



# Уязвимости корпоративных информационных систем

---

2017

POSITIVE TECHNOLOGIES

## СОДЕРЖАНИЕ

Введение.....	3
1. Резюме.....	3
2. Исходные данные.....	6
3. Статистика за 2016 год и ее сравнение с результатами 2015 года.....	7
3.1. Общие результаты тестов на проникновение.....	7
3.2. Результаты анализа защищенности сетевого периметра.....	8
3.3. Результаты анализа защищенности внутренних ресурсов.....	12
4. Оценка защищенности систем.....	15
5. Результаты оценки осведомленности сотрудников в вопросах информационной безопасности.....	16
6. Результаты оценки защищенности корпоративных беспроводных сетей.....	18
7. Интересные факты о словарных паролях.....	19
Заключение.....	20

## ВВЕДЕНИЕ

Корпоративные информационные системы (КИС) крупных компаний регулярно претерпевают изменения — обновляется конфигурация оборудования, изменяется топология сетей, появляются новые узлы и целые системы. Для большинства корпораций с распределенной инфраструктурой процесс непрерывного обеспечения комплексной защиты информационных активов становится непростой задачей из-за высокой сложности архитектуры и большого числа взаимосвязей внутри отдельных подсистем.

В настоящем исследовании представлен анализ наиболее популярных уязвимостей на основе проектов по анализу защищенности, проведенных экспертами Positive Technologies в 2016 году. В процессе таких тестирований моделируются атаки, аналогичные реальным попыткам проникновения со стороны внешних и внутренних злоумышленников, что позволяет выявить многие проблемы защиты, в том числе и такие, которые не выявляются другими способами. Данные за 2016 год приводятся в сравнении с результатами аналогичного исследования предыдущего года. Исследование позволяет оценить общий уровень защищенности тестируемых систем, выявить основные тенденции в этой области, а также предложить рекомендации для повышения уровня безопасности КИС.

При выборе систем, попавших в итоговое исследование, учитывалась информативность полученных результатов. Проекты по анализу защищенности, которые по просьбе заказчиков проводились на ограниченном количестве узлов, не были включены в исследование, так как не отражают реальное состояние защищенности корпоративной информационной системы в целом.

## 1. РЕЗЮМЕ

**Уязвимости критического уровня риска** найдены в 47% протестированных корпоративных систем.

**Преодолеть периметр** 55% систем может внешний нарушитель с минимальными знаниями и низкой квалификацией. В среднем внешнему нарушителю требуется всего два шага для преодоления периметра.

**Основные уязвимости на периметре:** словарные пароли и открытые протоколы передачи данных (найжены во всех системах), уязвимые версии ПО (91% систем) и общедоступные интерфейсы удаленного доступа, управления оборудованием и подключения к СУБД (91%). Отдельные уязвимости веб-приложений хотя и не попали в первые строчки рейтинга, но оказались наиболее опасны: в 77% систем преодолеть сетевой периметр удалось именно из-за уязвимостей веб-приложений.

**Получить полный контроль** над корпоративной инфраструктурой со стороны внешнего нарушителя возможно в 55% систем, со стороны внутреннего нарушителя — во всех системах. В 2015 году эти показатели составляли лишь 28% и 82% соответственно.

