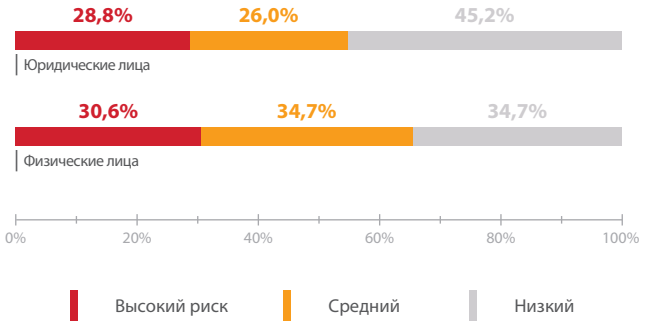

Рис. 12. Степень риска уязвимостей (системы для физических и юридических лиц)

Рис. 13. Максимальная степень риска уязвимостей (доля уязвимых систем)

Тенденция свидетельствует о некотором улучшении безопасности систем ДБО, однако общая защищенность все равно остается на довольно низком уровне. Все исследованные ресурсы содержат уязвимости, при этом все без исключения системы ДБО для

юридических лиц подвержены критически опасным уязвимостям. (Аналогичные результаты были получены и в предыдущие годы.) Все системы ДБО для физических лиц подвержены уязвимостям как минимум среднего уровня риска.

В системах ДБО для юридических лиц в 2015 году доли критически опасных уязвимостей и недостатков низкой степени опасности практически не изменились, при этом количество уязвимостей средней степени риска на одну систему возросло в несколько раз.

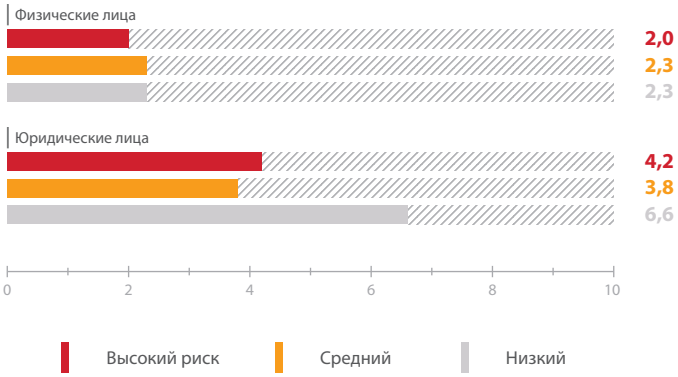

Рис. 14. Среднее количество уязвимостей различного уровня риска на одну систему

Полученные результаты свидетельствуют о том, что уровень защищенности систем ДБО для юридических лиц существенно снизился; в системах для физических лиц он понизился лишь незначительно в каждой категории, а в целом остался на том же, довольно низком, уровне.

3.3. Уязвимости систем ДБО для систем собственной разработки и систем от профессиональных вендоров

В системах, приобретенных банками у известных вендоров, доля уязвимостей, связанных с ошибками в программном коде, оказалась выше, чем в системах собственной разработки банков (40% против 28%). В то же время в системах собственной разработки был выявлен больший процент уязвимостей конфигурации по сравнению с платформами, поставляемыми вендорами (35% против 27%). Доли уязвимостей, связанных с недостатками реализации механизмов защиты в системах собственной разработки и в системах вендоров различаются незначительно.

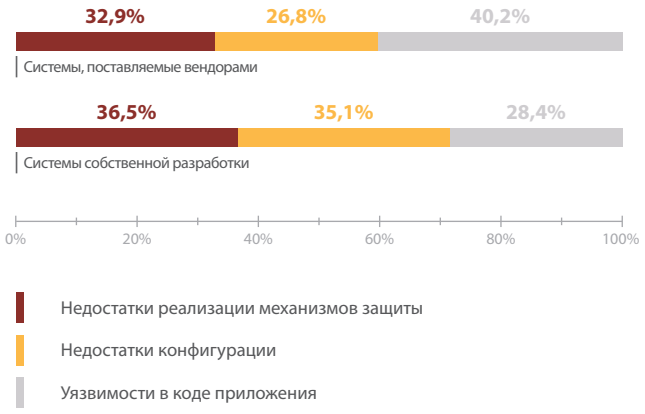

Рис. 15. Доли различных типов уязвимостей в системах разных разработчиков

Упомянутая ранее уязвимость MS15-034, связанная с отсутствием актуальных обновлений безопасности Windows, была выявлена в тех проектах, где рассматривались вендорские системы. Было принято решение не учитывать данную уязвимость в отчете, так как этот недостаток не может быть отнесен непосредственно к предоставленному вендором ПО.

Важно отметить, что в сравнении с результатами прошлых лет почти в два раза возросла доля систем ДБО, поставляемых вендорами, в которых обнаружены недостатки конфигурации (с 14 до 27%). В других категориях уязвимостей столь значимых изменений не отмечено. Что касается систем ДБО собственной разработки банков, доля систем с ошибками в коде осталась на прежнем уровне, другие показатели изменились незначительно. В целом уровень защищенности систем обоих типов остается низким.

Важно отметить общее снижение количества уязвимостей, приходящихся в среднем на одну систему. При этом прослеживается тенденция к выявлению большего числа уязвимостей именно в системах, разработанных вендорами. Банки уделяют больше внимания безопасности своих собственных продуктов в процессе разработки, продукты вендоров более уязвимы.

На каждую систему, разработанную известным вендором, в среднем приходится примерно в полтора-два раза больше ошибок. Эта тенденция была отмечена во все предыдущие периоды исследований и объясняется тем, что при использовании системы ДБО, поставляемой вендором, банк в вопросах контроля качества кода полагается в основном на поставщика. При этом сложная архитектура, кроссплатформенность и большое количество функций таких систем не всегда позволяют вендору обеспечить должный уровень защищенности на уровне кода приложения.

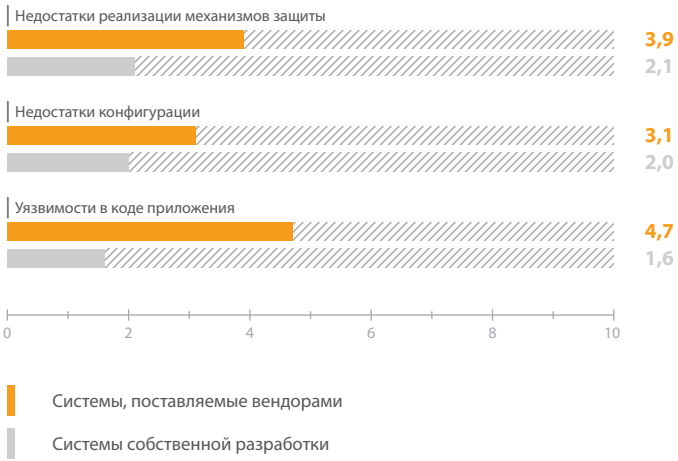

Рис. 16. Среднее количество уязвимостей в системах ДБО

В системах, поставляемых вендорами, 27% выявленных уязвимостей характеризуются высокой степенью риска. Каждая третья система ДБО собственной разработки также содержит критически опасные уязвимости. В целом соотношение недостатков всех уровней риска для систем двух типов различается незначительно. По сравнению с показателями прошлых лет наблюдается тенденция к существенному снижению доли критически опасных уязвимостей, особенно для систем ДБО от вендоров, где доля таких недостатков уменьшилась практически вдвое.

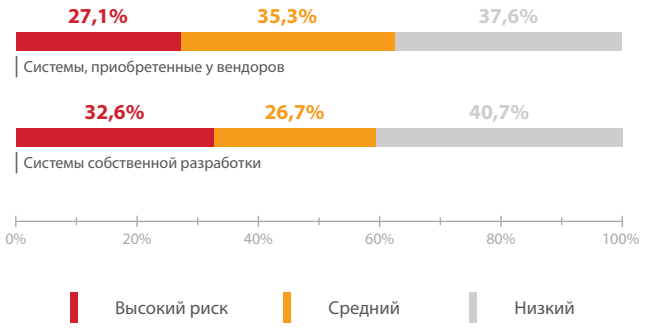

Рис. 17. Степень риска уязвимостей (доли от общего числа)

При наблюдаемом снижении доли критически опасных уязвимостей относительно общего их числа такие недостатки были выявлены абсолютно во всех исследованных системах ДБО, приобретаемых банками у профессиональных вендоров. Данные показатели значительно хуже результатов предыдущего периода исследования, когда в 17% систем ДБО от вендоров не было обнаружено уязвимостей высокой степени риска, а в 6% таких систем и вовсе были выявлены лишь незначительные недостатки. Результаты, полученные в 2015 году для систем собственной разработки, отличаются от данных предыдущих лет незначительно.

