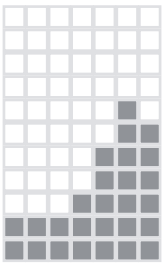


СТАТИСТИКА УЯЗВИМОСТЕЙ СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (2011—2012)

Москва, 2013

ОГЛАВЛЕНИЕ

1 РЕЗЮМЕ

В настоящем обзоре представлены обобщенные выводы об уязвимостях систем дистанционного банковского обслуживания (ДБО), обнаруженных в 2011 и 2012 годах, основанные на результатах работ по анализу защищенности систем ДБО, проведенных специалистами компании Positive Technologies для ряда крупнейших российских банков. По результатам проведенного исследования можно сделать следующие основные выводы.

В каждой третьей системе возможно получение доступа к операционной системе или СУБД сервера

СИСТЕМЫ ДБО, КАК ПРАВИЛО, ИМЕЮТ СРЕДНИЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ И НИЖЕ

В каждой третьей системе возможно получение доступа к операционной системе или СУБД сервера, в ряде случаев возможно получение полного контроля над ОС или СУБД. Еще 37% систем ДБО позволяют осуществлять несанкционированные транзакции на уровне пользователей. Каждая из рассмотренных систем содержит уязвимости среднего уровня риска.

Отсутствие уязвимостей высокой степени риска не означает, что система хорошо защищена

В РАССМОТРЕННЫХ СИСТЕМАХ ПРЕОБЛАДАЮТ УЯЗВИМОСТИ СРЕДНЕГО И НИЗКОГО УРОВНЯ РИСКА

Среди всех обнаруженных уязвимостей ДБО было выявлено 8% уязвимостей высокого уровня риска, 51% среднего уровня риска, и 41% — низкого уровня. Наиболее распространенные уязвимости: слабая парольная политика и недостаточная защита от подбора учетных данных (Brute Force), которым подвержены 82% рассмотренных систем. Тем не менее, зачастую для несанкционированного проведения транзакций на уровне пользователей систем ДБО злоумышленнику достаточно воспользоваться сразу несколькими уязвимостями средней критичности, что позволяет сделать вывод: отсутствие уязвимостей высокой степени риска не означает, что система хорошо защищена.

Критические уязвимости на уровне кода веб-приложения были обнаружены только в системах от вендоров

УЯЗВИМОСТИ ВЫСОКОЙ СТЕПЕНИ РИСКА ПРЕОБЛАДАЮТ В СИСТЕМАХ ДБО, ПРЕДЛАГАЕМЫХ ИЗВЕСТНЫМИ ВЕНДОРАМИ

Системы ДБО, поставляемые профессиональными разработчиками, в среднем содержат почти в 4 раза больше уязвимостей на уровне кода приложения, чем системы собственной разработки. Критические уязвимости на уровне кода веб-приложения были обнаружены только в системах от вендоров.

Данный факт можно объяснить тем, что при использовании системы, предоставляемой вендором, банк в основном полагается на поставщика продукта в вопросах контроля качества кода. При этом сложная архитектура, кросс-платформенность и большое количество функций таких систем не всегда позволяют вендору обеспечить должный уровень защищенности на уровне кода приложения.

В продуктивных системах было выявлено примерно в полтора раза больше уязвимостей всех уровней риска

ПРОДУКТИВНЫЕ СИСТЕМЫ БОЛЕЕ УЯЗВИМЫ, ЧЕМ ТЕСТОВЫЕ

Согласно проведенному исследованию, в продуктивных системах было выявлено примерно в полтора раза больше уязвимостей всех уровней риска по сравнению с тестовыми системами, находящимися на стадии приемки работ 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. Результаты проведенного исследования подчеркивают не только необходимость проведения анализа защищенности системы ДБО перед вводом в эксплуатацию, но и необходимость проведения регулярного тестирования в процессе эксплуатации.

В трех системах двухфакторная авторизация при проведении транзакции отсутствовала вовсе

ВСЕ ИССЛЕДОВАННЫЕ СИСТЕМЫ ДБО ИМЕЛИ ТЕ ИЛИ ИНЫЕ НЕДОСТАТКИ В РЕАЛИЗАЦИИ МЕХАНИЗМОВ ЗАЩИТЫ

Более 60% исследованных систем ДБО содержали как минимум один из недостатков механизма идентификации пользователей — предсказуемый формат идентификаторов пользователей или раскрытие информации о существующих в системе идентификаторах пользователей. Все рассмотренные системы имели недостатки реализации механизма аутентификации: слабую парольную политику или недостаточную защиту от подбора учетных данных. Двухфакторная аутентификация использовалась только в двух исследованных системах. Более 80% систем содержали различные недостатки реализации механизма авторизации, при этом в трех системах двухфакторная авторизация при проведении транзакции отсутствовала вовсе. Несмотря на то что по отдельности указанные недостатки, как правило, не несут высоких рисков для системы, их сочетание может быть использовано злоумышленником для получения доступа в личные кабинеты пользователей путем подбора идентификаторов и паролей и последующего проведения транзакций путем использования уязвимостей механизма авторизации.

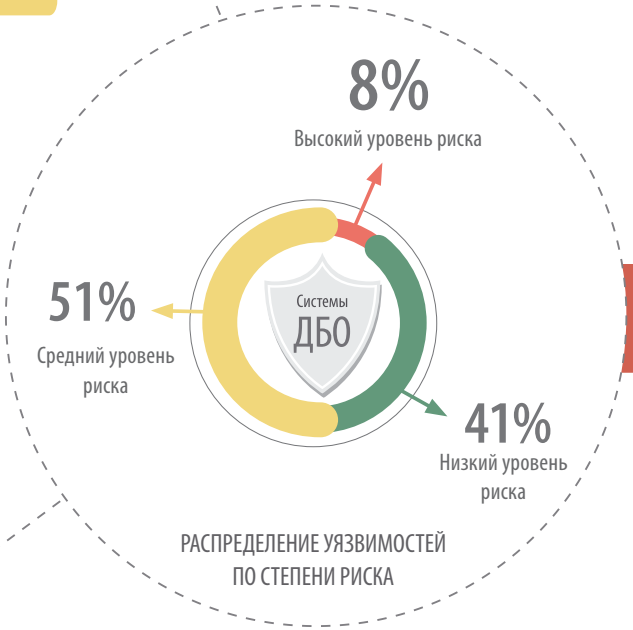
POSITIVE TECHNOLOGIES

АНАЛИТИКА 2011 • 2012

Статистика уязвимостей систем дистанционного банковского обслуживания

ИТОГОВЫЙ РЕЙТИНГ ДЕСЯТИ НАИБОЛЕЕ РАСПРОСТРАНЁННЫХ УЯЗВИМОСТЕЙ СИСТЕМ ДБО

РАСПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ ПО СТЕПЕНИ РИСКА



ОБЩАЯ СТАТИСТИКА ПО ВИДАМ УЯЗВИМОСТЕЙ

Системы ДБО, поставляемые известными вендорами, содержат в 4 раза больше уязвимостей высокого уровня риска в коде веб-приложения, чем системы собственной разработки.

Уровень риска в продуктивных системах в 1,5 раза выше, чем в тестовых.

Недостатки механизмов защиты обнаружены во всех рассмотренных системах.

РЕАЛИЗУЕМЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ДБО

Отсутствие уязвимостей высокой степени риска не означает, что система хорошо защищена

- 9% Полный контроль над системой
- 9% Полный контроль над СУБД
- 18% Выполнение команд на сервере
- 37% Несанкционированное проведение транзакций
- 9% Доступ в личные кабинеты пользователей
- 9% Проведение транзакций без ввода OTP авторизованным пользователем
- 9% Получение данных для подключения к СУБД и внутренним системам (возможно развитие атаки из внутренней сети)

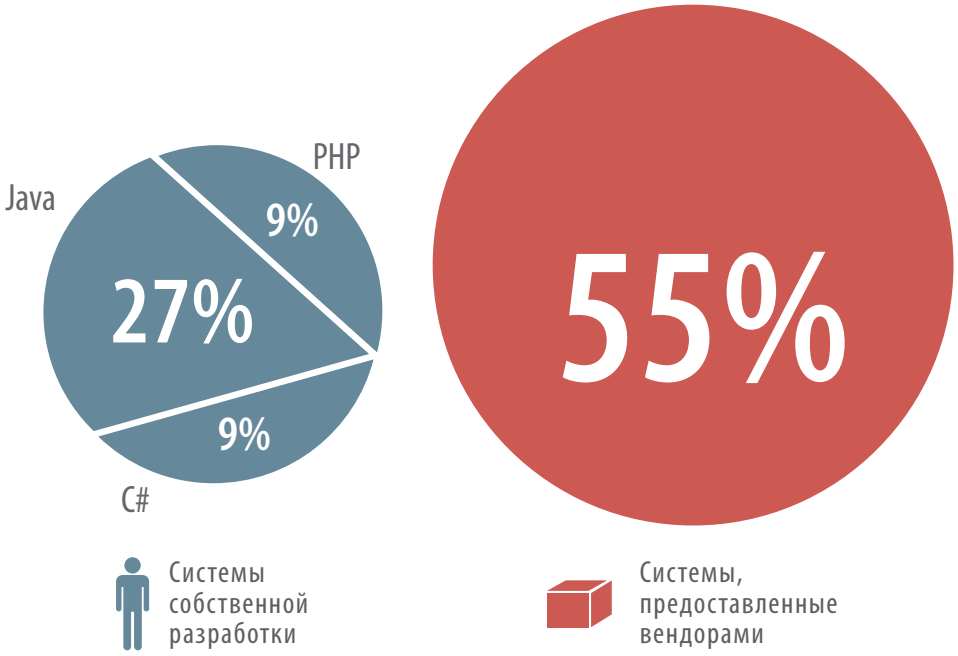
2 ИСХОДНЫЕ ДАННЫЕ

В рамках проведенного исследования было рассмотрено 11 систем дистанционного банковского обслуживания, анализ защищенности которых проводился специалистами Positive Technologies в течение 2011 и 2012 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 функционирования системы в динамике.

Рассмотренные системы ДБО относятся к различным сферам обслуживания. Более 70% всех рассмотренных систем ДБО относятся к системам, обслуживающим физические лица. Только три из рассматриваемых систем относились к типу «Клиент-банк» , во всех прочих для подключения использовался тонкий клиент («Интернет-банк»).

РАСПРЕДЕЛЕНИЕ СИСТЕМ ДБО ПО СФЕРАМ ОБСЛУЖИВАНИЯ КЛИЕНТОВ

55% рассмотренных систем ДБО построены на базе решений, поставляемых известными вендорами. Менее половины исследованных систем представлены собственными разработками: три системы разработаны на языке Java и по одной на языках C# и PHP.



Среди исследованных систем ДБО, приобретаемых банками у известных специализированных вендоров, были выявлены системы, содержащие критические уязвимости. В соответствии с политикой ответственного разглашения информации об уязвимостях в настоящем отчете названия компаний-производителей не указываются.

Все рассмотренные в ходе исследования системы представляли собой различные программные продукты. Кроме того, результаты повторного анализа защищенности систем ДБО, проводившегося в ряде случаев с целью проверки корректности устранения уязвимостей, не были включены в данную статистику. Таким образом в обзоре было исключено дублирование результатов для объективной оценки общего состояния защищенности систем ДБО российских банков. При этом, учитывая высокую распространенность рассмотренных систем от профессиональных разработчиков на российском рынке[1], результаты данного исследования могут быть актуальны не только для представленной здесь выборки, но и как минимум для сотни других банков.

[1] Согласно исследованию рынка систем ДБО, проведенному CNews Analytics в 2012 г. (http://www.cnews.ru/downloads/CNews_DBO_Report_2012.pdf), а также открытой информации о количестве банков, использующих системы от вендоров.

В ходе работ рассматривались продуктивные системы, тестовые стенды, представляющие собой копии продуктивных систем, а также тестовые системы, готовые к переводу в промышленную эксплуатацию. Более половины систем исследовались на тестовых площадках. Одна из систем была исследована как в рамках тестовой площадки, так и в продуктивном исполнении. Данная статистика отражена на диаграмме.

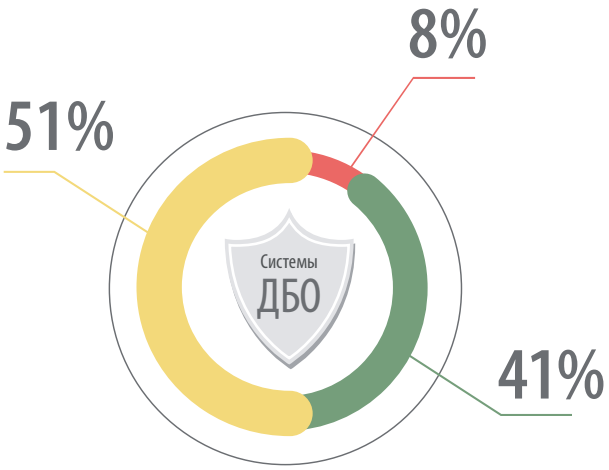
Среди продуктивных систем, предоставленных для анализа, все, кроме одной, представляли собой решения профессиональных разработчиков систем ДБО, тогда как для систем собственной разработки работы по анализу защищенности, как правило, проводились на тестовых стендах до ввода системы в промышленную эксплуатацию. Данный факт может говорить о высокой степени доверия банков к известным вендорам программных продуктов для систем ДБО.