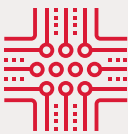
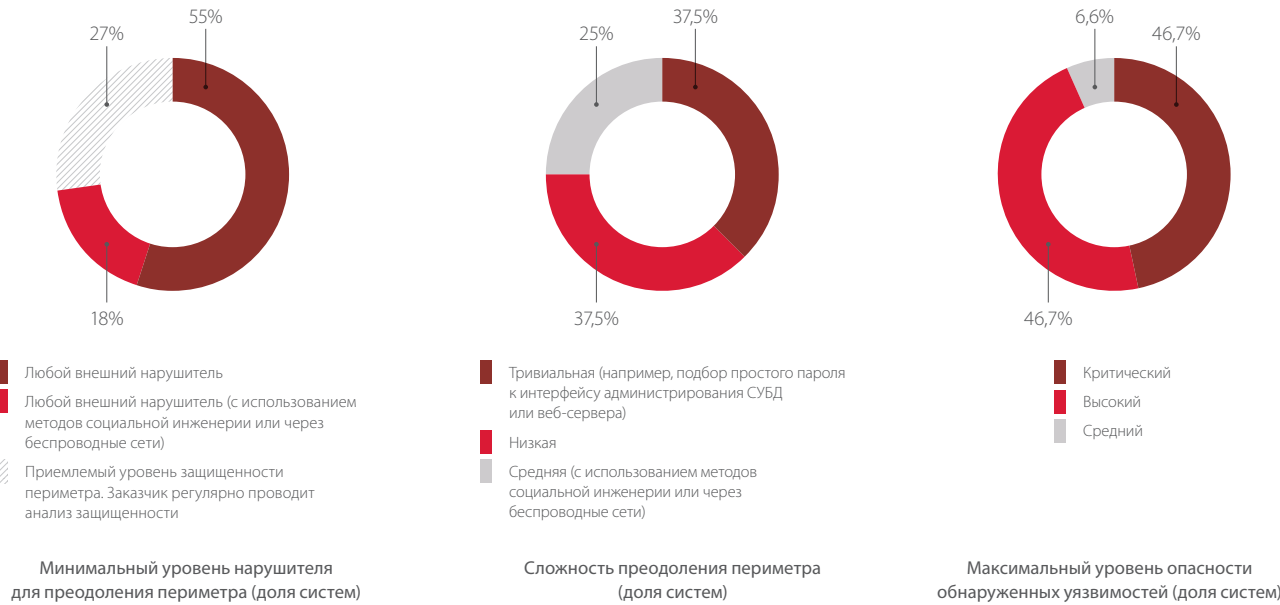
**Наиболее распространенные уязвимости внутренней сети** — недостатки защиты протоколов сетевого и канального уровней, приводящие к перенаправлению трафика и перехвату информации о конфигурации сети (найжены в 100% систем).

**Уровень осведомленности сотрудников** в вопросах ИБ оказался крайне низким в половине систем (в 2015 году — только в 25%).

**Уровень защищенности беспроводных сетей** в 75% случаев оценивается как крайне низкий. В каждой второй системе из беспроводной сети возможен доступ к ЛВС.



В среднем внешнему нарушителю требуется **всего 2 шага** для преодоления периметра

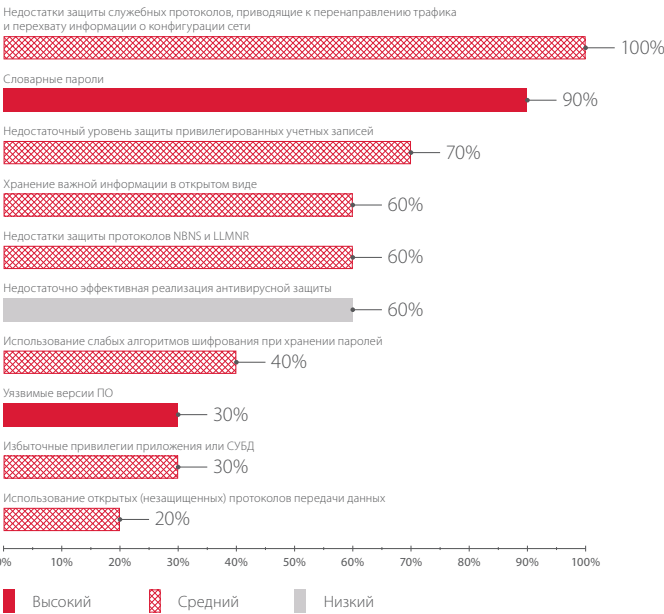


В 2016 году для оценки уязвимостей применялась система классификации CVSS версии 3.0 со стандартизированной качественной шкалой оценки опасности. После анализа выявленных уязвимостей было установлено, что **почти половина** протестированных корпоративных систем **содержит уязвимости критического уровня опасности.**