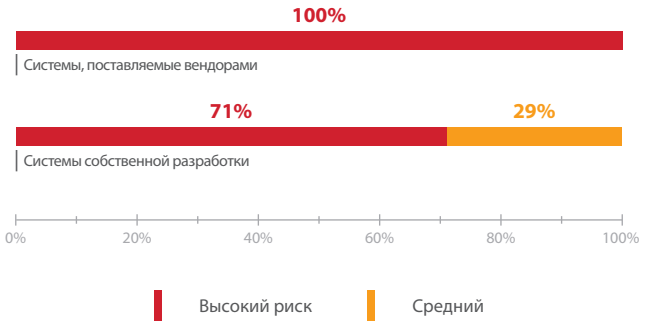

Рис. 18. Доли систем ДБО по максимальной степени риска уязвимостей

На каждую систему, приобретенную у вендора, в среднем приходится 3,3 критически опасной уязвимости, что в 3 раза лучше соответственного значения, полученного в прошлые годы. Для систем собственной разработки данный показатель составляет 2,2 уязвимости, что также меньше показателей за предыдущий период примерно в 3 раза (см. рис. 19).

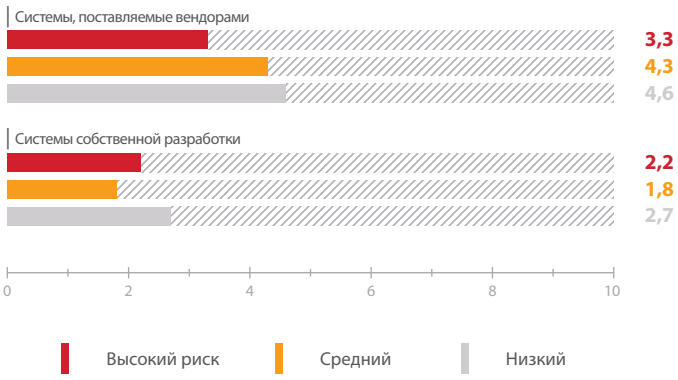

Рис. 19. Среднее количество уязвимостей в системах разных разработчиков

В целом каждая система ДБО, разработанная вендорами, в среднем содержит больше уязвимостей, чем в среднем одно приложение собственной разработки банков, поскольку собственные системы проектируются под конкретную архитектуру и имеют заведомо предусмотренные функции, что делает их более простыми и, следовательно, менее уязвимыми.

Опираясь на полученные результаты, мы не можем уверенно утверждать, что все системы всех вендоров сегодня так же уязвимы, как рассмотренные в рамках исследования. Однако полученные нами данные в любом случае показывают, что приобретение системы ДБО у профессионального вендора не гарантирует высокого уровня защищенности. Переход от систем известных вендоров к собственной разработке тоже не дает, впрочем, подобных гарантий.

Вендоры постоянно ведут работу по устранению уязвимостей, выявленных в результате работ по анализу защищенности, и выпускают соответствующие обновления. Чтобы обезопасить продуктивные системы ДБО от эксплуатации уязвимостей до выпуска исправлений вендором, — а также в случае использования собственных систем, — рекомендуется использовать превентивные средства защиты — межсетевые экраны уровня приложения (web application firewalls). Помимо того, рекомендуется проводить анализ защищенности систем ДБО до ввода их в эксплуатацию на каждом этапе разработки — с обеспечением контроля исправления выявленных уязвимостей. Также необходимо регулярно (к примеру, дважды в год) тестировать систему в ходе эксплуатации — вне зависимости от того, кто ее разработал.

3.4. Уязвимости тестовых и продуктивных систем ДБО

В данном разделе приведены результаты исследования уровня защищенности тестовых систем ДБО и систем ДБО, уже находящихся в эксплуатации. Для тестовых систем доли уязвимостей, возникших вследствие недостатков реализации механизмов защиты и некорректной конфигурации, оказались выше, чем доля ошибок в коде приложений.

В предыдущие годы в каждой второй системе, находящейся на этапе разработки (49%), были выявлены недостатки реализации механизмов защиты. Что касается продуктивных систем ДБО, в 2013–2014 годах в них также были распространены именно эти недостатки (41%).

Описанная выше уязвимость MS15-034 была выявлена в системах ДБО, находящихся на этапе разработки.

Рис. 20. Доли различных категорий уязвимостей

Количество уязвимостей различных категорий, приходящихся в среднем на одну тестовую систему, существенно выше аналогичных показателей для продуктивных систем ДБО. Это понятно, так как в процессе создания приложения могут быть допущены ошибки, которые будут исправляться на последующих этапах работы. Анализ защищенности в отношении этих систем проводится, среди прочего, именно с целью выявления таких ошибок.

Важно отметить, что количество недостатков конфигурации и реализации механизмов защиты для тестовых систем осталось примерно на том же уровне, что и в прошлые годы. Ошибок кода приложения в тестовых системах в 2015 году вдвое больше, чем в 2013–2014 годах, а в продуктивных системах, наоборот, меньше в 5 раз. Это говорит о том, что банки стали уделять больше внимания защищенности тех программных продуктов, которые предлагают своим пользователям.

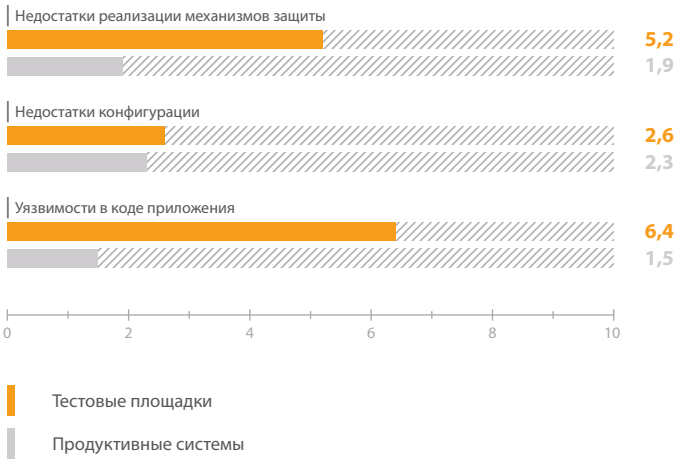

Рис. 21. Среднее количество уязвимостей различного вида в тестовых и продуктивных системах

Однако делать положительные выводы о защищенности систем ДБО, находящихся в эксплуатации, рано, так как уровень опасности выявленных в таких системах уязвимостей по-прежнему высокий. Доля критически опасных уязвимостей в продуктивных системах существенно превышает соответствующий показатель для тестовых.

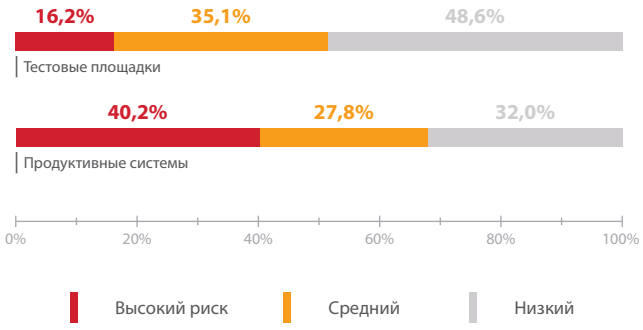

Рис. 22. Соотношение уязвимостей различного уровня риска в тестовых и продуктивных системах (доля от общего количества уязвимостей)

Доли уязвимостей всех уровней риска в системах ДБО, находящихся в эксплуатации, остались на прежнем уровне. Ситуация же в части тестовых систем значительно изменилась: доля критически опасных уязвимостей снизилась более чем в два раза. Столь большое

число уязвимостей, приходящихся в среднем на каждую из тестовых систем, объясняется, таким образом, именно широкой распространенностью уязвимостей низкого и среднего уровней риска.

Все исследованные системы ДБО содержали уязвимости как минимум средней степени риска. Практически все продуктивные приложения были подвержены критически опасным уязвимостям (см. рис 23). Такие результаты свидетельствуют о необходимости внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений (secure systems development life cycle), а также о необходимости регулярных проверок уровня защищенности систем, находящихся в эксплуатации.

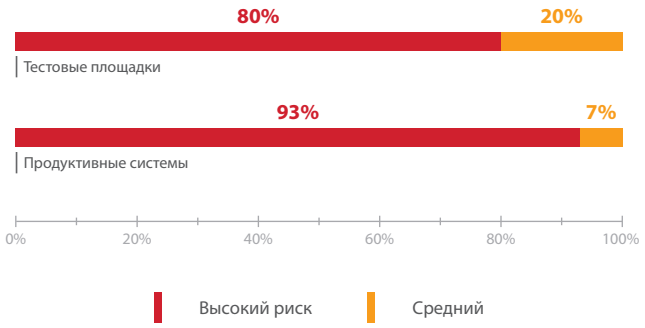

Рис. 23. Распределение тестовых и продуктивных систем по максимальной степени риска уязвимостей (доля уязвимых систем)

Предположение о распространенности уязвимостей низкого и среднего уровней риска в системах, находящихся на стадии разработки, подтверждается. Количество таких недостатков в тестовых системах ДБО в несколько раз выше, чем критически опасных уязвимостей. При этом количество уязвимостей высокого уровня риска, приходящееся в среднем на одну тестовую систему, находится примерно на том же уровне, что и в продуктивных системах.