3 ОБЩИЕ РЕЗУЛЬТАТЫ РАБОТ

3.1. НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ И СВЯЗАННЫЕ С НИМИ УГРОЗЫ

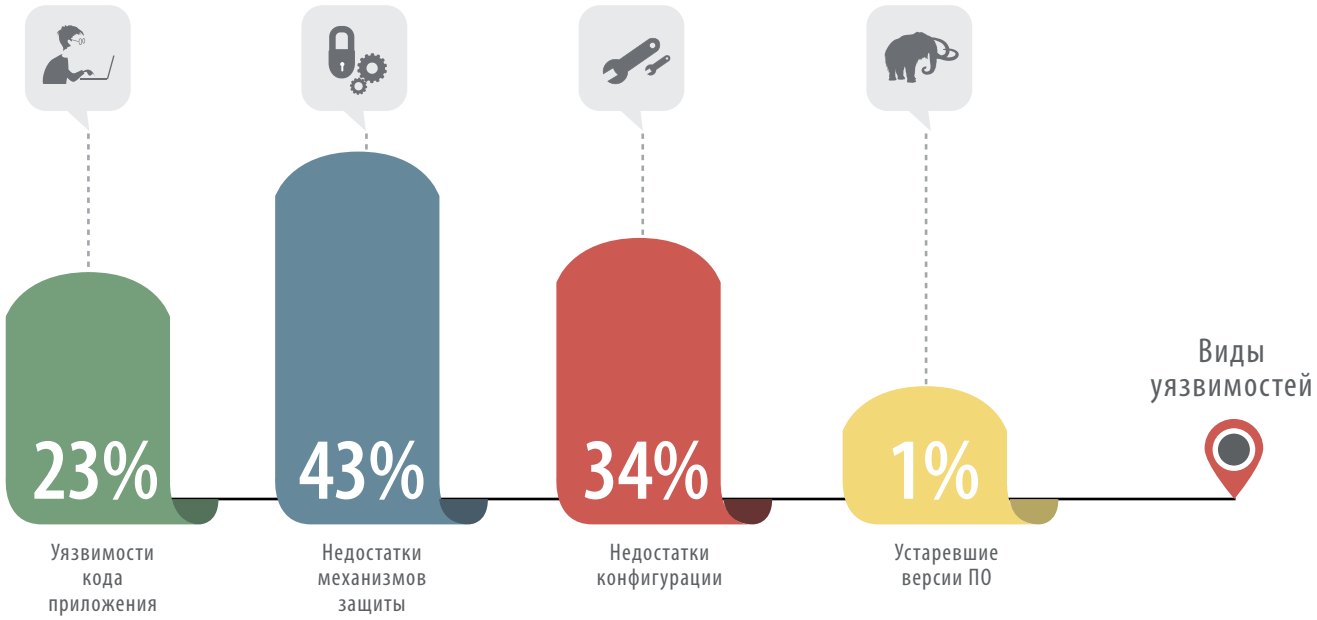
РАСПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ ПО СТЕПЕНИ РИСКА

В ходе анализа защищенности систем ДБО было выявлено множество уязвимостей различного уровня риска: 8% всех обнаруженных уязвимостей имеет высокую степень риска, больше всего уязвимостей имеют среднюю степень риска (51%), существенно количество уязвимостей низкой степени риска (41%).

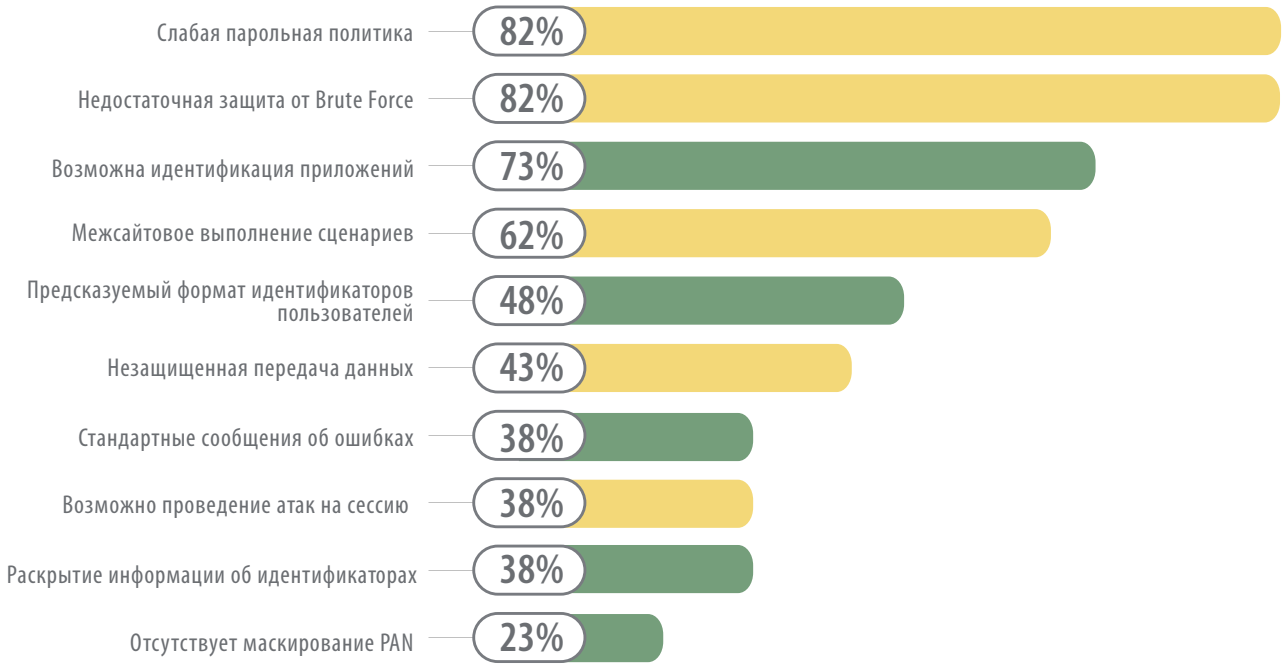


ОБЩАЯ СТАТИСТИКА ПО ВИДАМ УЯЗВИМОСТЕЙ

Выявленные уязвимости в большинстве случаев (43%) связаны с недостатками реализации механизмов защиты, а также с недостатками конфигурирования систем (34%), однако уязвимости на уровне кода веб-приложения также составляют значительную часть уязвимостей систем ДБО (23%).



ИТОГОВЫЙ РЕЙТИНГ ДЕСЯТИ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ УЯЗВИМОСТЕЙ СИСТЕМ ДБО



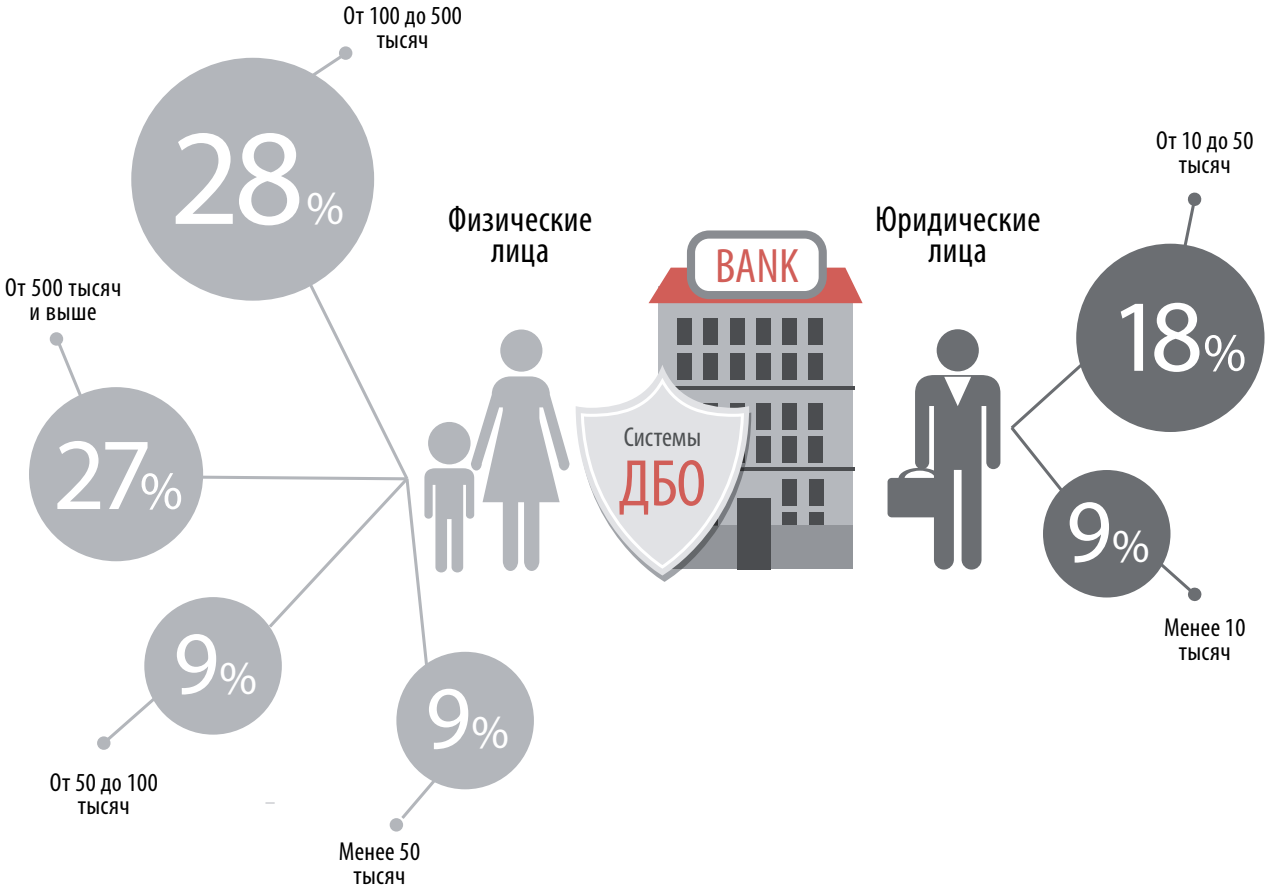
Наиболее распространенные уязвимости связаны с недостатками парольной политики (82%) и слабой защитой от атак, направленных на подбор учетных данных пользователей (82%). Также во многих системах присутствует раскрытие информации о версиях используемого программного обеспечения (73%), что облегчает планирование атак на уязвимую систему. Среди уязвимостей уровня кода веб-приложения широко распространены недостатки, приводящие к межсайтовому выполнению сценариев (64%), что делает возможным проведение атак на пользователей (например, с использованием методов социальной инженерии).

Самые распространенные уязвимости по результатам проведенного исследования имеют средний и низкий уровни риска. Однако сочетание подобных недостатков, а также наличие индивидуальных для конкретных систем критических уязвимостей может привести к серьезным последствиям, в том числе к получению полного контроля над системой. Описание и статистика наиболее опасных уязвимостей представлены в разд. 4 на стр. 18.

РЕАЛИЗУЕМЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ДБО

Более чем в 70% случаев было установлено, что злоумышленник может либо получить доступ к операционной системе или СУБД системы ДБО на уровне сервера, либо проводить несанкционированные транзакции на уровне отдельных пользователей. Уязвимости, приводящие к реализации подобных угроз, присутствуют как в системах собственной разработки, так и в системах, предоставленных вендорами. Зачастую для несанкционированного проведения транзакций на уровне пользователей систем ДБО злоумышленнику достаточно воспользоваться несколькими уязвимостями средней критичности, что позволяет сделать вывод: отсутствие уязвимостей высокой степени риска не означает, что система хорошо защищена.

КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ СИСТЕМ ДБО



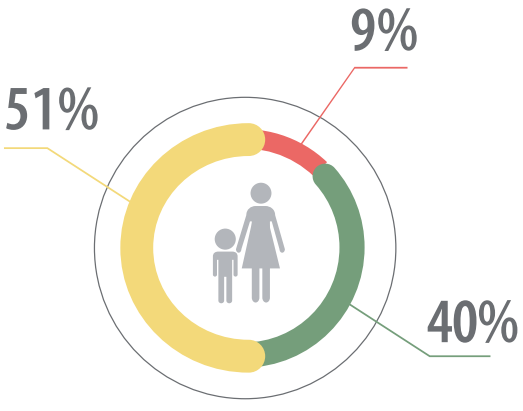
Согласно информации, полученной в ходе работ и из открытых источников, текущее количество пользователей в рассматриваемых системах ДБО в большинстве случаев исчисляется сотнями тысяч (для тестовых систем указывается количество пользователей системы после ее ввода в эксплуатацию).

Таким образом, в случае успешной реализации выявленных угроз информационной безопасности в отношении систем ДБО, под ударом могло оказаться множество пользователей подобных систем, а банки, в свою очередь, могли бы понести существенные финансовые потери за счет возмещения денежных средств клиентам.