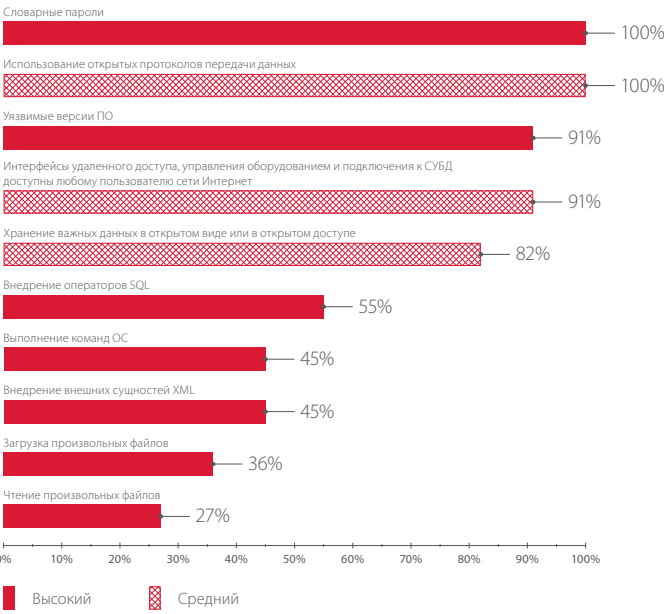
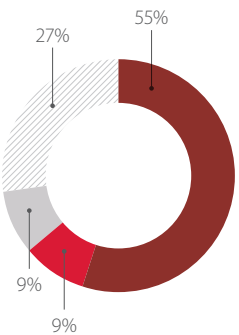


7 из 10 распространенных уязвимостей на сетевом периметре — уязвимости **высокого уровня риска**

### Локальная вычислительная сеть предприятия

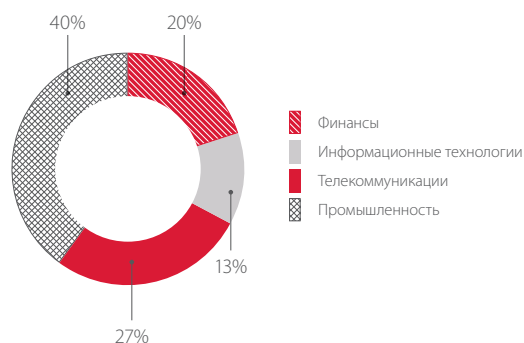


В **100%** работ от лица внутреннего нарушителя удалось получить **полный контроль** над инфраструктурой корпоративной информационной системы и критически важными ресурсами



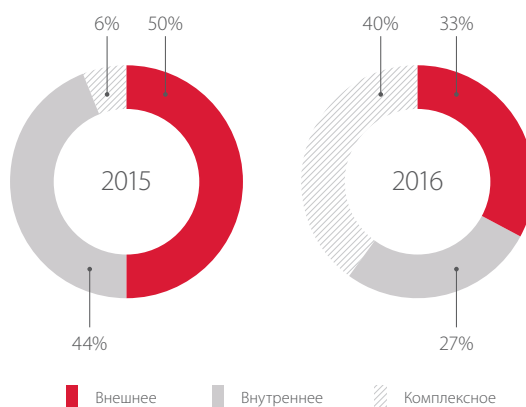
## 2. ИСХОДНЫЕ ДАННЫЕ

Для подведения итогов 2016 года были отобраны результаты анализа защищенности 15 корпоративных систем, принадлежащих российским и зарубежным компаниям из различных сфер экономики. Работы проводились для крупных промышленных компаний, в том числе с государственным участием, банков и финансовых организаций, поставщиков телекоммуникационных услуг и информационных технологий.



Распределение исследованных систем по отраслям экономики (доля систем)

В состав оказанных услуг для рассматриваемых систем входили различные виды тестирования на проникновение — внешнее, внутреннее и комплексное тестирование (последнее включает в себя как внешнее, так и внутреннее). В 2016 году стали более востребованными комплексные услуги по тестированию корпоративных систем.



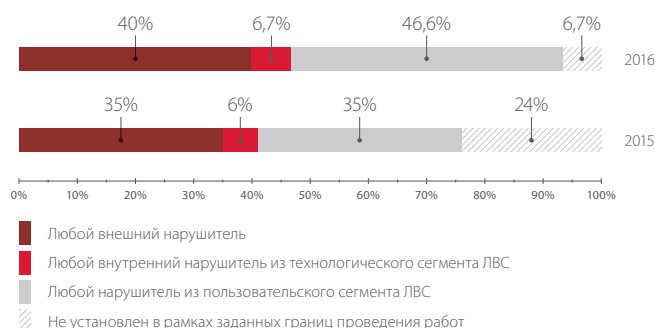
Виды тестирования на проникновение (доля систем)

Также для некоторых компаний помимо различных услуг по анализу защищенности корпоративных систем проводились отдельные работы по оценке осведомленности персонала в вопросах информационной безопасности и тестированию защищенности корпоративных беспроводных сетей.