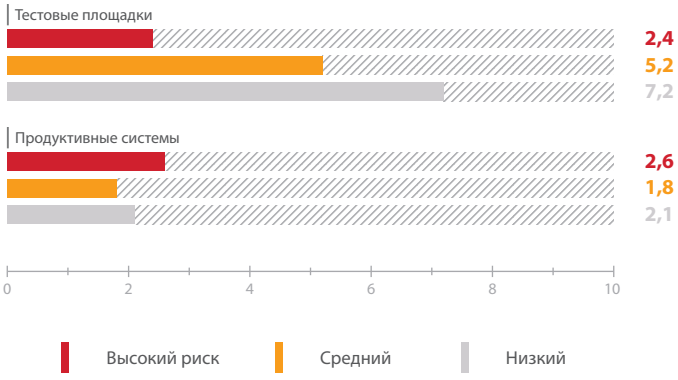

Рис. 24. Среднее количество уязвимостей различного уровня риска в тестовых и продуктивных системах

Результаты исследования свидетельствуют, что количество уязвимостей в продуктивных системах в 2015 году заметно ниже, чем в тестовых. Это свидетельствует о том, что работа банков по обеспечению защиты приложений, находящихся в эксплуатации, дает результат. Тем не менее уровень защищенности систем ДБО нельзя назвать высоким, поскольку практически во всех системах были выявлены критически опасные уязвимости.

4. Обзор критически опасных уязвимостей

В данном разделе приведен обзор уязвимостей высокой степени риска, которые были обнаружены в большинстве рассмотренных систем ДБО.

Уязвимости «Недостаточная авторизация при доступе к данным пользователей» и «Внедрение внешних сущностей XML» по-прежнему распространены в системах ДБО. По сравнению с прошлыми годами значительно снизилась доля систем с ошибками в коде веб-приложений, которые позволяют осуществлять внедрение операторов SQL. При этом доля систем ДБО, уязвимых к внедрению произвольного кода, а также к атакам на округление, существенно возросла. В результате эксплуатации таких уязвимостей нарушитель может получить полный контроль над сервером приложения (в результате внедрения кода), а также осуществлять хищение денежных средств банка (в результате атак на логику приложения).

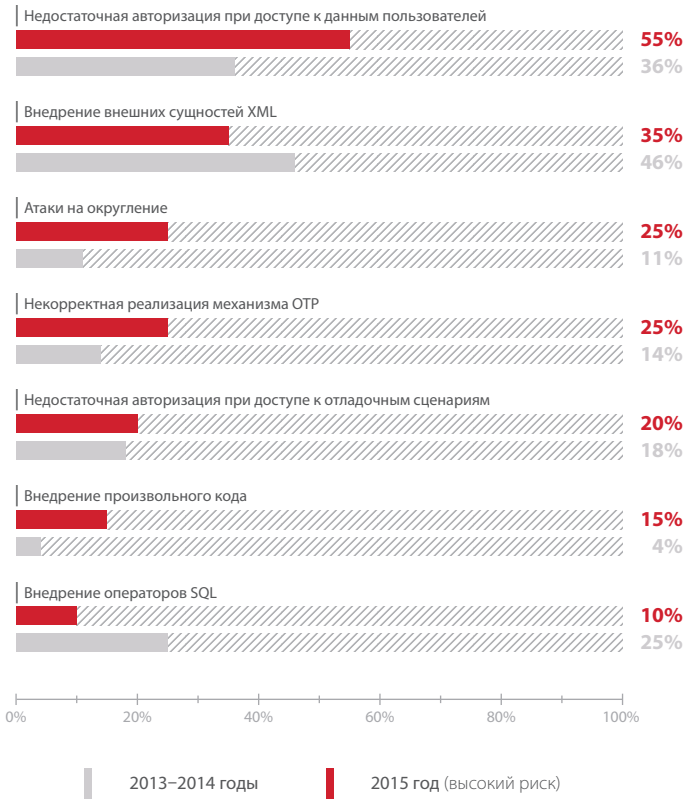

Рис. 25. Наиболее распространенные критически опасные уязвимости систем ДБО

Чаще стали встречаться критически опасные уязвимости, связанные с некорректной реализацией механизма OTP (one-time password), например в тех случаях, когда при изменении реквизитов шаблона не требуется подтверждение с помощью одноразового пароля (злоумышленник может воспользоваться действующей сессией и похитить денежные средства при наличии у атакуемого пользователя подходящего шаблона) или когда с помощью одного OTP можно осуществить несколько транзакций (в частности, при реализации атак Race Condition («Состояние гонки»).

4.1. Недостаточная авторизация при доступе к данным пользователей

Данная уязвимость связана с недостатками реализации механизма авторизации пользователей. В каждой второй исследованной системе ДБО (55%) проверка пользовательских привилегий реализована некорректно, вследствие чего злоумышленник может получить доступ к некоторым сценариям и файлам, обратившись к ним напрямую. В частности, злоумышленник может получить несанкционированный доступ:

+ к персональным данным пользователей;
+ информации о транзакциях и платежных картах;
+ файлам, загруженным в систему ДБО;
+ информации о сертификатах;
+ специфическим данным о клиентах — в зависимости от особенностей системы (счета, шаблоны платежей).

В ходе анализа защищенности одной из систем ДБО для физических лиц было обнаружено, что приложение выполняет недостаточную проверку авторизации пользователей в системе, и злоумышленник может получить доступ к различным процедурам и функциям, в том числе к интерфейсам настройки системы ДБО, а также к функции онлайн-выписки по счету, не требующей двухфакторной аутентификации.

4.2. Внедрение внешних сущностей XML

Уязвимость позволяет злоумышленнику получить содержимое файлов, расположенных на атакуемом сервере, либо совершать запросы в локальную сеть от имени атакуемого сервера. Она обусловлена недостаточной проверкой приложением данных, поступающих от пользователя, что позволяет злоумышленнику осуществлять атаку, направленную на изменение логики запроса посредством внедрения произвольной DTD-схемы в тело XML-документа. Это может привести к разглашению важных данных, получению злоумышленником исходных кодов приложения, файлов конфигурации и другой чувствительной информации о системе, а также к отказу в обслуживании приложения.

Данной уязвимости в 2015 году оказались подвержены 35% исследованных систем. В предыдущие годы данный недостаток был самым распространенным среди критически опасных уязвимостей систем ДБО, и доля уязвимых систем составляла 46%.

4.3. Атаки на округление

В каждой четвертой системе ДБО была обнаружена возможность проведения атак на логику работы приложения. Вследствие некорректного использования алгоритмов округления чисел злоумышленник может получить бóльшую сумму денег, чем предусмотрено текущим обменным курсом банка.

Пример подобной атаки:

1. Злоумышленник переводит 0,29 рубля (29 копеек) в доллары США. При стоимости одного доллара США в 80 рублей сумма в 0,29 рублей соответствует 0,003625 доллара США. Данная сумма будет округлена до двух знаков после запятой, т.е. до 0,01 доллара, что соответствует одному центу.
2. Затем нарушитель переводит 1 цент обратно в рубли. В результате он получит 0,8 рубля (80 копеек). Таким образом, за одну итерацию злоумышленнику будет начислено на счет 0,51 рубля (51 копейка).

В результате автоматизации данной атаки злоумышленник может похищать больше денег. Например, при отсутствии ограничений на количество транзакций в сутки и минимальный размер транзакции, а также при возможности реализации атак типа Race Condition («Состояние гонки»), злоумышленник может получать в день порядка 100 рублей с одной учетной записи. Обладая достаточными техническими средствами и доступом к нескольким учетным записям, нарушитель может похищать у банка значительные суммы денежных средств.

Данный метод атаки известен довольно давно, однако не во всех системах ДБО защита от него реализована эффективно (иногда она вовсе отсутствует). Для противодействия атакам на округление и минимизации рисков хищений денежных средств рекомендуется ввести ограничение на минимально возможный размер денежных средств, которые могут быть переведены в другую валюту в рамках одной транзакции (например, 5—10 рублей и 2—3 доллара США).