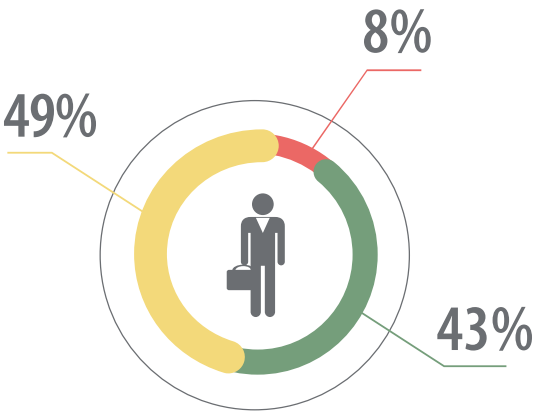
3.2. УЯЗВИМОСТИ СИСТЕМ ДБО ДЛЯ ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ

В системах для юридических лиц преобладают уязвимости в коде приложения (38% против 18% в системах для физических лиц), при этом в системах для физических лиц было выявлено больше уязвимостей, связанных с недостатками конфигурации (37% против 24%).

По распределению уровня критичности выявленных уязвимостей системы ДБО для физических и юридических лиц отличаются незначительно.



Распределение уязвимостей по степени риска (системы для физических лиц)

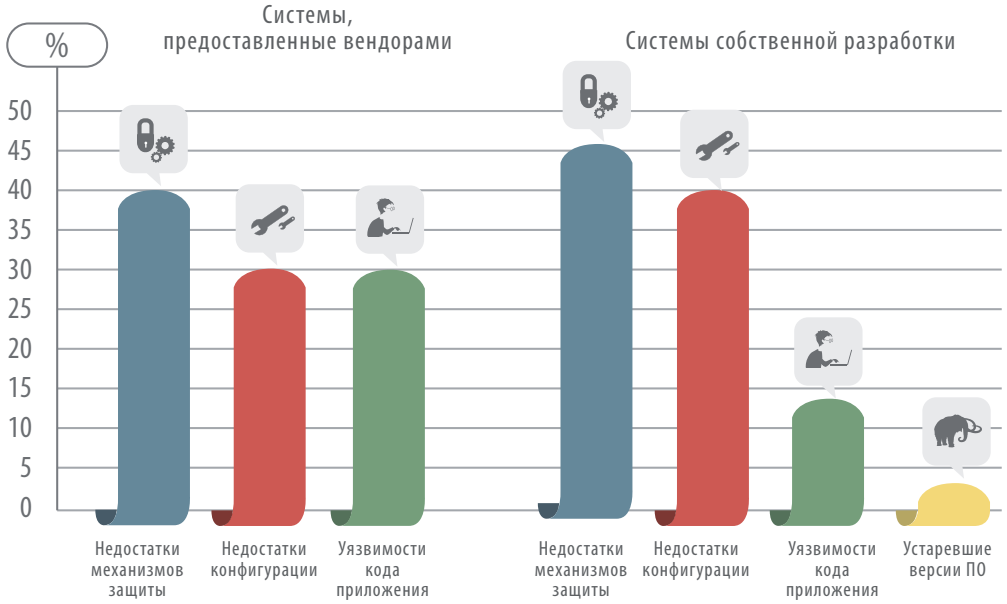


Распределение уязвимостей по степени риска (системы для юридических лиц)

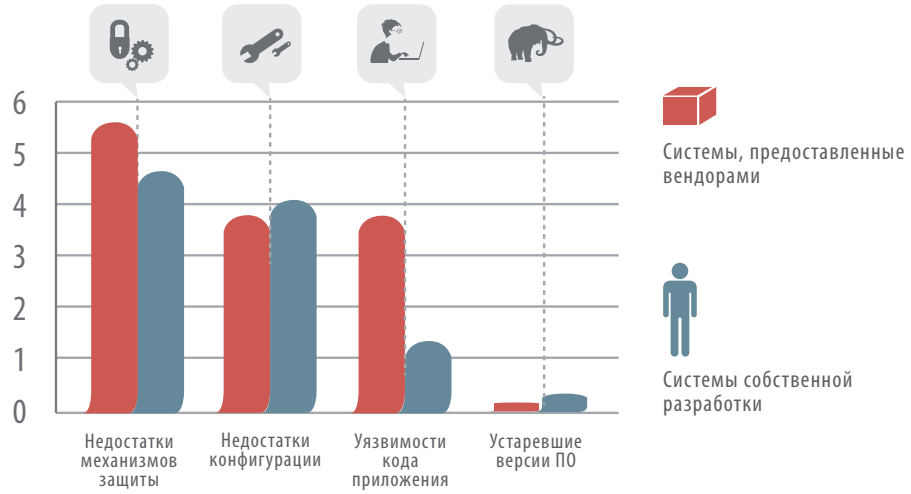
3.3. УЯЗВИМОСТИ СИСТЕМ ДБО ДЛЯ СИСТЕМ СОБСТВЕННОЙ РАЗРАБОТКИ И СИСТЕМ ОТ ПРОФЕССИОНАЛЬНЫХ ВЕНДОРОВ

Статистика по составу уязвимостей для систем, предоставленных разными категориями разработчиков (собственная разработка и системы от профессиональных вендоров), представлена ниже.

ДОЛИ РАЗЛИЧНЫХ УЯЗВИМОСТЕЙ В СИСТЕМАХ РАЗНОГО ТИПА

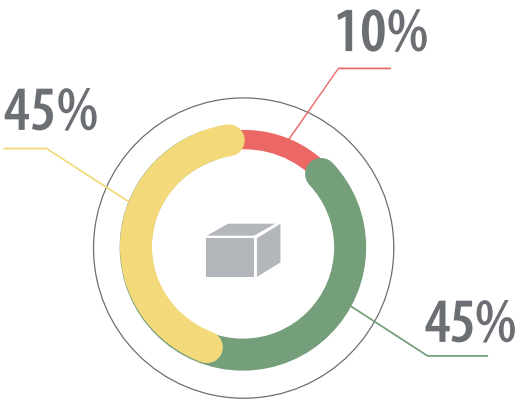


СРЕДНЕЕ КОЛИЧЕСТВО УЯЗВИМОСТЕЙ В РАЗЛИЧНЫХ СИСТЕМАХ

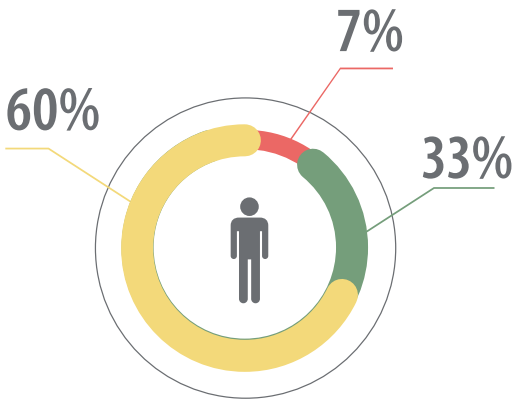


Стоит отметить, что уязвимости в коде приложения гораздо менее распространены в системах ДБО собственной разработки, чем в системах, предоставленных вендорами. Это можно объяснить тем, что при использовании систем, предоставляемых вендором, банк в основном полагается на поставщика продукта в вопросах контроля качества кода.

При этом сложная архитектура, кроссплатформенность и большое количество функций таких систем не всегда позволяют вендору обеспечить должный уровень защищенности на уровне кода приложения.



Распределение уязвимостей по степени риска для систем, предоставленных вендорами



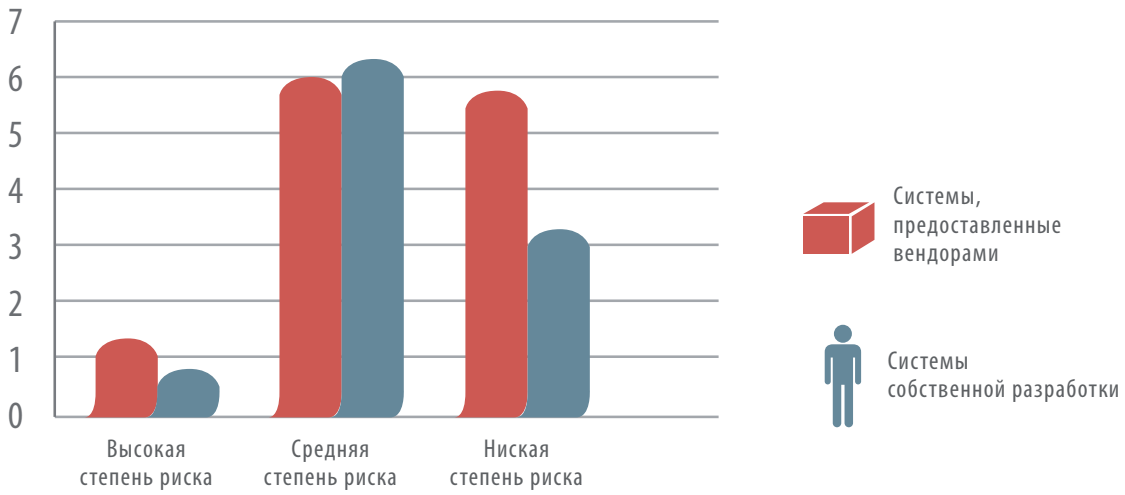
Распределение уязвимостей по степени риска для систем собственной разработки

Уязвимости высокой степени риска преобладают в системах, предоставленных вендорами. При этом системы собственной разработки не содержат уязвимостей высокой степени риска в коде приложения.

Рекомендуется проводить анализ защищенности систем ДБО до ввода эксплуатацию, а также регулярно тестировать системы в ходе эксплуатации, вне зависимости от разработчика.

Результаты проведенного исследования показывают, что приобретение системы ДБО у профессионального вендора не гарантирует высокого уровня защищенности

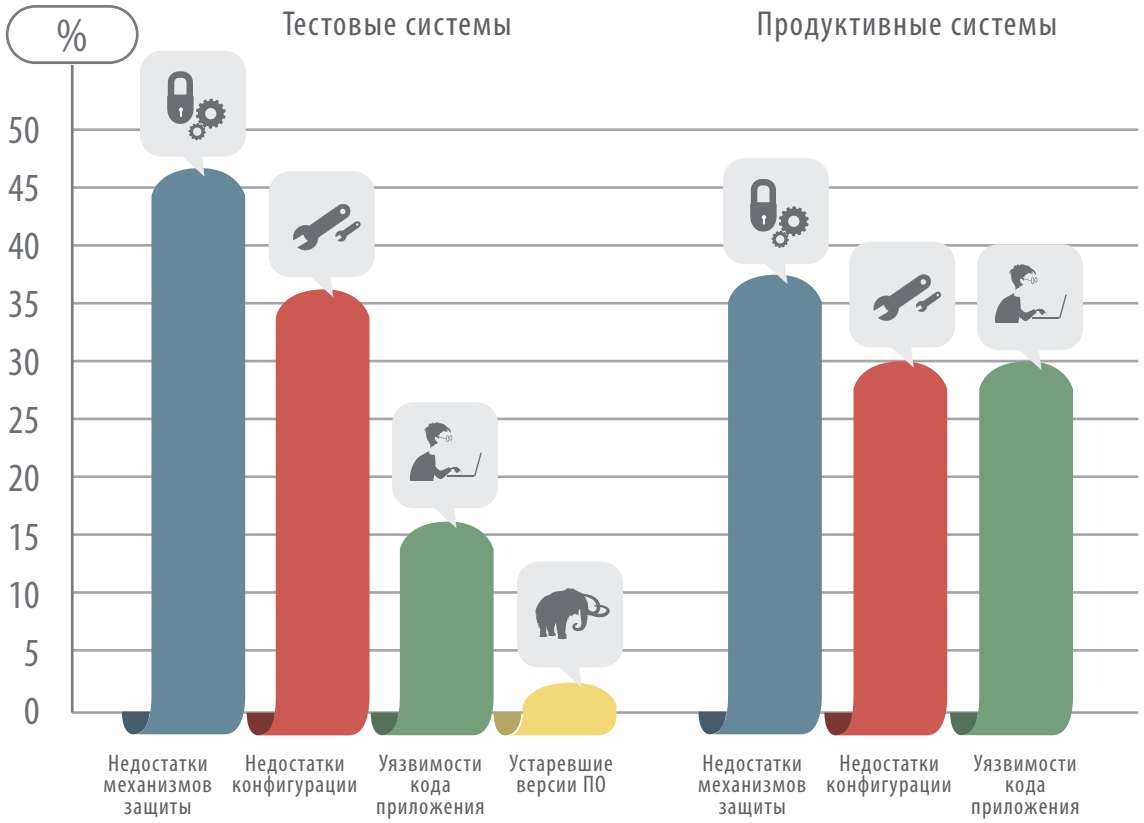
СРЕДНЕЕ КОЛИЧЕСТВО УЯЗВИМОСТЕЙ В РАЗЛИЧНЫХ СИСТЕМАХ