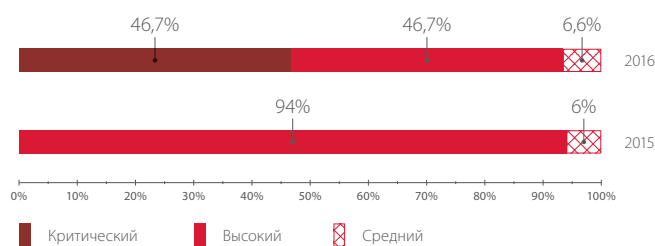


### 3. СТАТИСТИКА ЗА 2016 ГОД И ЕЕ СРАВНЕНИЕ С РЕЗУЛЬТАТАМИ 2015 ГОДА

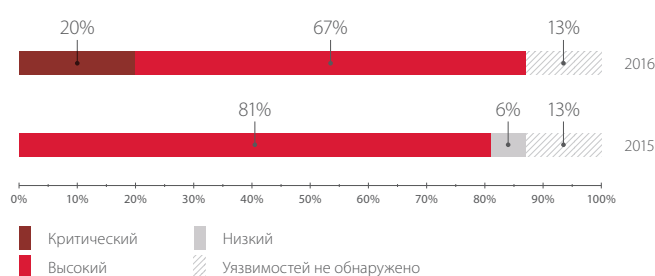
#### 3.1. Общие результаты тестов на проникновение



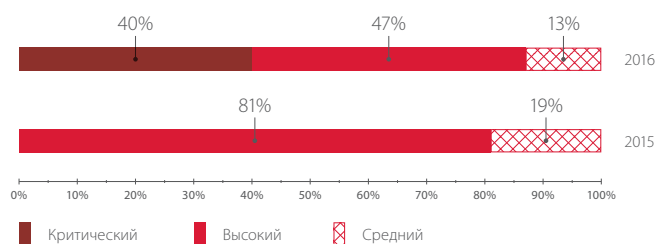
Минимальный уровень доступа, необходимый нарушителю для получения полного контроля над отдельными критически важными ресурсами (доля систем)



Доля систем по максимальному уровню опасности обнаруженных уязвимостей



Максимальный уровень риска уязвимостей, связанных с отсутствием обновлений безопасности (доля систем)



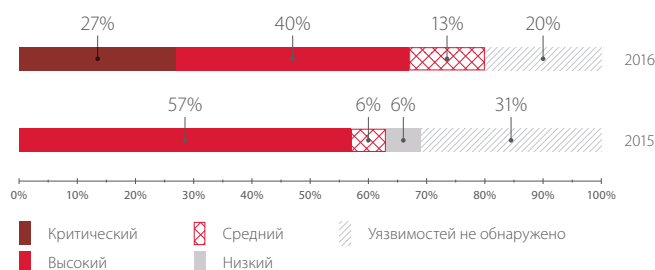
Максимальный уровень риска уязвимостей, связанных с недостатками конфигурации (доля систем)

Важно отметить, что уязвимости, связанные с ошибками в коде веб-приложений и отсутствием обновлений безопасности, могут присутствовать во всех исследуемых корпоративных информационных системах, но поскольку тестирование на проникновение проводится методом черного ящика, эти уязвимости могли остаться невыявленными.



## Интересный факт

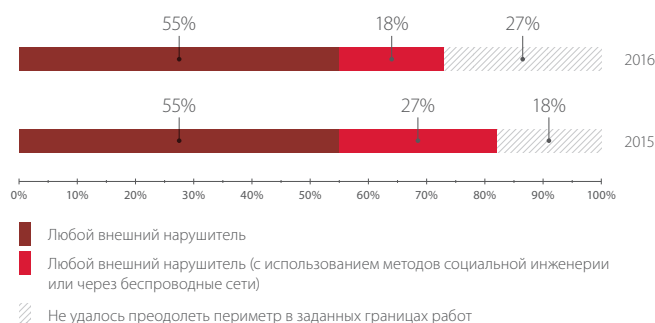
Средний возраст наиболее устаревших неустановленных обновлений по системам, где такие уязвимости были обнаружены, составляет 108 месяцев (9 лет). Самая старая из обнаруженных уязвимостей (CVE-1999-0024) **опубликована более 17 лет назад** и связана с тем, что DNS-сервер поддерживает рекурсию запросов. В результате эксплуатации данной уязвимости злоумышленник может проводить атаки на отказ в обслуживании.