5. Недостатки механизмов идентификации

Наиболее распространенными недостатками механизмов идентификации систем ДБО являются предсказуемость формата идентификатора учетной записи и раскрытие информации о зарегистрированных в системе идентификаторах.

Предсказуемый формат идентификатора позволяет злоумышленнику проанализировать механизм его формирования и составить список зарегистрированных идентификаторов пользователей. Такой список нарушитель может получить и в результате эксплуатации другой уязвимости низкого уровня риска — разглашение информации. Полученные данные нарушитель может использовать с целью получения несанкционированного доступа к системе ДБО (например, в результате подбора пароля). Также возможно проведение атак с использованием недостаточной авторизации для получения доступа к персональным данным пользователей или информации о платежных картах и транзакциях. Несмотря на низкий уровень опасности указанных недостатков, возможность получения злоумышленником информации о существующих идентификаторах в совокупности с выявленными недостатками механизмов аутентификации, авторизации и защиты транзакций (см. разделы 5 и 6) может сыграть существенную роль в получении несанкционированного доступа к личным кабинетам пользователей и последующем проведении транзакций от их имени.

5.1. Предсказуемый формат идентификаторов

Все исследованные системы ДБО содержали такой недостаток механизма идентификации пользователей, как предсказуемый формат идентификаторов учетных записей.

Как правило, банки для доступа к личному кабинету в системе ДБО предоставляют клиенту учетную запись, а идентификатор и пароль формируются по заданному разработчиком алгоритму; нарушитель может вычислить такой алгоритм. Нередки на практике случаи, когда идентификатором для доступа к системе ДБО служит номер мобильного телефона: в 10% рассмотренных нами систем используются именно такие идентификаторы. В одной из систем в качестве идентификатора использовалось шестизначное число, и каждому новому пользователю выдавался идентификатор со значением на 1 больше предыдущего.

Для снижения рисков компрометации системы в результате подбора учетных данных в системе ДБО должны быть предусмотрены функции смены пароля и идентификатора пользователя. При этом важно, чтобы пользователь системы, уровень осведомленности

которого в вопросах информационной безопасности может быть недостаточно высок, был предупрежден о необходимости смены учетных данных, выданных банком. (Для этого в системе может быть предусмотрено специальное сообщение, которое появляется на странице системы ДБО при первом входе в личный кабинет.) Можно также предусмотреть принудительный запрос на смену учетных данных по истечении заданного промежутка времени (например, 90 дней). Не менее важным фактором безопасности систем ДБО является строгость парольной политики, которая должна запрещать пользователям устанавливать в качестве паролей простые комбинации символов.

Среди всех исследованных систем ДБО возможность смены выданного банком идентификатора обеспечивали лишь 60%.

5.2. Раскрытие информации об идентификаторах

В системах ДБО в случае ввода идентификатора, отсутствующего в системе, сервер возвращает ответ на запрос, содержащий сообщение о ошибке. Уязвимая система в таком случае может выдавать текстовое сообщение, в котором прямо указано, что данный идентификатор не зарегистрирован. Встречаются также системы ДБО, в которых сообщение об ошибке не раскрывает информацию о существовании идентификатора напрямую, однако предусмотрены различные ответы сервера в зависимости от того, зарегистрирован в системе введенный идентификатор или нет. Проанализировав ответы сервера на отправку разных учетных данных, нарушитель может вычислить зарегистрированные в системе идентификаторы. Часто такая уязвимость встречается в сценариях регистрации новых пользователей или смены пароля.

В 2013–2014 годах данной уязвимости была подвержена каждая третья система ДБО. В настоящее время ситуация изменилась: из всех исследованных систем ДБО только одна была подвержена данной уязвимости. Сокращение доли уязвимых систем можно объяснить тем, что этот недостаток сравнительно просто выявить и устранить, в отличие от множества уязвимостей среднего и высокого уровней риска, для устранения которых зачастую требуется вносить множество изменений в исходный код приложения.

6. Анализ механизмов аутентификации

В большинстве рассмотренных систем (60%) использовалась обязательная двухфакторная аутентификация пользователей с использованием токена или одноразового пароля. В остальных системах ДБО аутентификация осуществлялась лишь на основании идентификатора и пароля пользователя.

Выявленные недостатки механизмов аутентификации систем ДБО преимущественно относятся к следующим категориям:

+ отсутствие обязательной двухфакторной аутентификации при доступе в личный кабинет и (или) на этапе проведения транзакций;
+ недостаточная аутентификация;
+ недостаточно строгая парольная политика;
+ недостаточная защита от подбора учетных данных.

Уязвимости, связанные с отсутствием либо недостатками реализации обязательной двухфакторной аутентификацией (на вход в личный кабинет или осуществление транзакций), — наиболее распространенные недостатки механизмов аутентификации в 2015 году. В предыдущие годы наиболее распространенной проблемой были недостатки парольной политики.

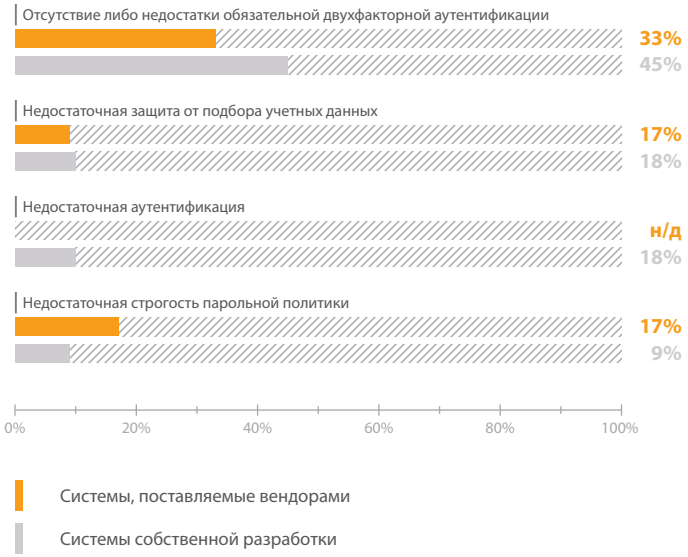

Рис. 26. Доли систем с уязвимыми механизмами аутентификации

6.1. Недостатки реализации двухфакторной аутентификации

Почти в половине всех рассмотренных систем ДБО собственной разработки (45%) и в каждой третьей системе ДБО, предоставленной вендорами (33%), обнаружились те или иные недостатки в механизме двухфакторной аутентификации. Обязательная двухфакторная аутентификация на вход в личный кабинет либо для подтверждения транзакций отсутствовала почти в каждой третьей системе (рис. 27).

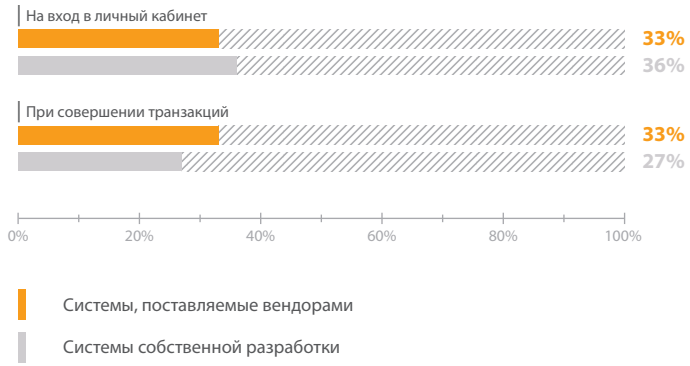

Рис. 27. Доли систем с уязвимыми механизмами двухфакторной аутентификации

В случае отсутствия двухфакторной аутентификации злоумышленник получает возможность беспрепятственно осуществлять транзакции при получении доступа к личному кабинету пользователя (например, в результате подбора учетных данных или перехвата сессии).

6.1.1. Механизм одноразовых паролей

Практически треть систем собственной разработки, проанализированных в 2015 году (27%), обеспечивали некорректную реализацию механизма OTP. Для систем, поставленных вендорами, этот показатель составил 17%. Недостатки реализации механизма OTP, выявленные в системах ДБО:

+ возможность подбора OTP;
+ отсутствие подтверждения транзакций и других операций с помощью OTP (нарушитель может изменять, к примеру, шаблоны операций без такого подтверждения);
+ недостаточно эффективно реализованная защита от несанкционированной смены SIM-карты (может привести к получению одноразового пароля нарушителем).

6.1.2. Другие механизмы

Одна из проанализированных систем имела уязвимый механизм двухфакторной аутентификации, основанный на электронной подписи документа с помощью ключа. Реализация данного механизма не обеспечивала достаточный контроль целостности, вследствие чего злоумышленник потенциально мог внедрить произвольные данные в подписанный сертификат, то есть подменить сертификат или подделать корневой сертификат.