3.4. УЯЗВИМОСТИ ТЕСТОВЫХ И ПРОДУКТИВНЫХ СИСТЕМ ДБО

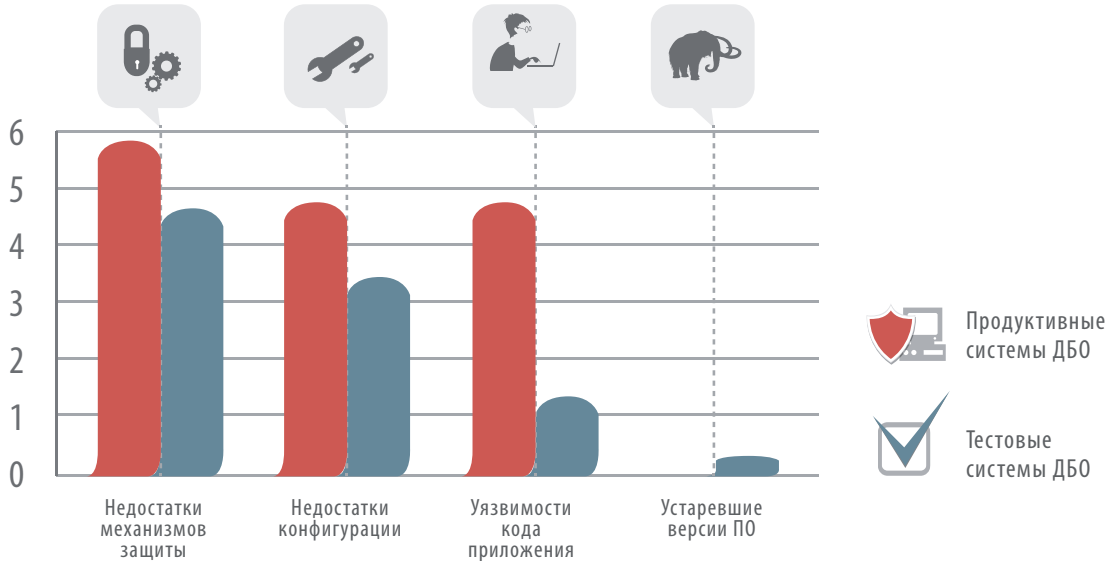
В данном разделе приведены результаты исследования уровня защищенности тестовых и продуктивных систем.

ДОЛЯ УЯЗВИМОСТЕЙ РАЗЛИЧНОГО ВИДА ДЛЯ ТЕСТОВЫХ И ПРОДУКТИВНЫХ СИСТЕМ



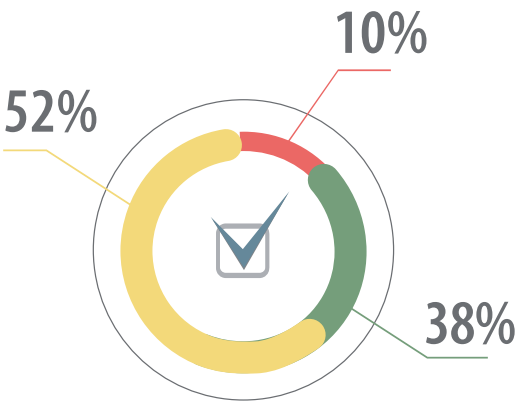
Согласно результатам исследования, для тестовых систем преобладают недостатки механизмов защиты (47% против 38% в продуктивных системах), в то время как для продуктивных систем было выявлено больше уязвимостей в коде приложения (31% против 16% в тестовых системах).

СРЕДНЕЕ КОЛИЧЕСТВО УЯЗВИМОСТЕЙ В ТЕСТОВЫХ И ПРОДУКТИВНЫХ СИСТЕМАХ

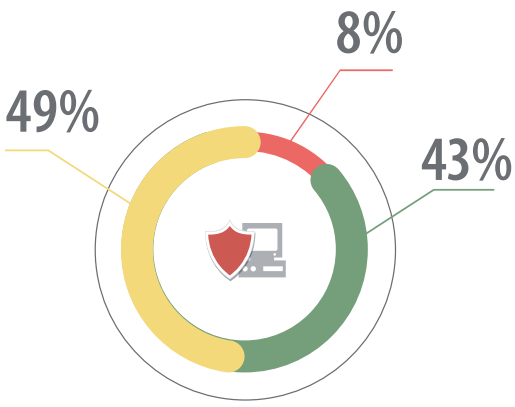


По всем категориям уязвимостей, кроме уязвимостей, связанных с устаревшими версиями ПО, продуктивные системы лидируют по среднему количеству уязвимостей. Это можно объяснить тем, что при вводе систем в эксплуатацию банки уделяют больше внимания выявлению уязвимостей в новой системе ДБО. А для уже функционирующих систем анализ защищенности проводится нерегулярно, и при выявлении уязвимостей сложность реализации уже функционирующих систем не всегда позволяет оперативно вносить изменения в приложения.

Стоит отметить, что единственная обнаруженная уязвимость, связанная с устаревшей версией ПО, найдена в одной из тестовых систем ДБО, находящихся на стадии приемки в эксплуатацию. Данная уязвимость имеет высокую степень риска и может привести к получению злоумышленником полного контроля над системой.



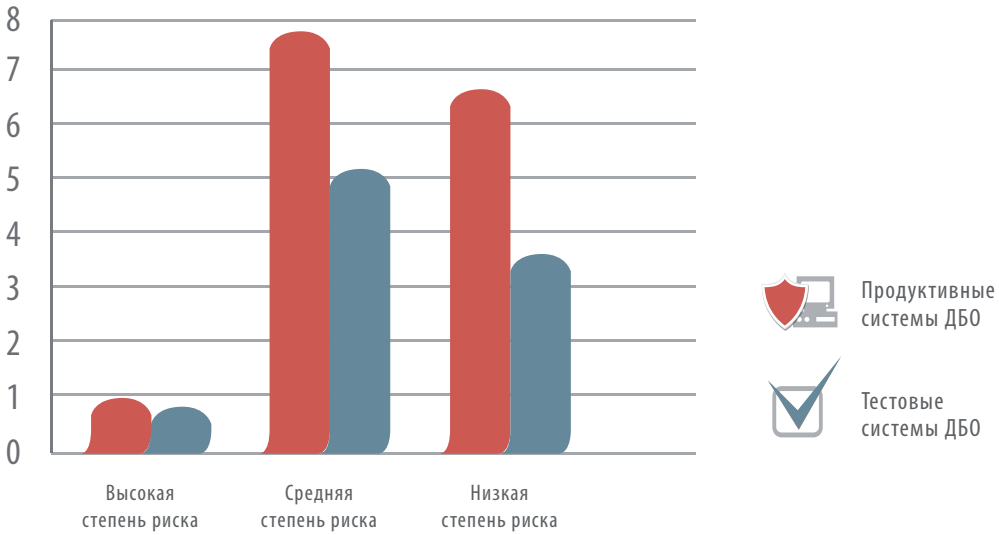
Распределение уязвимостей по степени риска для тестовых систем



Распределение уязвимостей по степени риска для продуктивных систем

СРЕДНЕЕ КОЛИЧЕСТВО УЯЗВИМОСТЕЙ РАЗЛИЧНОГО УРОВНЯ РИСКА В ТЕСТОВЫХ И ПРОДУКТИВНЫХ СИСТЕМАХ

Доля уязвимостей различного уровня риска для тестовых и продуктивных систем примерно одинакова. Однако сравнение среднего количества уязвимостей различного уровня риска для этих двух категорий систем показывает, что продуктивные системы более уязвимы.



Уязвимости как высокой, так и средней и низкой степеней риска преобладают в продуктивных системах, находящихся в эксплуатации.

Результаты проведенного исследования показывают не только необходимость анализа защищенности системы ДБО перед вводом в эксплуатацию, но и необходимость регулярного тестирования в процессе самой эксплуатации.

4 ОБЗОР НАИБОЛЕЕ КРИТИЧЕСКИХ УЯЗВИМОСТЕЙ

НАИБОЛЕЕ КРИТИЧЕСКИЕ УЯЗВИМОСТИ СИСТЕМ ДБО

Перечень всех уязвимостей с высокой степенью риска, обнаруженных в системах ДБО в процессе проведенных исследований, дан на диаграмме. Представлено процентное соотношение систем, содержащих критические уязвимости, и общего количества рассмотренных систем.

В целом, **уязвимости высокой критичности были выявлены в каждой второй системе**. Некоторые примеры эксплуатации критических уязвимостей в системах ДБО приведены ниже.

4.1. ИЗБЫТОЧНАЯ ФУНКЦИОНАЛЬНОСТЬ

Интерфейс администрирования веб-приложения одной из систем ДБО позволял выполнять произвольный код, что является примером избыточной функциональности. Злоумышленник мог получить доступ к панели администрирования в результате использования недостатков механизма авторизации и далее из панели администрирования выполнять произвольные команды на сервере. В результате эксплуатации уязвимости и последующего повышения привилегий в ходе исследования был получен полный контроль над системой.

4.2. ВНЕДРЕНИЕ ВНЕШНИХ СУЩНОСТЕЙ XML (XXE)

«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.

Так, в одной из исследуемых систем использование данной уязвимости и уязвимости «Предсказуемое расположение каталогов и файлов, содержащих важные данные» позволило получить доступ к файлам журналов системы ДБО. В файлах содержалась информация об идентификаторах пользователей и паролях в открытом виде (уязвимость «Хранение чувствительной информации в файлах журналов»). При получении доступа к личному кабинету тестового пользователя с использованием обнаруженных данных была получена возможность несанкционированно проводить финансовые транзакции: информация об одноразовых паролях, высылаемая пользователю в SMS, дублировалась в открытом виде в файле журнала, доступном злоумышленнику.

4.3. 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: это позволяет злоумышленнику осуществлять атаку, направленную на изменение логики запроса к базе данных путем внедрения произвольных операторов SQL. Злоумышленник в результате успешной эксплуатации сможет осуществлять несанкционированные действия:

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

В одной из исследованных систем эксплуатация уязвимости типа «Внедрение операторов SQL» позволяла работать с базой данных системы ДБО с правами приложения, то есть проводить любые транзакции без знания учетных данных пользователей и одноразовых паролей. Стоит отметить, что возможен сценарий эксплуатации подобной уязвимости, который останется незамеченным для антифрод-систем, поскольку с точки зрения подобных систем изменения в содержимом базы данных осуществляются приложением системы ДБО штатным образом.

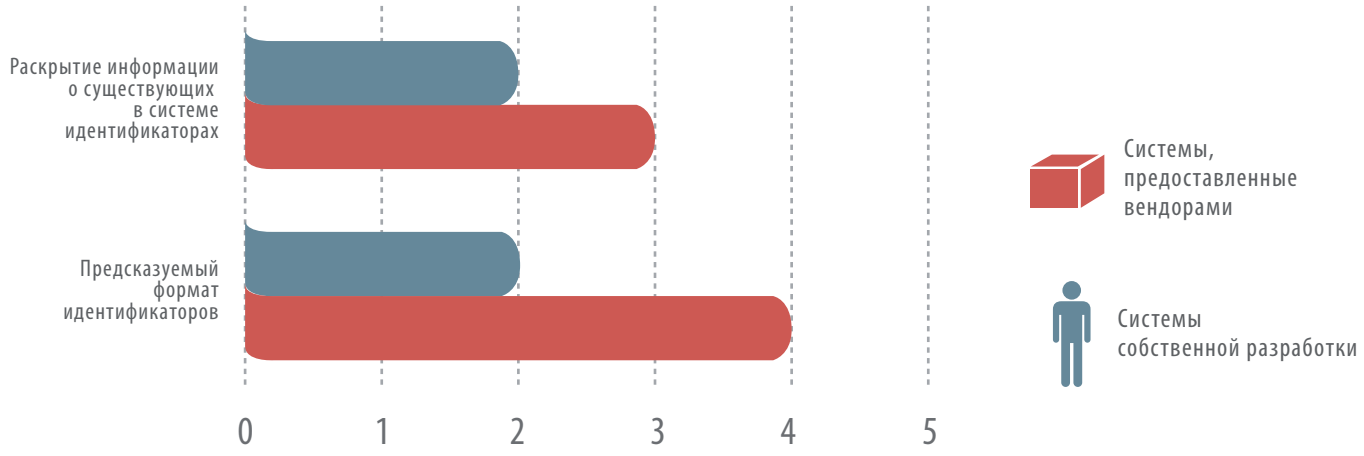
5 НЕДОСТАТКИ МЕХАНИЗМОВ ИДЕНТИФИКАЦИИ

Более 60% исследованных систем ДБО содержали как минимум один из следующих недостатков механизма идентификации пользователей:

- предсказуемый формат идентификаторов пользователей;
- 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 и авторизации (см. разделы 6 и 7) может сыграть существенную роль для получения несанкционированного доступа к личным кабинетам пользователей и последующего проведения транзакций. Кроме того, знание идентификаторов пользователей зачастую может позволить злоумышленнику провести атаку, направленную на отказ в обслуживании, в случае если в системе ДБО используется блокировка учетных записей пользователей после нескольких попыток неправильного ввода пароля.

НЕДОСТАТКИ МЕХАНИЗМОВ ИДЕНТИФИКАЦИИ



5.1. ПРЕДСКАЗУЕМЫЙ ФОРМАТ ИДЕНТИФИКАТОРОВ

Наиболее распространенным недостатком механизма идентификации исследованных систем ДБО является предсказуемость формата идентификатора учетной записи. Указанная уязвимость обнаружена более чем в половине рассмотренных систем.