Максимальный уровень риска уязвимостей, связанных с ошибками в коде веб-приложений (доля систем)

## 3.2. Результаты анализа защищенности сетевого периметра

В 2016 году сохраняется тенденция к повышению общего уровня защищенности сетевого периметра корпоративных информационных систем. В 27% случаев специалистам Positive Technologies не удалось преодолеть сетевой периметр и получить доступ к ресурсам внутренней локальной вычислительной сети. Данные результаты связаны с тем, что некоторые заказчики регулярно проводят тестирование на проникновение и устраняют выявленные уязвимости. Однако важно помнить, что конфигурация сетевой инфраструктуры регулярно изменяется, поэтому тестирование на проникновение необходимо проводить на регулярной основе. Кроме того, нужно следить за тем, какие службы доступны для подключения из сети Интернет. Не исключено, что завтра по ошибке или из-за недостаточной компетентности в вопросах информационной безопасности кто-то из администраторов откроет на периметре «опасный» сетевой порт, и корпоративная система окажется уязвимой.



Минимальный уровень нарушителя, достаточный для преодоления периметра (доля систем)

Сложность преодоления периметра по сравнению с 2015 годом снизилась. Практически в 55% случаев (против 46% в 2015 году) внешний нарушитель, обладая минимальными знаниями и низкой квалификацией, способен преодолеть периметр и получить доступ к ресурсам локальной вычислительной сети. При этом в 2016 году, как и в предыдущие годы, для преодоления сетевого периметра необходима эксплуатация в среднем двух различных уязвимостей.



Сложность преодоления периметра (доля систем)

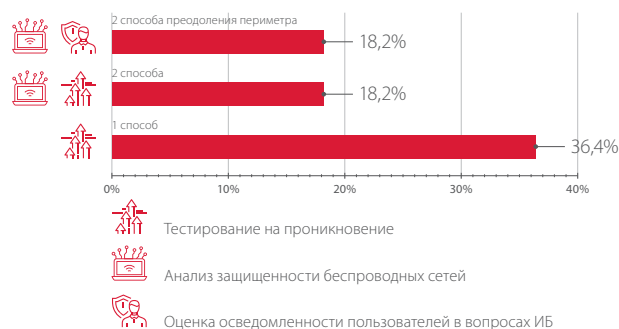
### Примеры преодоления периметра и получения доступа к ресурсам локальной вычислительной сети

<b>Тривиальная сложность преодоления периметра</b>	На периметре сети доступен для подключения интерфейс отладки JDWP. Любой внешний нарушитель может использовать общедоступный эксплойт ( <a href="https://github.com/IOActive/jdwp-shellifier">github.com/IOActive/jdwp-shellifier</a> ) и выполнить произвольные команды на сервере. Используя эту уязвимость и избыточные привилегии службы, удалось получить полный контроль над сервером и доступ к ЛВС (на узле был доступен интерфейс внутренней сети)
<b>Низкая сложность преодоления периметра</b>	На тестируемом узле выявлено веб-приложение для управления обучением сотрудников заказчика. Путем регистрации новой учетной записи без подтверждения личности удалось получить доступ к функциональности веб-приложения и загрузить веб-интерпретатор командной строки (веб-шелл) на сервер, что сделало возможным выполнение произвольных команд ОС на сервере с привилегиями веб-приложения. Таким образом удалось получить доступ к ЛВС, поскольку на узле был доступен интерфейс внутренней сети
<b>Средняя сложность преодоления периметра</b>	<p><b>Пример 1.</b> Используя известную уязвимость ПО Adminer, удалось выполнить чтение локальных файлов на узле и обнаружить конфигурационный файл с учетной записью для доступа к БД. В самой БД была обнаружена таблица с более чем 400 учетными записями пользователей и хеш-суммами их паролей. С одной из таких учетных записей (пароль подобран по хеш-сумме) получен доступ к веб-приложению на атакованном ресурсе. Функциональность веб-приложения позволила загрузить веб-интерпретатор командной строки на сервер и выполнять команды ОС. В результате атаки был получен доступ к ЛВС (на узле доступен интерфейс внутренней сети).</p> <p><b>Пример 2.</b> В ходе работ по оценке осведомленности сотрудников в вопросах информационной безопасности была произведена массовая рассылка электронных писем от внутреннего лица со ссылкой на веб-ресурс, содержащий фишинговую форму для ввода учетных данных. Некоторые сотрудники ввели учетные данные в ложную форму аутентификации. Полученные учетные данные могут быть использованы для несанкционированного доступа к ресурсам тестируемой системы.</p> <p>Для использования фишинговых сценариев атак как минимум необходимо зарегистрировать собственный домен и разработать ложную форму аутентификации. Более того, важно сделать фишинговый ресурс максимально приближенным по дизайну страницы к тому ресурсу, которым привык пользоваться сотрудник. Для этого необходимо проводить дополнительные разведывательные действия, что существенно повышает сложность реализации атаки</p>