6.2. Недостаточная защита от подбора учетных данных

Ряд исследованных систем ДБО не обеспечивают достаточную защиту от подбора учетных данных пользователей (18% систем собственной разработки и 17% систем от вендоров). Среди недостатков этого типа можно выделить:

+ отсутствие либо возможность обхода механизма CAPTCHA;
+ отсутствие временной блокировки учетных записей пользователей после нескольких неудачных попыток ввода учетных данных.

Для защиты от атак, направленных на подбор учетных данных, часто применяется механизм временной или постоянной блокировки учетных записей после нескольких неудачных попыток ввода пароля, однако он не позволяет защититься от подобных атак полностью. В случае когда парольная политика разрешает использование простых паролей, при отсутствии двухфакторной аутентификации злоумышленник может провести атаку, направленную на подбор идентификаторов по какому-либо одному словарному паролю.

Важно отметить и тот факт, что в случае использования временной или постоянной блокировки учетной записи в результате многократного ввода неверных учетных данных нарушитель может использовать данный механизм для целенаправленной блокировки учетных записей клиентов банка (например, если нарушитель получил информацию об используемых в приложении идентификаторах). Это может привести к существенным репутационным потерям.

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). Данный механизм запрашивает у пользователя ввод отображенной на экране информации (например, текста с картинки) при частых попытках ввода учетных данных. Это существенно затрудняет злоумышленнику проведение автоматизированной атаки и позволяет избежать блокировки учетной записи.

Использование 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 временной промежуток между последовательными попытками входа, IP-адрес источника, факты подбора не только паролей, но и идентификаторов.

6.3. Недостаточная аутентификация

Данная уязвимость заключается в том, что приложение не проверяет легитимность пользователя (ввод учетных данных и их корректность) при доступе к важной информации или к различным функциям системы. Уязвимость данного типа была обнаружена лишь в одной из исследованных систем. В результате эксплуатации этой уязвимости было продемонстрировано получение доступа к сценарию, уязвимому к внедрению внешних сущностей XML. В первую очередь приложение осуществляло обработку XML-документа, а затем уже проверку учетных данных. Злоумышленник, таким образом, мог путем эксплуатации двух различных уязвимостей осуществлять чтение произвольных файлов на сервере.

Необходимо обеспечить строгое разграничение доступа к функциям приложения. Необходимо проверять привилегии пользователей на доступ ко всем сценариям и функциям системы ДБО, особенно к тем, которые должны быть доступны только администраторам.

6.4. Недостатки парольной политики

В 12% исследованных систем ДБО выявлены те или иные недостатки парольной политики. К таким недостаткам относятся, например, отсутствие либо некорректная реализация ограничений:

+ на допустимую длину пароля,
+ сложность пароля,
+ срок действия пароля.

Подобные недостатки в совокупности с недостаточной защитой от атак, направленных на подбор учетных данных, а также отсутствием двухфакторной аутентификации при входе в систему, дают нарушителю возможность осуществлять атаки, приводящие к несанкционированному доступу к личным кабинетам клиентов банка.

Рекомендуется использовать пароли длиной не менее 8 символов. В пароле должны быть обязательно использованы прописные и строчные латинские буквы, цифры и спецсимволы. Кроме того, следует запретить использование словарных паролей (например, P@ssw0rd) и сочетаний близких клавиш на клавиатуре. Срок действия пароля должен быть ограничен (например, 90 дней), при этом пользователь не должен иметь возможность выбрать новый пароль, совпадающий с одним из трех предыдущих.

7. Недостатки механизмов авторизации и защиты транзакций

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

Для защиты транзакций в большинстве систем применялась двухфакторная аутентификация с использованием OTP.

Наиболее распространены следующие серьезные недостатки механизмов защиты транзакций:

+ недостаточная авторизация, в том числе при доступе к данным пользователей (см. раздел 3.2) и отладочным сценариям (70% систем ДБО);
+ некорректная реализация механизма OTP, вследствие которой злоумышленник может проводить несколько транзакций по одному одноразовому паролю или перехватить значение пароля (24% систем);
+ отсутствие двухфакторной аутентификации на этапе проведения транзакций (29% систем).

Большинство недостатков авторизации были выявлены в системах ДБО собственной разработки. В качестве наиболее опасных можно выделить недостатки, возникшие в результате недостаточной проверки прав доступа при совершении критически важных операций. К таким недостаткам, в частности, относится возможность сменить пароль или отключить механизм OTP путем отправки специально сформированного запроса к приложению без дополнительного предъявления основного пароля.

Около 35% всех проанализированных систем содержали недостатки защиты сессии от перехвата и последующего использования злоумышленником. Для перехвата сессии злоумышленник может, к примеру, использовать межсайтовое выполнение сценариев. Среди выявленных недостатков защиты сессии можно выделить отсутствие привязки сессии к IP-адресу и недостаточную защиту cookie-параметров, содержащих идентификатор сессии и другие важные данные.

8. Уязвимости на уровне кода веб-приложений

8.1. Общая статистика

Приведем обзор уязвимостей, обусловленных ошибками в программном коде. Уязвимостям на уровне кода приложений подвержены больше половины исследованных систем (68%). Это лучше, чем в 2013—2014 годах (было 82%). При этом все ресурсы, подверженные уязвимостям данного типа, содержат недостатки как минимум средней степени риска. Более половины исследованных систем (63%) содержат ошибки, уровень риска которых оценивается как высокий (см. рис. 28). В предыдущие годы этот показатель был выше на 5%.

По сравнению с прошлыми годами доля уязвимых систем снизилась, однако по-прежнему более половины всех систем ДБО подвержены критически опасным уязвимостям на уровне кода.

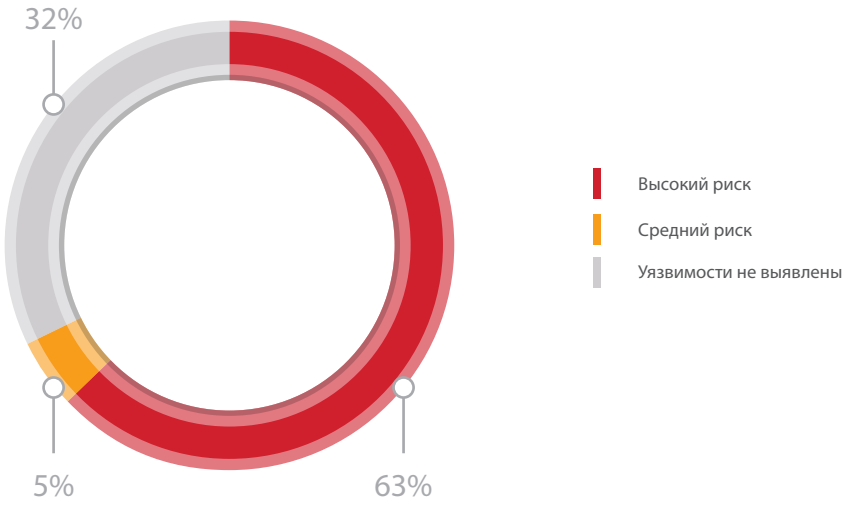

Рис. 28. Распределение систем по максимальной степени риска уязвимостей на уровне кода приложений

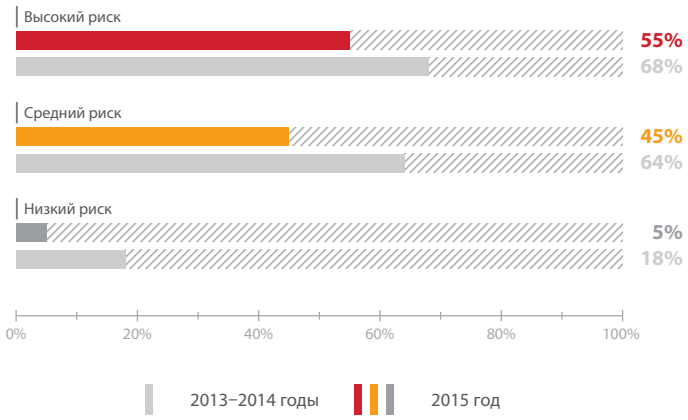

Рис. 29. Доли систем, клиентская часть которых подвержена уязвимостям на уровне кода приложения

Распределение ошибок кода веб-приложений по уровню опасности практически не изменилось по сравнению с результатами предыдущих лет. Около 42% всех выявленных ошибок в программном коде приложений характеризуются высоким уровнем риска. К данной категории относится одна из самых распространенных критически опасных уязвимостей систем ДБО — «Внедрение внешних сущностей XML» (см. раздел 4.2). Более половины уязвимостей на уровне кода характеризуются средним уровнем риска (55%).