Формат идентификаторов систем ДБО зачастую позволяет злоумышленнику, узнав несколько существующих в системе идентификаторов (например, прочитав содержимое выброшенных квитанций по проведенным транзакциям, или с помощью перебора), предсказать другие существующие в системе идентификаторы, вычислив механизм их формирования системой. Наиболее распространенные предсказуемые идентификаторы это:

- идентификаторы, состоящие только из набора цифр (например: 344985127) — встретились в 27% случаев;
- идентификаторы, состоящие из набора цифр и постоянного постфикса или префикса (например: 211113AA, c1231254) — также встретились в 27% случаев.

Зачастую в качестве цифрового идентификатора используется уникальный номер клиента (УНК), который при этом может иметь небольшую длину (7 символов). Идентификаторы подобного формата могут быть легко подобраны злоумышленником.

Стоит отметить, что в 37% рассмотренных систем использовались форматы идентификаторов, подбор которых затруднителен. Для одной из тестовых систем анализ идентификаторов не проводился в связи с тем, что механизм идентификации на момент проведения работ по анализу защищенности еще не был определен владельцем.

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 распространенных словарных комбинаций в качестве идентификатора (таких как qwerty).

5.2. РАСКРЫТИЕ ИНФОРМАЦИИ ОБ ИДЕНТИФИКАТОРАХ

Еще одним распространенным недостатком механизма идентификации является раскрытие информации о существующих в системе идентификаторах пользователей, которое было выявлено для 45% систем. Данная уязвимость обусловлена возможностью определять существующие в системе учетные записи пользователей по ответам сервера.

Зачастую раскрытие информации встречается в сценариях регистрации новых пользователей или смены пароля, когда система ДБО выдает различный результат для зарегистрированных и незарегистрированных пользователей.

Пример ответа сервера с раскрытием информации представлен в листинге.

```
HTTP/1.1 200 OK
***
<Message>1|Имя уже существует в системе. Укажите другое имя.</Message >
```

Стоит отметить, что в 36% случаев системы ДБО содержали оба недостатка: как раскрытие информации об идентификаторах, так и предсказуемый формат идентификаторов.

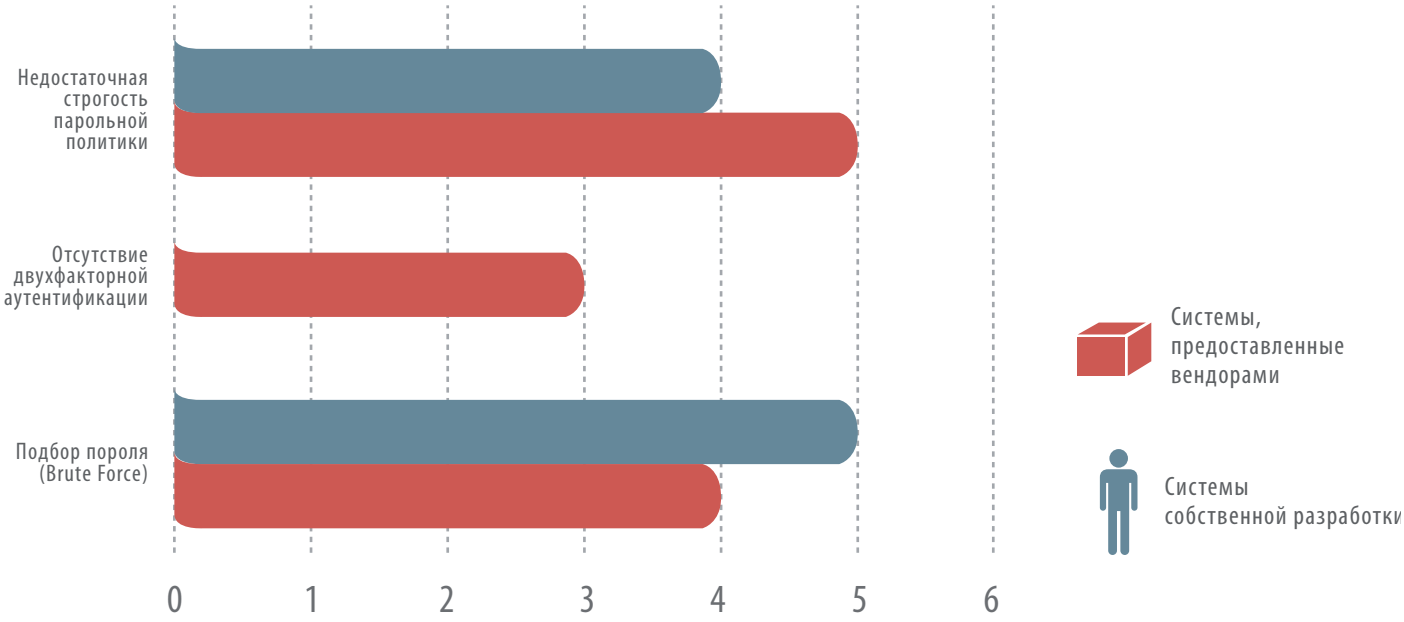
6 НЕДОСТАТКИ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ

Для большинства рассмотренных систем (82%) аутентификация пользователей при входе в систему осуществляется по идентификатору и паролю. Двухфакторная аутентификация, требующая дополнительного предъявления аппаратного токена, использовалась только в двух системах для юридических лиц типа «Клиент-банк».

Большинство выявленных недостатков механизмов аутентификации систем ДБО можно разделить на следующие основные категории:

- недостатки парольной политики;
- недостаточная защита от подбора учетных данных (Brute Force);
- отсутствие двухфакторной аутентификации.

Уязвимости, связанные с недостатками механизмов аутентификации «Недостаточная защита от подбора учетных данных (Brute Force)» и «Недостатки парольной политики» являются двумя самыми распространенными уязвимостями систем ДБО.



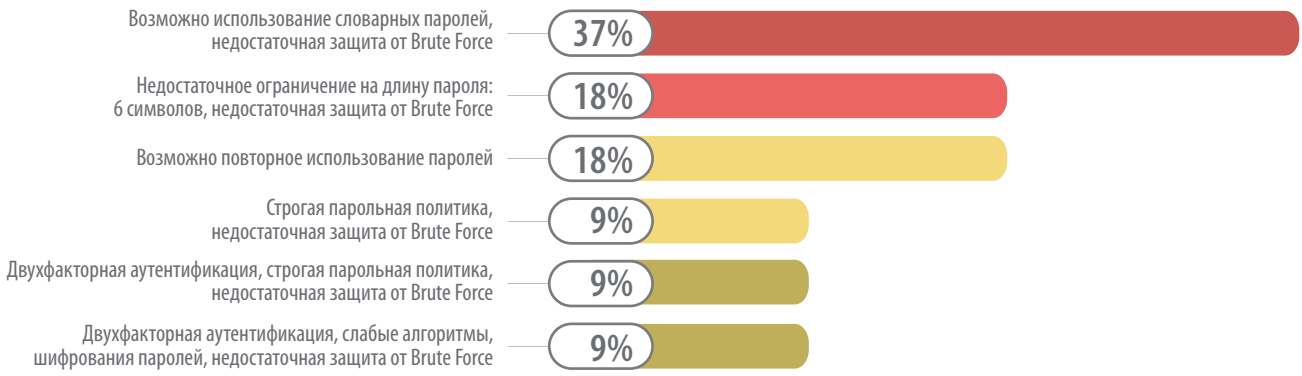
6.1. НЕДОСТАТКИ ПАРОЛЬНОЙ ПОЛИТИКИ

Среди недостатков парольной политики наиболее распространенными являются следующие:

- недостаточное ограничение длины пароля: возможен выбор пароля длиной менее 8 символов;
- отсутствие проверки на использование пользователями словарных паролей (например, 111111, P@ssw0rd);
- возможность задания пароля, который уже использовался ранее.

Подобные недостатки в совокупности с недостаточной защитой от атак, направленных на подбор пароля, делают возможными атаки на пользователей, приводящие к успешному входу злоумышленника в личные кабинеты клиентов банков. Поскольку аутентификация является первым барьером для доступа к системе, рекомендуется внимательно относиться к реализации парольной политики, исключая возможность использования коротких и словарных паролей. Срок действия пароля должен быть ограничен, при этом пользователь не должен иметь возможность выбрать новый пароль, совпадающий с последними из предыдущих.

НЕДОСТАТКИ МЕХАНИЗМА АУТЕНТИФИКАЦИИ
(доля уязвимых систем, в %)



6.2. НЕДОСТАТОЧНАЯ ЗАЩИТА ОТ ПОДБОРА УЧЕТНЫХ ДАННЫХ

Что касается недостаточной защиты от атак, направленных на подбор пароля, зачастую банками используется механизм временной или постоянной блокировки учетных записей после нескольких неудачных попыток ввода пароля, однако данный механизм не позволяет в полной мере защититься от подбора. В случае, когда возможно задание словарных паролей, злоумышленник может провести атаку, направленную на подбор учетных записей по заданному словарному паролю. Кроме того, некорректно реализованная блокировка может привести к отказу в обслуживании для легальных пользователей системы.

На диаграмме представлена статистика по недостаткам парольной политики и механизмам защиты от атак, направленных на подбор учетных данных пользователей. Технология Completely Automatic Public Turing test to tell Computers and Humans Apart (CAPTCHA) в уязвимых системах не используется. Данный механизм запрашивает у пользователя ввод отображенной на экране информации при частых попытках ввода неверных учетных данных и 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 (Brute Force). При реализации блокировки рекомендуется учитывать различные факторы, такие как временной промежуток между последовательными попытками входа, IP-адрес источника, факты подбора не только паролей, но и идентификаторов.

6.3. ОТСУТСТВИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

В большинстве рассмотренных систем 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 авторизацией на этапе проведения транзакции, как правило, позволяет обеспечить приемлемый уровень безопасности. Однако для некоторых систем было выявлено, что дополнительная проверка принадлежности учетных данных легитимному пользователю не осуществляется ни на стадии аутентификации, ни на стадии авторизации. В данном случае отсутствие двухфакторной аутентификации рассматривалось как уязвимость, поскольку подобная реализация механизмов защиты создает повышенные риски для системы ДБО.

В общем случае даже для систем, в которых отсутствуют первые два описанные в данном разделе недостатка и реализована двухфакторная авторизация, рекомендуется рассмотреть возможность перехода к двухфакторной аутентификации. Данная мера позволит снизить риски несанкционированного доступа к личным кабинетам пользователей, в которых, как правило, содержатся персональные данные, информация о счетах и получателях платежей. Кроме того, при наличии пользовательского доступа злоумышленник получает возможность развивать атаку не только в направлении обхода авторизации и проведения транзакции от имени пользователя, но и с целью выявления и эксплуатации уязвимостей серверных компонентов системы (например, уязвимостей типа «Внедрение внешних сущностей XML» и «Внедрение операторов SQL»).

7 НЕДОСТАТКИ МЕХАНИЗМОВ АВТОРИЗАЦИИ

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 идентификатор пользователя или уникальный токен запроса. Во всех исследованных системах идентификатор сессии обладал достаточной энтропией, что делает подбор идентификатора затруднительным. Однако для ряда систем сессия была недостаточно защищена от перехвата и последующего использования злоумышленником.

- В 27% случаев отсутствовала привязка сессии к IP-адресу и браузеру клиента, еще в 18% систем присутствовала привязка сессии к IP-адресу, но не к браузеру.
- В каждой третьей системе была возможна параллельная работа с одной учетной записью.
- В двух рассмотренных системах необходимые для авторизации данные передавались небезопасным образом — в POST- и GET-параметрах (таким образом данные могли быть закэшированы поисковыми системами или перехвачены при переходе на внешние ресурсы)

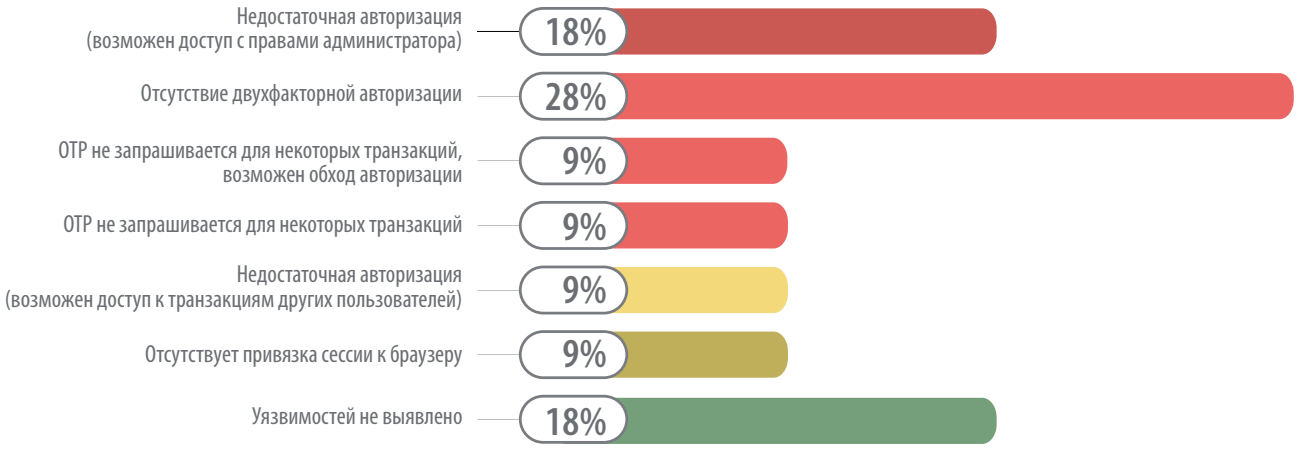
Кроме того, для cookie-параметров, содержащих идентификатор сессии и другие важные данные, зачастую не были установлены свойства secure и HttpOnly, что делало возможным проведение атак на сессии пользователей (см. разд. 8). При этом во многих системах данные передавались незащищенным образом и могли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

Для защиты процесса проведения транзакций в большинстве рассмотренных систем применялась двухфакторая авторизация с использованием одноразовых паролей (one time passwords, OTP). Однако для ряда систем двухфакторная авторизация отсутствовала вовсе либо была некорректно реализована. Так, в 18% систем было выявлено, что двухфакторная авторизация используется не для всех транзакций.