В среднем в каждой системе при проведении работ по тестированию на проникновение выявлено два вектора атак для получения несанкционированного доступа к ресурсам локальной вычислительной сети. Максимальное количество выявленных в одной системе векторов атак — 5.

Также важно отметить, что в нескольких проектах преодолеть сетевой периметр и получить доступ к ресурсам внутренней локальной вычислительной сети удалось несколькими разными способами, как в рамках обычного тестирования на проникновение, так и с использованием методов социальной инженерии и через беспроводные сети.





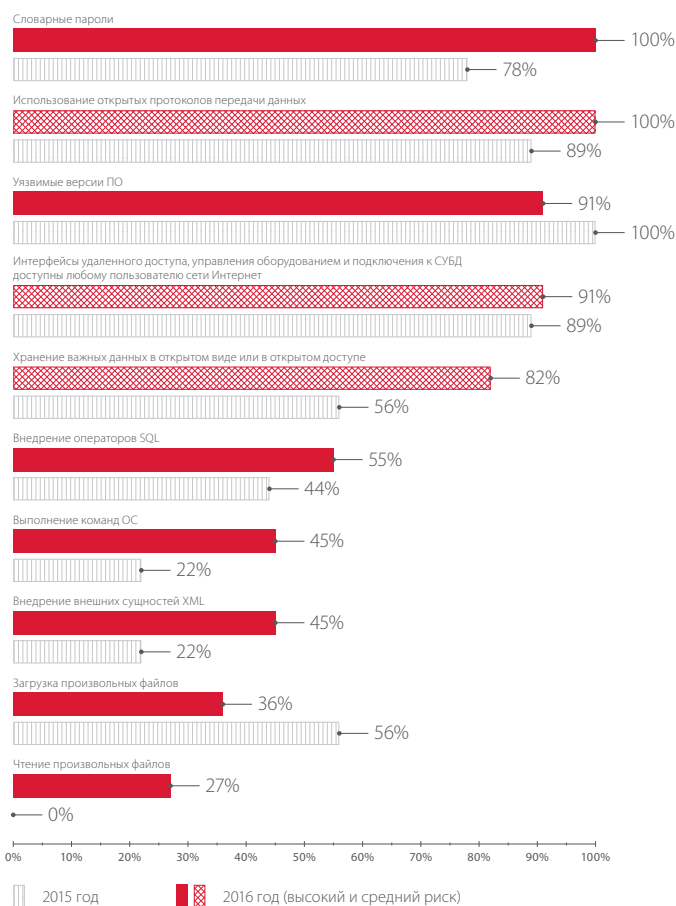
Доля работ, в рамках которых удалось преодолеть сетевой периметр

В 77% работ сетевой периметр удалось преодолеть из-за уязвимостей веб-приложений, а в 23% — из-за уязвимостей, связанных с использованием словарных паролей.



### Интересный факт

На внешних ресурсах (серверы веб-приложений) сразу нескольких заказчиков были обнаружены несанкционированно установленные веб-интерпретаторы командной строки, которые свидетельствуют о ранее проведенных успешных атаках. Более того, нарушители могли успешно проводить атаки на ресурсы локальных вычислительных сетей в течении нескольких месяцев, так как данные веб-интерпретаторы оставались не выявленными до проведения работ по анализу защищенности.