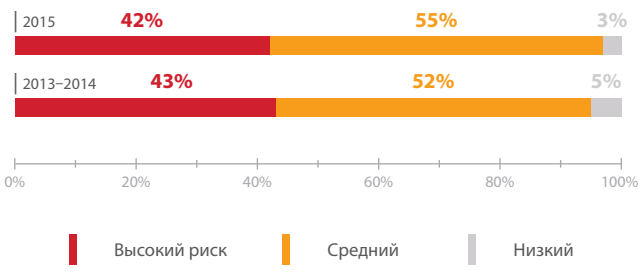

Рис. 30. Уязвимости на уровне кода приложений

Среднее количество ошибок в программном коде, приходящееся на одну систему, представлено на рис. 31. Эти показатели лучше результатов предыдущих лет практически в 2 раза. К примеру, прежде на одну систему в среднем приходилось 3,2 критически опасной ошибки в коде приложения.

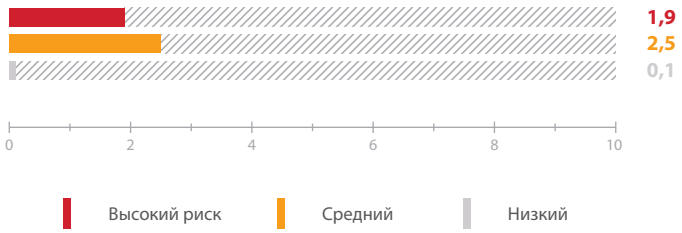

Рис. 31. Среднее количество ошибок в коде приложений на одну систему

8.2. Системы вендорские и собственной разработки

Как упоминалось ранее, системы, поставляемые известными вендорами, содержат большее количество уязвимостей в программном коде (см. раздел 3.3). Кроме того, для данной категории систем более половины выявленных уязвимостей, связанных с ошибками кода (55%), характеризуются высоким уровнем риска (рис. 32). Полученные результаты практически повторяют данные предыдущих лет.

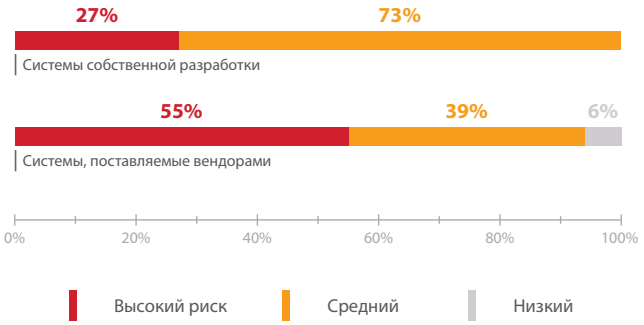

Рис. 32. Доли ошибок различной степени риска в программном коде

Рис. 33. Среднее количество уязвимостей кода на одну систему

В 2015 году во всех системах ДБО собственной разработки банков были выявлены ошибки в коде как минимум среднего уровня риска, при этом критически опасные уязвимости встречались в 27% систем (в 2013—2014 годах было 25%).

В среднем в каждой системе ДБО, поставляемой вендором, содержится 2,6 критически опасной уязвимости на уровне кода приложения. Системы собственной разработки содержат существенно меньше таких ошибок. (То же было отмечено и в предыдущие годы.)

Как мы уже отмечали, собственные системы ДБО банков проектируются под конкретную архитектуру и имеют заданный набор функций; они проще и, как следствие, менее уязвимы (см. раздел 3.3).

8.3. Наиболее распространенные уязвимости

Наиболее распространены оказались ошибки в коде приложений, связанные с внедрением внешних сущностей XML, межсайтовым выполнением сценариев и выполнением произвольного кода. Всего в список распространенных ошибок входят 4 критически опасные уязвимости.

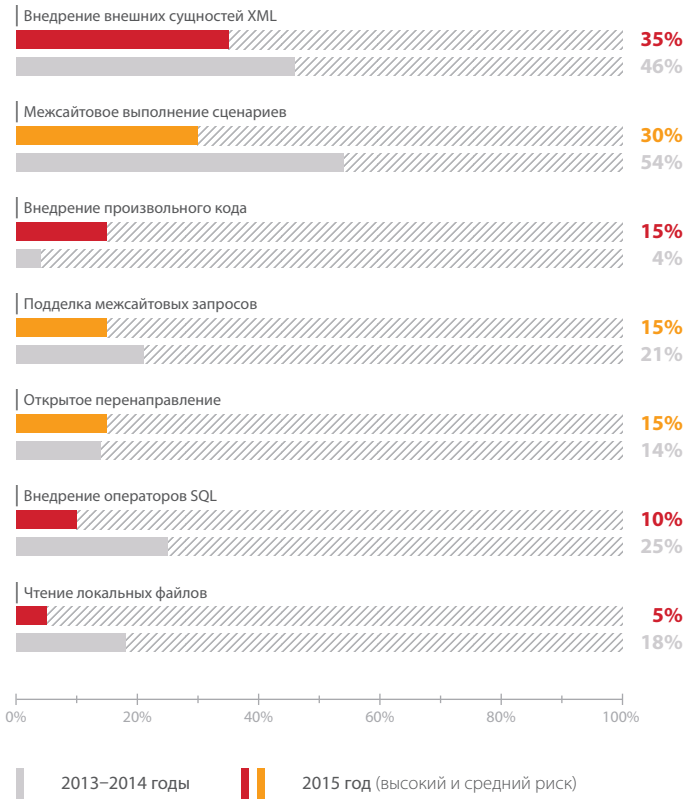

Рис. 34. Доли систем, подверженных распространенным уязвимостям уровня кода приложения

В 2015 году заметно возросла доля систем, уязвимых для выполнения произвольного кода. Данный недостаток высокой степени риска позволяет нарушителю выполнять команды ОС на сервере приложения и повышать свои привилегии. Нарушитель может получить доступ к важной информации, хранящейся в файлах на сервере, а также осуществлять различные атаки, в том числе направленные на полный отказ в обслуживании системы ДБО.

Стоит отметить, что в системах от вендоров не было обнаружено таких недостатков, как внедрение произвольного кода, открытое перенаправление и чтение локальных файлов. Однако в этих системах было выявлено множество критически опасных уязвимостей, таких как внедрение внешних сущностей XML и внедрение операторов SQL.

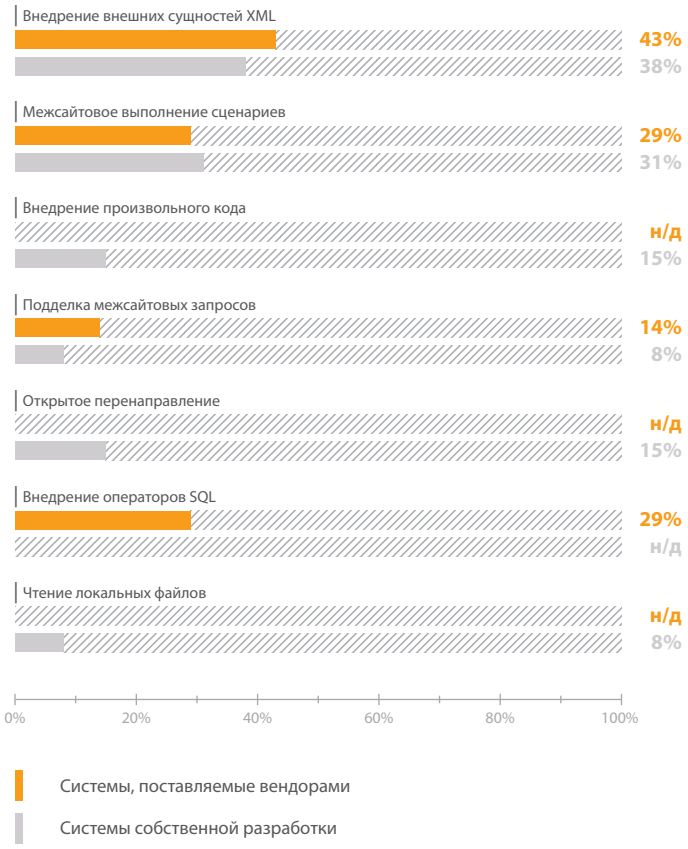

Рис. 35. Уязвимости кода приложения (доли систем)

Для снижения рисков, связанных с эксплуатацией уязвимостей на уровне кода веб-приложения, рекомендуется внедрять практики безопасного программирования, регулярно проводить анализ защищенности приложений, в том числе с анализом исходного кода (например, дважды в год), и оперативно устранять выявленные уязвимости. В случае использования систем, поставляемых вендорами, а также при невозможности оперативно исправлять недостатки в системах собственной разработки рекомендуется использовать превентивные средства защиты — межсетевые экраны уровня приложения (WAF).