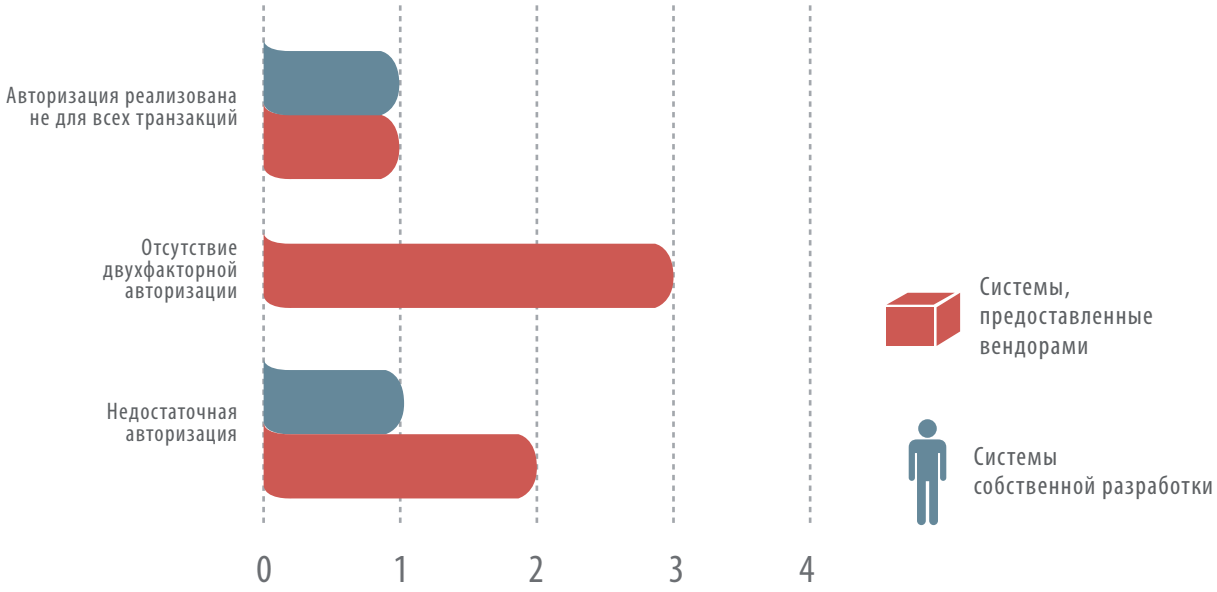
Наиболее распространенными серьезными недостатками механизмов авторизации систем ДБО, согласно проведенному исследованию, являются:

- недостаточная строгость авторизации,
- отсутствие двухфакторной авторизации,
- использование двухфакторной авторизации не для всех транзакций.

НЕДОСТАТКИ МЕХАНИЗМА АВТОРИЗАЦИИ
(доля уязвимых систем в %)



НЕДОСТАТКИ МЕХАНИЗМА АВТОРИЗАЦИИ СИСТЕМ ДБО РАЗЛИЧНЫХ ВИДОВ РАЗРАБОТКИ



7.1. НЕДОСТАТОЧНАЯ АВТОРИЗАЦИЯ

Недостаточная строгость авторизации — наиболее опасная уязвимость, обнаруженная в механизмах авторизации исследованных систем ДБО. Уязвимость обнаружена в каждой третьей системе, причем в 18% исследованных систем злоумышленник получает доступ к системе с правами администратора. Уязвимость обусловлена некорректной организацией механизма авторизации в сценариях администрирования и позволяет неавторизированным пользователям обращаться к сценариям системы администрирования и обращаться к элементам управления (к примеру, просматривать или удалять данные). Доступ к системе администрирования может быть вовсе не ограничен для неавторизированных пользователей, что позволит им использовать функции и элементы управления приложением (в том числе, выполнение команд операционной системы). К примеру, в одной из систем неавторизированный пользователь может вызывать системные функции. Вызвав функцию переназначения пути вывода отладочной информации, нарушитель может прочитать все данные о подписанных транзакциях в системе. В совокупности с другими уязвимостями эксплуатация уязвимости злоумышленником может привести к серьезным последствиям, вплоть до получения им полного контроля над системой. Для устранения уязвимости необходимо исправить все недостатки в коде приложения.

7.2. ОТСУТСТВИЕ ДВУХФАКТОРНОЙ АВТОРИЗАЦИИ

Использование одноразовых паролей при проведении транзакций позволяет повысить безопасность системы в части осуществления несанкционированного доступа. Но, как показало исследование, для трети рассмотренных систем ДБО двухфакторная авторизация не использовалась в принципе. Злоумышленник получал возможность беспрепятственно осуществлять транзакции при получении доступа с правами пользователя (например, в результате подбора учетных данных или перехвата сессии).

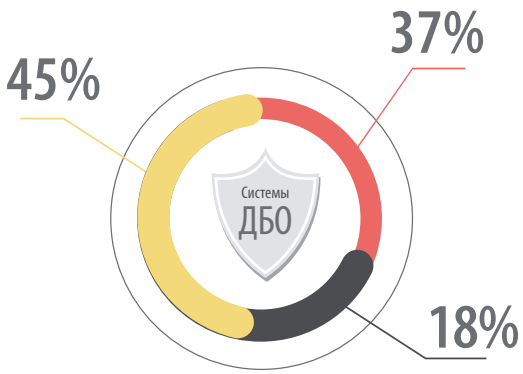
7.3. ИСПОЛЬЗОВАНИЕ ДВУХФАКТОРНОЙ АВТОРИЗАЦИИ НЕ ДЛЯ ВСЕХ ТРАНЗАКЦИЙ

Использование двухфакторной авторизации не для всех типов транзакций по сути идентично отсутствию двухфакторной авторизации как таковой. Если существуют некоторые типы транзакций, для которых двухфакторная аутентификация не требуется, злоумышленник может использовать их для вывода денежных средств со счетов пользователей.

8 УЯЗВИМОСТИ НА УРОВНЕ КОДА ВЕБ-ПРИЛОЖЕНИЙ

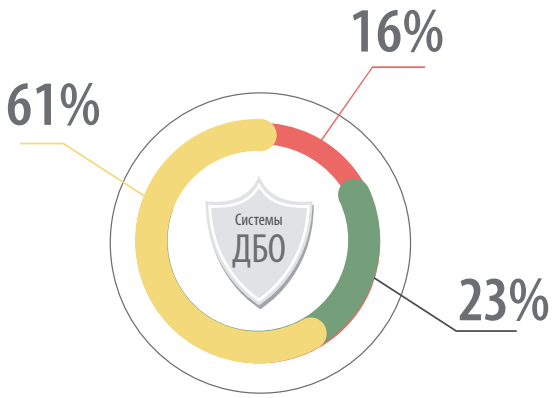
ДОЛИ СИСТЕМ ДБО С УЯЗВИМОСТЯМИ РАЗЛИЧНЫХ УРОВНЕЙ РИСКА

Среди рассмотренных систем ДБО 82% содержат уязвимости, связанные с ошибками в коде веб-приложения. На рисунке представлена доля уязвимых систем среди всех рассмотренных систем ДБО по максимальному уровню риска: 37% систем содержат уязвимости высокого уровня риска и ниже, 45% систем содержат уязвимости среднего и низкого уровней риска, 18% — уязвимостей не выявлено.

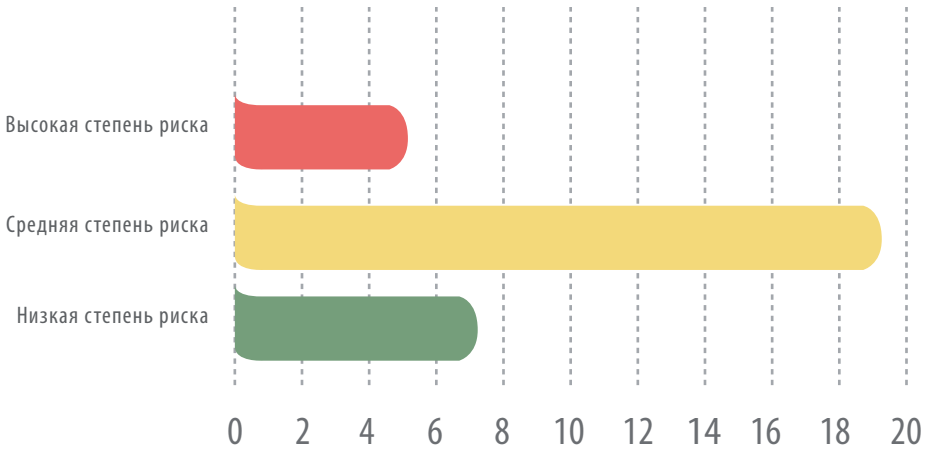


РАСПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ УРОВНЯ ПРИЛОЖЕНИЯ ПО СТЕПЕНИ РИСКА

16% всех найденных уязвимостей уровня приложения относятся к уязвимостям высокой степени риска.



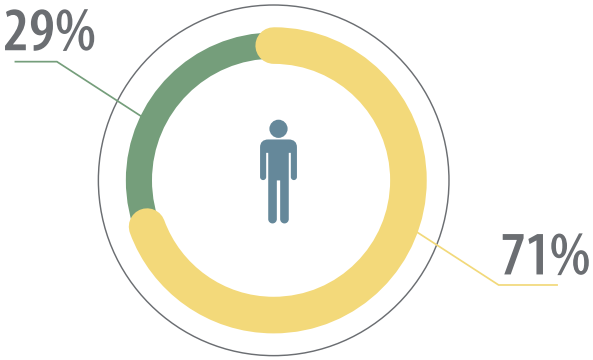
КОЛИЧЕСТВО УЯЗВИМОСТЕЙ, ОБНАРУЖЕННЫХ В КОДЕ ВЕБ-ПРИЛОЖЕНИЙ



8.1. УЯЗВИМОСТИ ВЕБ-ПРИЛОЖЕНИЙ В СИСТЕМАХ СОБСТВЕННОЙ РАЗРАБОТКИ И В СИСТЕМАХ, ПОСТАВЛЯЕМЫХ ВЕНДОРАМИ

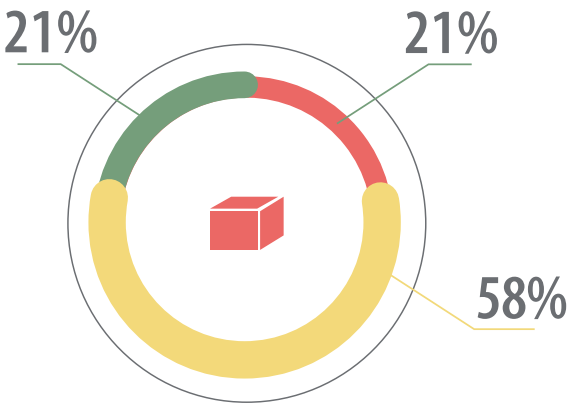
СТЕПЕНЬ РИСКА УЯЗВИМОСТЕЙ СИСТЕМ СОБСТВЕННОЙ РАЗРАБОТКИ

Уязвимости присутствуют как в системах ДБО собственной разработки, так и в системах, поставляемых известными вендорами. Проведенные исследования показали, что системы ДБО собственной разработки содержат значительно меньше уязвимостей в коде приложения, при этом вовсе не содержат уязвимостей высокой степени риска.