9. Недостатки конфигурации

9.1. Общая статистика

Уязвимости данной категории вызваны некорректной настройкой ОС, СУБД, веб-сервера и компонентов веб-приложений. Примерно 27% всех обнаруженных недостатков систем ДБО относятся к этому типу (см. рис. 8). Большинство уязвимостей данной категории характеризуются средним уровнем риска (57%): в отличие от предыдущих лет не было выявлено критически опасных недостатков конфигурации (например, избыточных привилегий приложения).

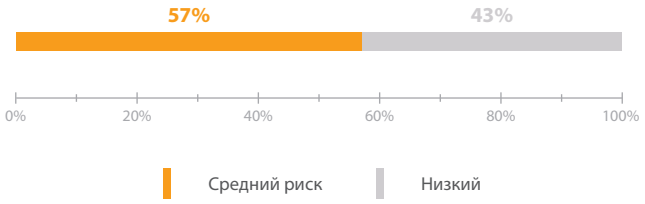

Рис. 36. Недостатки конфигурации систем ДБО

Порядка 90% рассмотренных систем содержали хотя бы одну уязвимость, связанную с недостатками конфигурирования; 65% содержали недостатки среднего уровня риска.

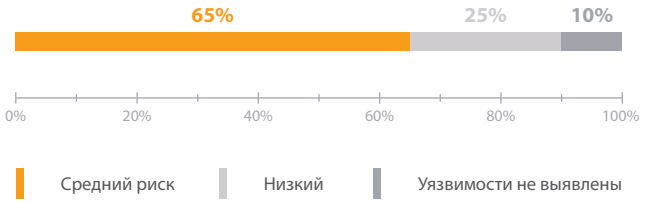

Рис. 37. Максимальный уровень риска недостатков конфигурации (доли систем)

В среднем каждая система ДБО содержит хотя бы одну уязвимость среднего и одну уязвимость низкого уровня риска, связанные с некорректными настройками.

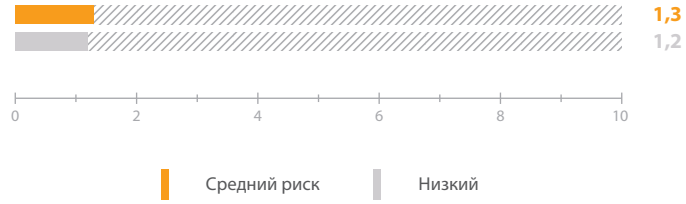

Рис. 38. Среднее число уязвимостей конфигурации на одну систему

Наиболее распространенные уязвимости данной категории:

+ возможность проведения атак на сессию (50% систем);
+ возможность идентификации ПО (40%);
+ разглашение важных данных (25%);
+ небезопасная передача данных (25%).

Приведем пример. Если для cookie-параметра, передающего идентификатор сессии, не устанавливается свойство secure, браузер пользователя может передавать параметр не только по безопасному протоколу HTTPS, но и по открытому протоколу HTTP. При использовании небезопасного протокола передачи данных или недостаточно стойких алгоритмов шифрования злоумышленник может перехватить пользовательские данные, в том числе идентификатор сессии.

9.2. Недостатки конфигурации в системах собственной разработки и поставляемых вендорами

В системах собственной разработки немногим больше половины уязвимостей, связанных с недостатками конфигурации, характеризуются средним уровнем риска (57%). В системах от вендоров уязвимостей среднего и низкого уровней риска поровну.

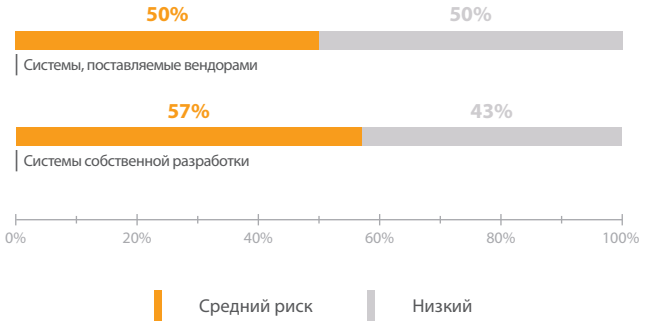

Рис. 39. Доля уязвимостей различного уровня риска в общем числе недостатков конфигурации

На рис. 40 представлено среднее количество уязвимостей различной степени опасности, приходящееся на одну систему, для различных категорий разработчиков. В целом количество недостатков конфигурации невелико для обоих типов систем (в системах от вендоров их в среднем выявлено несколько больше).

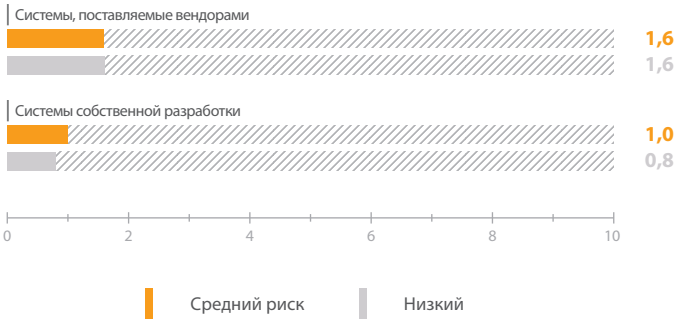

Рис. 40. Среднее количество уязвимостей конфигурации на одну систему

10. Отказ в обслуживании

Атаки, направленные на отказ в обслуживании (DoS), — одна из самых актуальных угроз безопасности. В случае систем ДБО такая атака может быть направлена на нарушение доступности как серверной части системы, так и личного кабинета пользователя. При отказе серверной части банк может понести существенные репутационные потери (банковские продукты будут какое-то время недоступны для клиентов). Могут возникать и крупные финансовые потери, в том числе за счет прибыли, упущенной из-за остановки транзакций.

Отказ в обслуживании всей системы может быть вызван некорректной обработкой поступающих данных, а также возникать в результате эксплуатации уязвимостей — внедрения

сущностей XML, внедрения операторов XPath, внедрение произвольного кода и ряда других. Вызвать полный отказ в обслуживании системы ДБО возможно для 40% исследованных ресурсов.

С другой стороны, используя предсказуемость формата идентификатора учетных записей, нарушитель способен спровоцировать блокировку учетных записей отдельных пользователей — путем многократного ввода неверных учетных данных (если в данной системе такая блокировка производится автоматически). Подобная возможность была в 2015 году выявлена только в одной системе ДБО.

11. Уязвимости клиентского ПО мобильных систем ДБО

Клиентское ПО для Android, как и в предыдущие годы, более уязвимо по сравнению с приложениями для iOS. В 2015 году 75% мобильных систем ДБО для Android содержали критически опасные уязвимости, в то время как доля приложений на базе iOS, подверженных уязвимостям высокой степени риска, составила 33% (см. рис. 41).

Важно отметить, что хотя обычно уровень риска уязвимостей, связанных с хранением и передачей важных данных в открытом виде, оценивается как средний, в некоторых случаях такие уязвимости клиентского ПО в исследованных мобильных системах ДБО были переквалифицированы как критически опасные — по рекомендации владельцев соответствующих систем. Других уязвимостей высокой степени риска (например, «Внедрение операторов SQL», «Внедрение внешних сущностей XML», «Внедрение произвольного кода») в рамках проектов 2015 года выявлено не было.

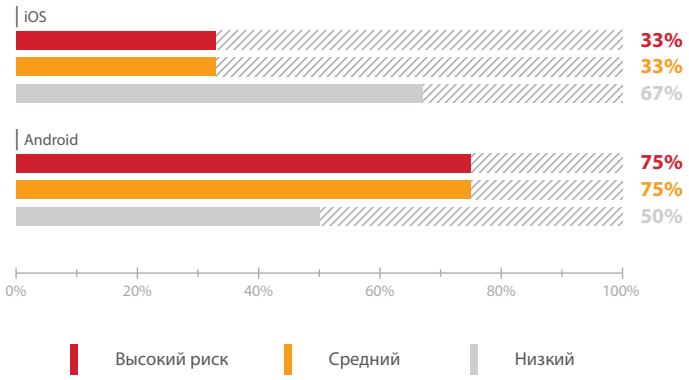

Рис. 41. Доли клиентского ПО мобильных систем ДБО с уязвимостями различной степени опасности

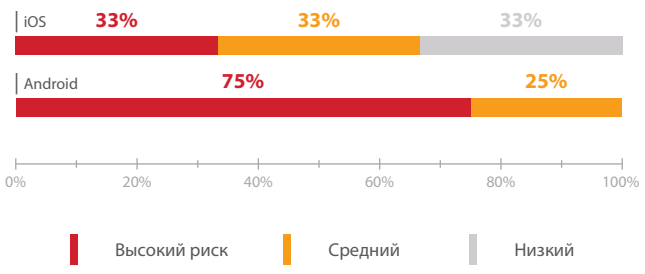

Рис. 42. Максимальный уровень риска уязвимостей мобильных систем ДБО

Все исследованные в 2015 году мобильные системы ДБО содержали уязвимости, при этом Android-системы содержали недостатки как минимум среднего уровня риска. В 33% мобильных ДБО на базе iOS были обнаружены недостатки только низкой степени опасности.

В среднем каждое приложение на базе Android содержит 3,8 уязвимости, что примерно соответствует уровню 2013–2014 годов, когда их было 3,7. Для iOS-приложений данный параметр равен 1,6, что значительно лучше результата предыдущих лет, когда на каждое приложений приходилось 2,3 уязвимости. Недостаток низкого уровня риска «Идентификация приложений» был выявлен как в системах на iOS, так и на Android.

Рис. 43. Среднее количество уязвимостей в клиентском ПО мобильных систем

Наиболее часто в мобильных системах ДБО встречались уязвимости, связанные с небезопасным хранением и передачей данных. Распространенными остаются также уязвимости, связанные с недостатками защиты сессии, хотя доля систем с такими недостатками заметно снизилась.

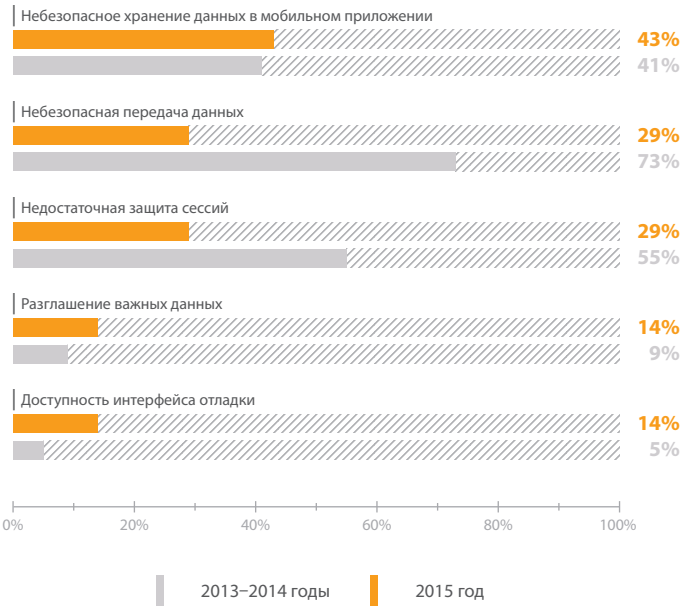

Рис. 44. Распространенные уязвимости клиентского ПО мобильных систем (доли систем)

Хотя самые распространенные уязвимости мобильных систем ДБО характеризуются средней степенью риска, в ряде случаев совокупность нескольких недостатков позволяла реализовать серьезные угрозы безопасности. И как мы указали выше, такие недостатки были отмечены владельцами конкретных систем как критически опасные. Например, некорректная реализация механизма входа по короткому PIN-коду в совокупности с хранением идентификатора сессии в файловой системе позволяют злоумышленнику, обладающему физическим доступом к устройству, подменить ответ веб-сервера таким образом, что на любую попытку неверного ввода PIN-кода сервер будет возвращать значение true. В результате успешной атаки злоумышленник может получить полный контроль над личным кабинетом атакуемого пользователя, в том числе изменять настройки и совершать транзакции от его имени. Также в одном из проектов нарушитель мог получить доступ к мобильному банкингу пользователя вследствие недостаточно защищенной передачи данных: система позволяла использовать самоподписанные сертификаты при использовании протокола HTTPS.

11.1. Небезопасное хранение данных

Многие мобильные приложения хранят в файловой системе важные данные в открытом виде (это почти каждая вторая система, 43%). К такой чувствительной информации относятся, к примеру, персональные данные клиентов, идентификаторы и пароли пользователей, идентификаторы сессий, отладочная информация.

Рекомендуется не сохранять важные данные в общедоступных каталогах или использовать шифрование. Также рекомендуется обеспечить строгое разграничение доступа к данным приложения, руководствуясь принципом минимизации привилегий.

11.2. Небезопасная передача данных

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

+ передача данных по незащищенному протоколу HTTP;
+ отсутствие проверки SSL-сертификатов;
+ возможность добавления на устройстве пользователя самоподписанных сертификатов в список доверенных;
+ передача важных данных (например, пароля пользователя) в открытом виде без использования механизмов хеширования.

В результате эксплуатации указанных уязвимостей злоумышленник может получить доступ к важным данным, передаваемым приложением (идентификаторам и паролям пользователей, геолокационным данным и прочей 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 этом, в случае автоматизированного сценария атаки, злоумышленник может вмешаться в процесс проведения транзакций, подменяя реквизиты платежей в режиме реального времени.

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

11.3. Недостаточная защита сессий

В исследованных мобильных системах ДБО было выявлено большое количество уязвимостей, позволяющих реализовать атаки на сессии пользователей. К ним относились следующие:

- при выходе из учетной записи приложение не отправляет запрос к серверу для закрытия сессии. Нарушитель может использовать активную сессию для проведения атак. В случае перехвата нарушитель может использовать сессию пользователя и получить доступ к его данным, а также данным платежных карт;
- при выходе из учетной записи приложение отправляет запрос к серверу для закрытия сессии, однако сессия остается активной на протяжении еще 20 минут. Нарушитель может использовать это время для осуществления атак. Также злоумышленник может продлять активность сессии, периодически отправляя запросы серверу;
- идентификатор сессии не привязан к конкретному IP-адресу. В случае перехвата такого идентификатора нарушитель может получить несанкционированный доступ к личному кабинету пользователя;
- для cookie-параметров не устанавливается свойство secure, вследствие чего разрешается передавать идентификатор сессии по незащищенному протоколу HTTP.

Для защиты рекомендуется завершать активную сессию при выходе из учетной записи: идентификатор сессии не должен быть активен после выхода пользователя из системы. Не рекомендуется разрешать подключение к одной учетной записи одновременно с нескольких устройств. При подключении к учетной записи с другого устройства рекомендуется автоматически завершать текущую активную сессию. Также необходимо устанавливать свойство secure для защиты cookie-параметров, содержащих идентификатор сессии и другие важные данные.

Заключение

Уровень защищенности систем ДБО на сегодняшний день по-прежнему остается низким, несмотря на сокращение общей доли критически опасных уязвимостей по сравнению с прошлыми годами. Уязвимыми остаются как системы для физических, так и для юридических лиц — независимо от того, разработаны они известным вендором либо самим банком.

Низкая защищенность систем ДБО, находящихся в эксплуатации, наглядно свидетельствует о необходимости внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений. Анализ защищенности системы ДБО необходимо проводить не только на этапах разработки и перед вводом в эксплуатацию, но и во время ее активного использования клиентами банка. Причем такой анализ необходимо осуществлять на регулярной основе (например, дважды в год) с контролем устранения выявленных недостатков. Системам ДБО, приобретенным у вендоров, стоит уделить особое внимание: зачастую они более подвержены уязвимостям, чем системы собственной разработки банков. Кроме того, рекомендуется использовать средства превентивной защиты, такие как межсетевой экран уровня приложения (WAF). В частности, для продуктивных систем, приобретаемых у вендоров, межсетевой экран уровня приложения рекомендуется использовать во избежание эксплуатации известных уязвимостей до выпуска очередного обновления.

Как показало исследование, проблемы реализации механизмов идентификации, аутентификации и авторизации по-прежнему актуальны. Недостаточное внимание разработчиков к таким недостаткам может привести к реализации различных угроз безопасности вплоть до несанкционированного проведения транзакций и получения полного контроля над системой ДБО. Стоит отметить, что для получения доступа к личному кабинету пользователя нарушителю достаточно использовать давно известные и по-прежнему распространенные уязвимости (например, недостаточную защиту сессии). Необходимо уделять особое внимание корректной реализации механизмов защиты. Также следует внедрять процессы безопасной разработки, обеспечивать всестороннее тестирование безопасности систем при приемке работ. В качестве основы для внедрения процессов обеспечения информационной безопасности систем ДБО на всех стадиях жизненного цикла могут быть использованы выпущенные в 2014 году рекомендации Банка России — РС БР ИББС-2.6-2014.

Учитывая высокую долю критически опасных уязвимостей на уровне кода веб-приложений, необходимо проводить регулярные проверки его качества, например путем анализа защищенности методом белого ящика (в том числе с помощью автоматизированных средств). Регулярный и всесторонний контроль защищенности систем ДБО позволит снизить риски реализации угроз безопасности и избежать финансовых и репутационных потерь.

О компании

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

Подробнее: facebook.com/PositiveTechnologies, facebook.com/PHDays, twitter.com/ptsecurity

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.ru