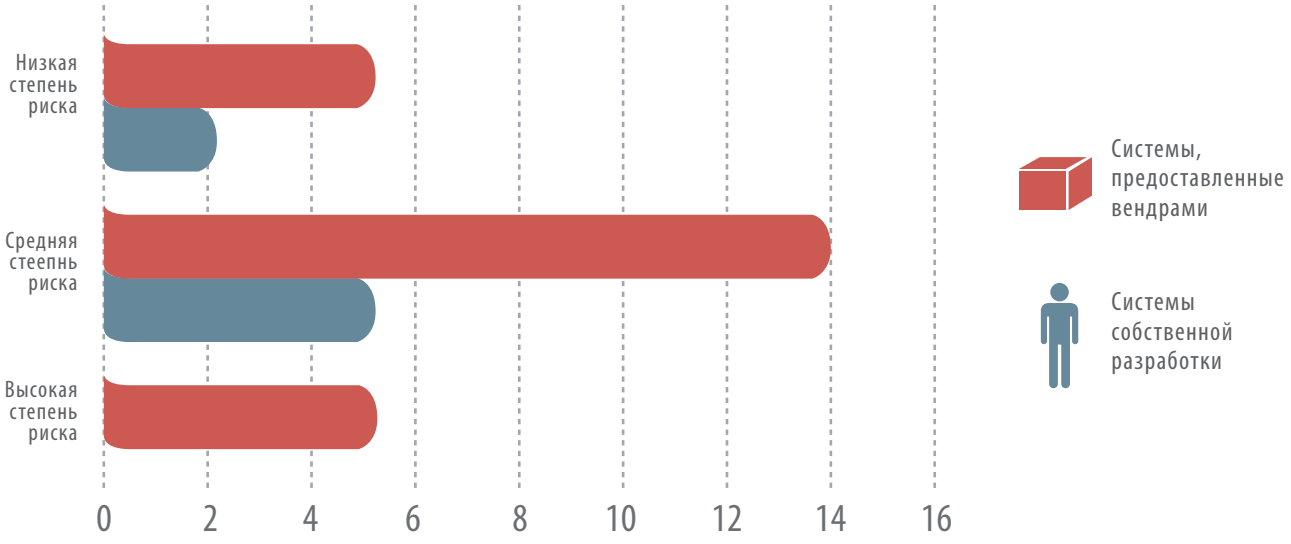


СООТНОШЕНИЕ УЯЗВИМОСТЕЙ СИСТЕМ, ПРЕДОСТАВЛЯЕМЫХ ВЕНДОРАМИ

Все найденные уязвимости высокой степени риска относятся к системам, поставляемым известными вендорами.

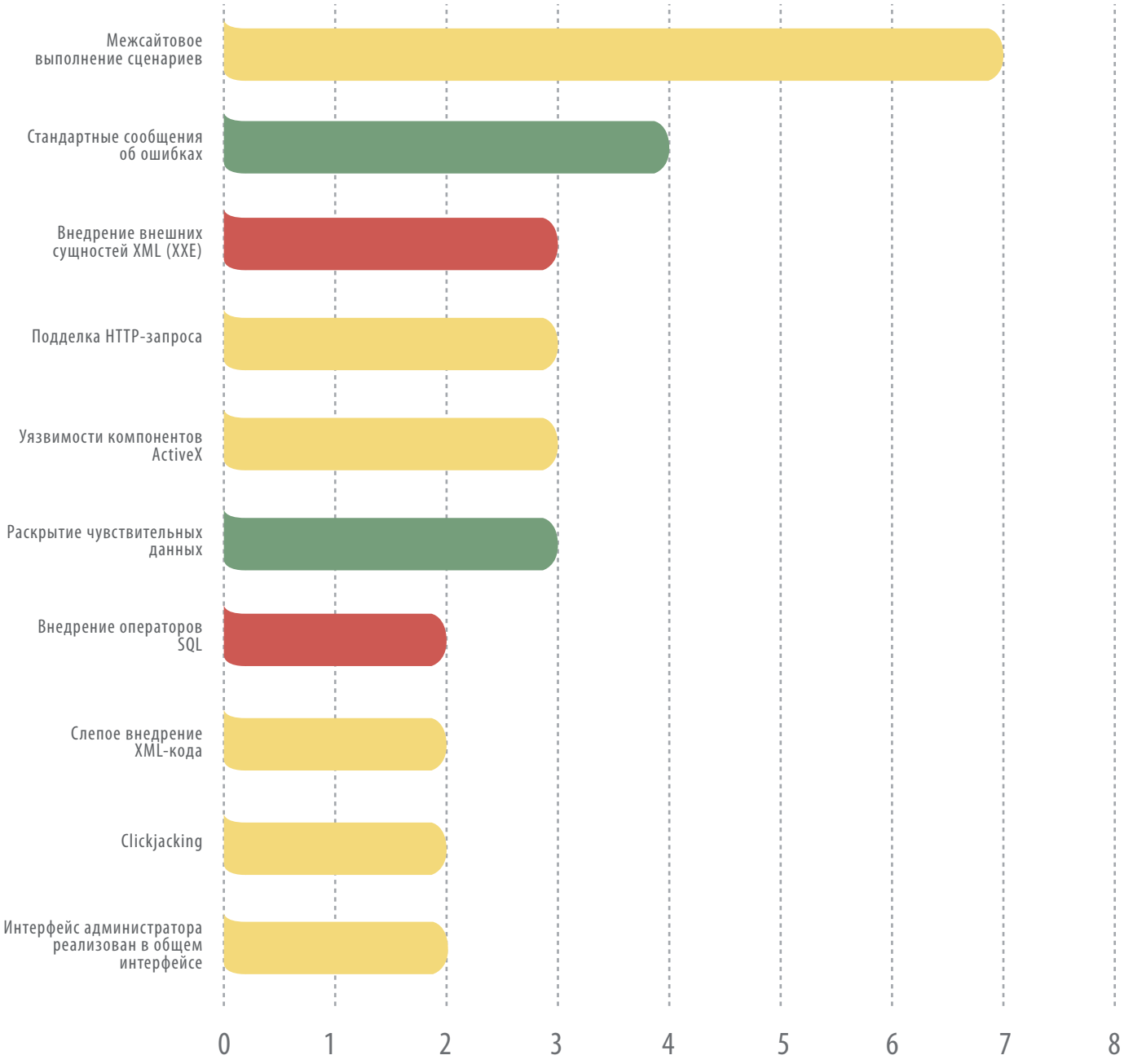


ОБЩЕЕ КОЛИЧЕСТВО ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ УРОВНЯ ПРИЛОЖЕНИЯ

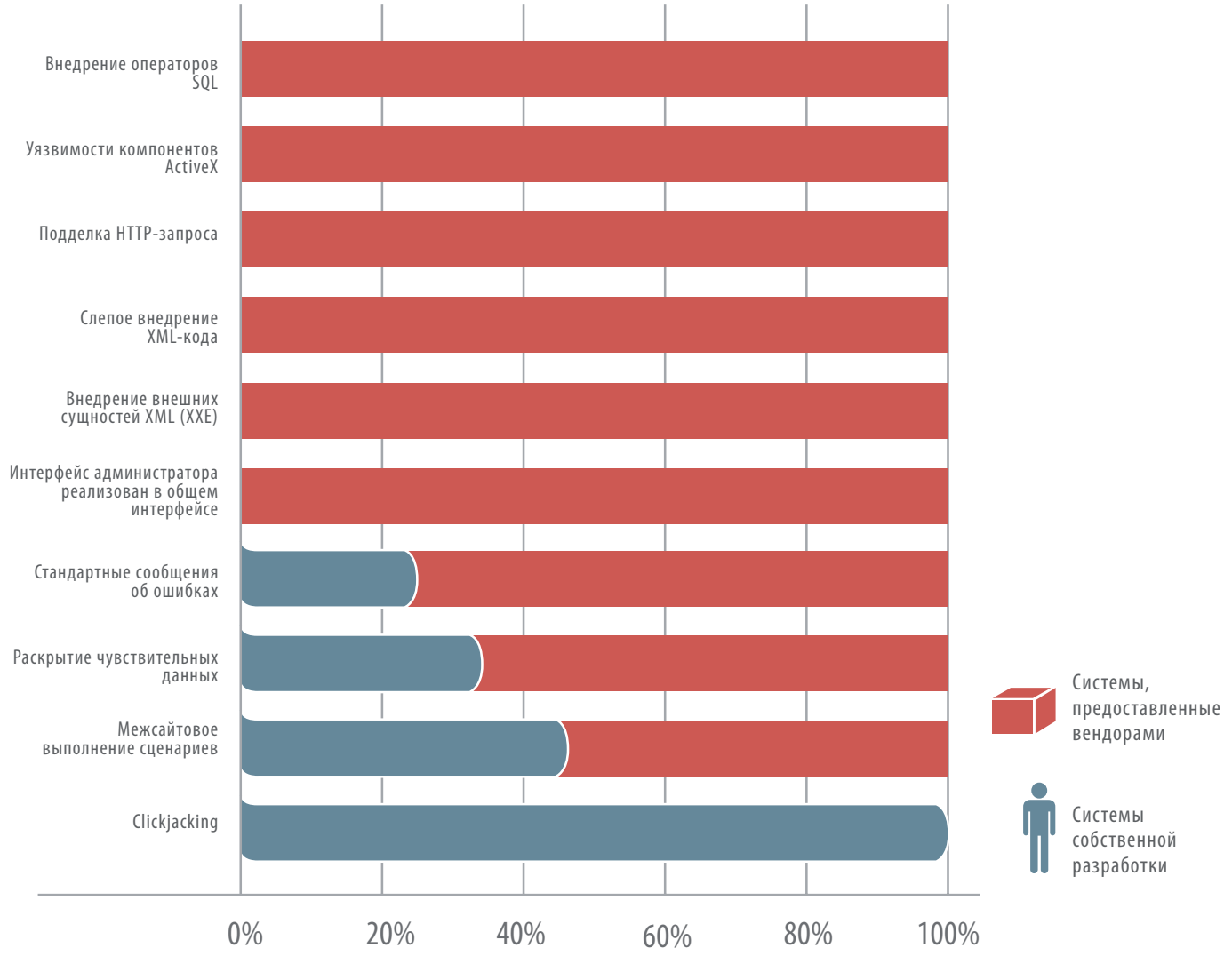


8.2. НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ УРОВНЯ ВЕБ-ПРИЛОЖЕНИЯ

КОЛИЧЕСТВО СИСТЕМ ДБО, В КОТОРЫХ БЫЛИ ОБНАРУЖЕНЫ УЯЗВИМОСТИ УРОВНЯ КОДА ПРИЛОЖЕНИЯ



СООТНОШЕНИЕ УЯЗВИМОСТЕЙ В СИСТЕМАХ РАЗЛИЧНЫХ ТИПОВ



Множественные уязвимости типа «Межсайтовое выполнение сценариев» обнаружены более чем в половине исследованных систем ДБО. Таким образом, каждая вторая система позволяет проводить атаки на клиентов. Наличие данной уязвимости обусловлено недостаточной проверкой веб-приложением данных, поступающих от пользователя: это позволяет злоумышленнику внедрить в браузер пользователя произвольные HTML-теги, включая сценарии на языке JavaScript.

Злоумышленник получает возможность проводить атаки на клиентов системы с использованием фишинга — с целью хищения учетных данных пользователей и получения несанкционированного доступа к системе, а также распространять вредоносный код через компьютеры пользователей системы ДБО. В одной из систем, в которой отсутствовала двухфакторная авторизация при проведении транзакций, данная уязвимость могла быть использована для массового вывода средств со счетов пользователей.

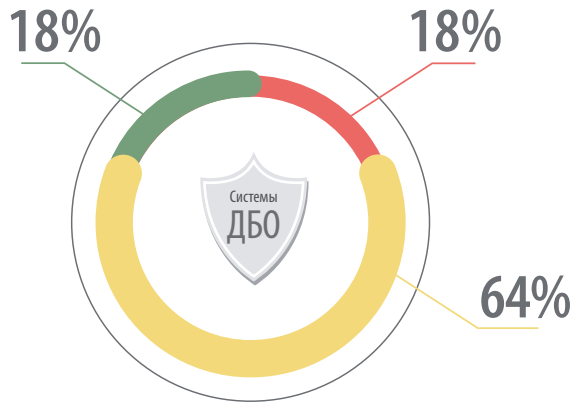
Примером другой уязвимости, связанной с реализацией атак на клиентов, является уязвимость компонентов ActiveX. Уязвимости данного вида были обнаружены во всех трех системах типа «Клиент-банк», предоставленных вендорами. Эксплуатация данных уязвимостей осуществляется при помощи атак других типов, таких как «Межсайтовое выполнение сценариев» и «Внедрение внешних сущностей XML». Используя различные методы компонентов ActiveX, злоумышленник может записать или прочитать произвольный файл на компьютере пользователя.

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

9 НЕДОСТАТКИ КОНФИГУРАЦИИ

ДОЛИ СИСТЕМ С НЕДОСТАТКАМИ КОНФИГУРАЦИИ
(ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА)

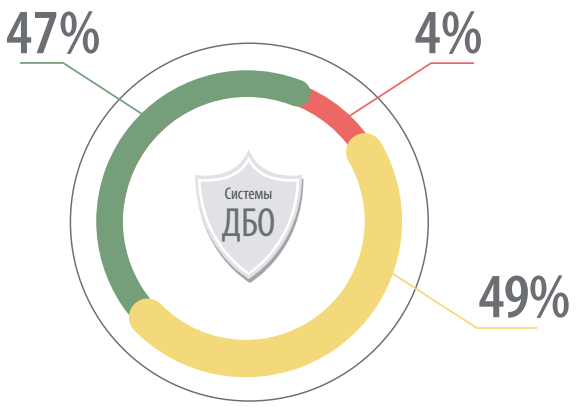
Недостатки данной категории вызваны некорректной настройкой операционных систем, СУБД, веб-сервера и компонентов веб-приложений. Треть всех обнаруженных уязвимостей систем ДБО относятся к этому типу). Все рассмотренные системы содержали хотя бы одну уязвимость, связанную с недостатками конфигурирования. При этом 18% систем содержали недостатки, которые были связаны с высокими рисками для системы ДБО.



Было обнаружено лишь две уязвимости высокой степени риска в двух из 11 систем ДБО (18%). Из них одна уязвимость высокого уровня приходятся на системы ДБО, предоставленные вендорами, и одна — на системы собственной разработки.

ДОЛЯ УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С НЕДОСТАТКАМИ КОНФИГУРАЦИИ

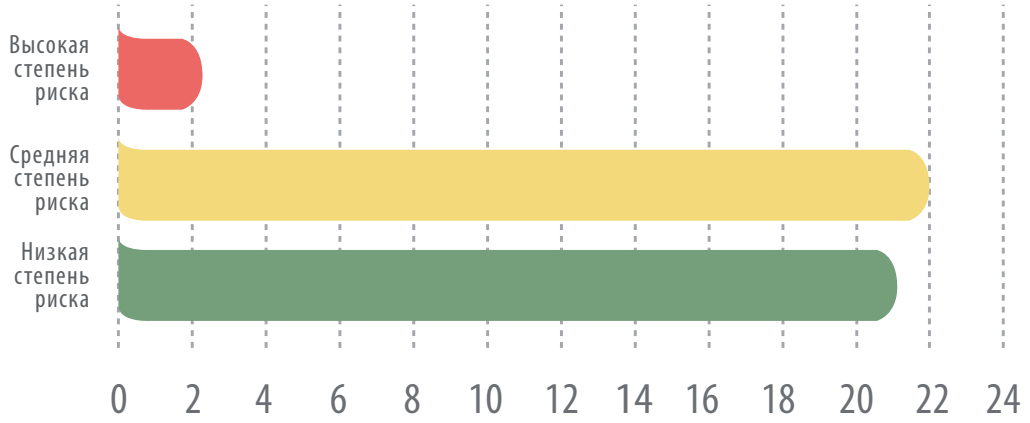
Только 4% обнаруженных уязвимостей данного типа имеют высокую критичность. Доля обнаруженных недостатков конфигурации среднего и низкого уровней риска примерно одинакова: 49% и 47% соответственно



Наиболее опасными уязвимостями данного типа являются избыточная функциональность, предсказуемое расположение файлов и каталогов, использование небезопасных протоколов. Также к распространенным недостаткам конфигурации относятся:

- незащищенная передача данных (45% систем);
- небезопасная настройка cookie-параметров (36% систем).

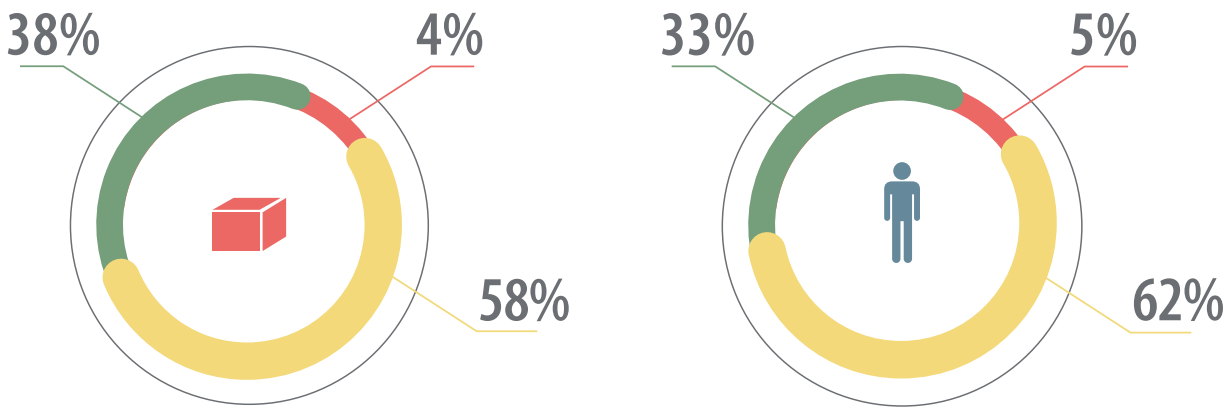
ЧИСЛО УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С НЕДОСТАТКАМИ КОНФИГУРАЦИИ



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. Отметим, что большинство рассмотренных систем, в которых использовалась незащищенная передача данных, были тестовыми, и реализация безопасного взаимодействия была запланирована на более поздние этапы внедрения.

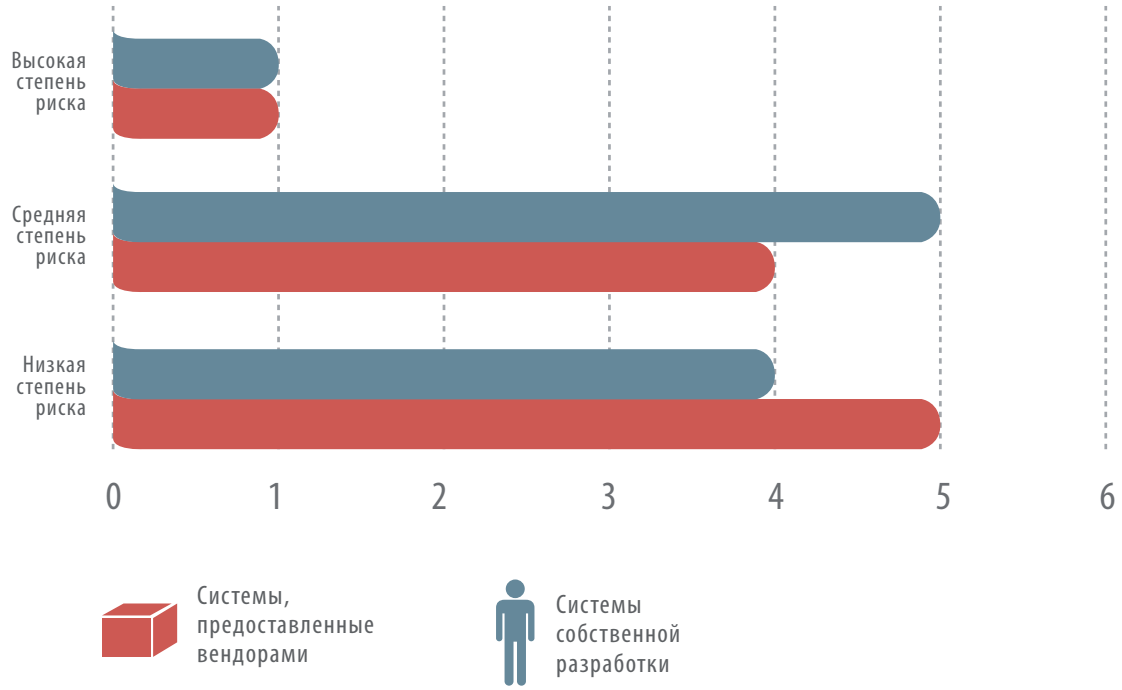
9.1. НЕДОСТАТКИ КОНФИГУРАЦИИ В СИСТЕМАХ СОБСТВЕННОЙ РАЗРАБОТКИ И В СИСТЕМАХ, ПОСТАВЛЯЕМЫХ ВЕНДОРАМИ

Для систем, предоставляемых вендорами, большая часть уязвимостей, связанных с недостатками конфигурации (58%), имеет низкий уровень критичности. В системах же собственной разработки преобладают недостатки конфигурации среднего уровня риска (62%). Доля недостатков конфигурации высокой критичности для этих двух категорий систем примерно одинакова (4% и 5% соответственно).



НЕДОСТАТКИ КОНФИГУРАЦИИ РАЗЛИЧНЫХ СИСТЕМ

На диаграмме представлено количественное соотношение обнаруженных уязвимостей различной степени риска для различных категорий систем. Из полученных результатов следует, что уровень защищенности систем собственной разработки и систем, предоставляемых вендорами, с точки зрения конфигурирования системы ДБО примерно одинаковый.



10 УСТАРЕВШИЕ ВЕРСИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

При анализе защищенности систем ДБО банки, как правило, ограничивают область проведения работ поиском уязвимостей, связанных с недостатками на уровне кода приложения, логикой функционирования системы и особенностями конфигурации. При этом владелец системы подразумевает, что в случае наличия известных уязвимостей, связанных с использованием устаревших версий системного программного обеспечения и СУБД, подобные недостатки будут оперативно устраняться в рамках обновлений.

Однако на основе информации о версиях используемого программного обеспечения, раскрываемой некоторыми уязвимыми системами, можно утверждать, что системы ДБО могут содержать множество уязвимостей уровня ОС и СУБД. Для верификации наличия данных уязвимостей необходимо проведение работ по анализу защищенности для серверных компонентов системы ДБО. В рамках подобных работ можно установить точные версии используемого программного обеспечения, наличие или отсутствие актуальных обновлений безопасности, а также оценить возможность эксплуатации уязвимостей для получения контроля над системой ДБО.

К примеру, в одной из систем ДБО собственной разработки в ходе анализа защищенности была выявлена уязвимость высокого уровня критичности, связанная с устаревшей версией библиотеки glibc операционной системы. Используя известные уязвимости данной библиотеки (http://www.opennet.ru/opennews/art.shtml?num=28338 и http://www.exploit-db.com/exploits/15024/), специалисты Positive Technologies сумели получить привилегии суперпользователя (root) на сервере.

Таким образом, системы ДБО, как и любые другие информационные системы, подвержены уязвимостям, связанным с использованием устаревших версий программного обеспечения. Несмотря на то что зачастую данные уязвимости становятся доступны злоумышленнику только после успешной эксплуатации уязвимостей уровня веб-приложения, именно уязвимые версии ОС и СУБД могут стать причиной существенного расширения привилегий, полученных злоумышленником, — вплоть до полного контроля над системой ДБО и доступа во внутреннюю сеть банка. Во избежание эксплуатации известных уязвимостей ОС, СУБД и других программных компонентов, рекомендуется периодически проводить анализ защищенности серверных компонентов системы ДБО и своевременно обновлять используемые программные продукты.

11 ДРУГИЕ НЕДОСТАТКИ

Рассмотренные в рамках проведенного исследования системы ДБО содержат также ряд других существенных недостатков. К примеру, в одной из систем были обнаружены файлы журналов, в которых хранилась чувствительная информация:

- **данные, необходимые для аутентификации** (идентификатор пользователя и хэш пароля);
- **sms-сообщение**, содержащее код подтверждения, необходимый для проведения транзакции;
- **установочный путь** (может быть использован злоумышленником при эксплуатации ряда уязвимостей);
- **пароль в открытом виде** (сохраняется в файл журнала после смены через соответствующий сценарий).

Обладая данной информацией, злоумышленник может осуществлять несанкционированный доступ к системе ДБО от лица произвольного пользователя, выполнять денежные переводы и осуществлять другие несанкционированные действия в системе.

В ряде систем ДБО недостаточно маскируются номера платежных карт (PAN). Существуют примеры, когда PAN вообще не маскируется, либо маскируется при отображении страницы, но содержится в HTML-коде. 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 3 из 11 систем ДБО.

Атаки типа «Отказ в обслуживании» (DoS) являются одной из наиболее актуальных угроз, связанных с использованием сети Интернет. В случае систем ДБО данная атака может быть направлена на нарушение доступности как серверной части системы, так и личного кабинета пользователя. Используя предсказуемость формата идентификатора учетных записей, нарушитель способен осуществить блокировку учетных записей при многократном вводе неверных данных в поле пароля. Атаки, направленные на отказ в обслуживании обслуживании могут привести к репутационным потерям для банка.

12 ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования было показано, насколько уязвимы современные системы дистанционного банковского обслуживания.

Результаты проведенного исследования лишний раз подтверждают, что перед вводом системы ДБО в эксплуатацию необходимо проводить анализ ее защищенности, в том числе для систем, предоставляемых профессиональными вендорами

Кроме того, необходимо уделить особое внимание корректной реализации механизмов защиты, особенно в части аутентификации и авторизации, а также обеспечить контроль качества кода веб-приложения. При эксплуатации системы необходимо регулярно проводить анализ защищенности, проверять корректность настроек компонентов системы ДБО и обновлять программное обеспечение до актуальных версий.

Для продуктивных систем, приобретаемых у вендоров, рекомендуется использовать межсетевой экран уровня приложения (Web Application Firewall) с целью исключения эксплуатации уязвимостей в коде приложения до выпуска вендором обновления

Обеспечение безопасности системы ДБО, как и любой информационной системы, требует комплексного подхода на всех этапах ее жизненного цикла.

Реализация процесса безопасной разработки и регулярный контроль защищенности системы ДБО позволят снизить риски несанкционированного доступа к системе и сохранить в целости денежные средства клиентов банка