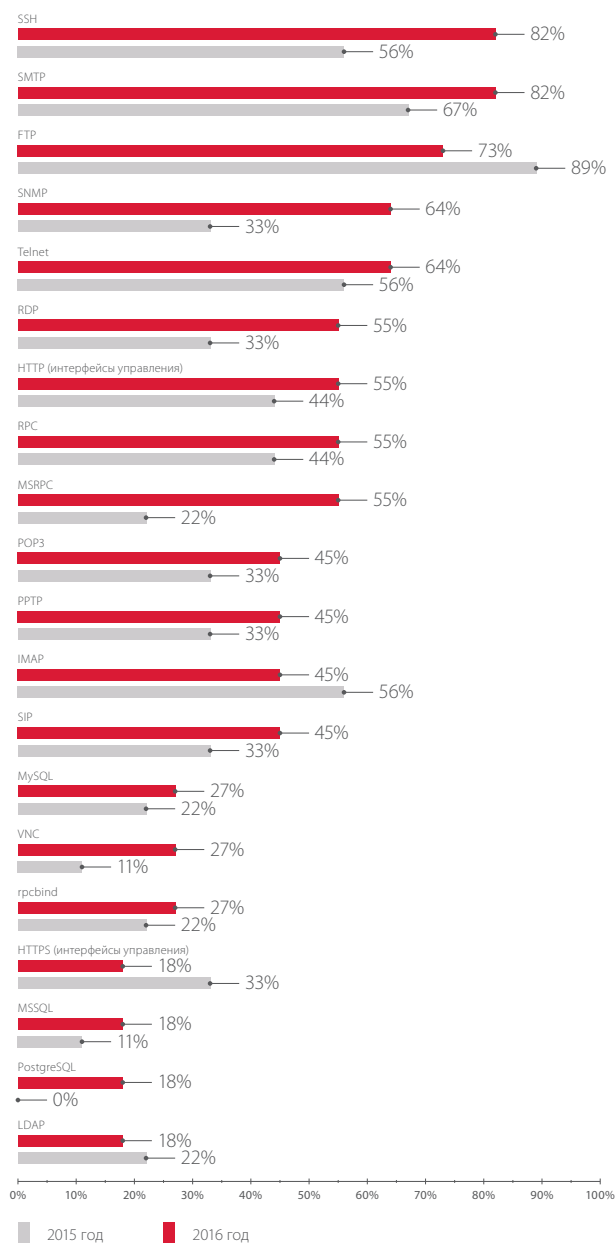


Наиболее распространенные уязвимости на сетевом периметре (доля систем)



## Интересный факт

При тестировании одной корпоративной информационной системы в 2016 году не только были выявлены веб-интерпретаторы командной строки на внешних ресурсах, но и обнаружено сразу 5 векторов атак, позволяющих внешнему нарушителю низкой квалификации преодолеть сетевой периметр и получить доступ к ресурсам локальной вычислительной сети.



Протоколы на сетевом периметре (доля систем)

Первая пятерка самых распространенных уязвимостей на сетевом периметре за год изменилась незначительно. По результатам внешних тестов на проникновение во всех системах выявлено использование словарных паролей<sup>1</sup> и открытых протоколов передачи данных, почти в каждой системе найдены компоненты с уязвимыми версиями программного обеспечения. В ходе работ по сканированию узлов сетевого периметра в 91% случаев были выявлены

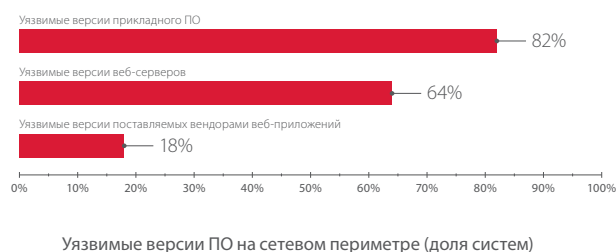
<sup>1</sup> С детальной статистикой по уязвимости, связанной с использованием словарных паролей, в том числе на сетевом периметре, можно ознакомиться в разделе 7 настоящего документа.

интерфейсы удаленного доступа, управления оборудованием и подключения к СУБД, доступные любому пользователю сети Интернет. Также значительно увеличилась доля систем, в которых обнаружена уязвимость, связанная с хранением важных данных в открытом виде или открытом доступе. Вторая пятерка уязвимостей связана с различными ошибками и недостатками в коде веб-приложений. Можно утверждать, что общий уровень защищенности веб-приложений по-прежнему остается низким, что подтверждается результатами соответствующего исследования «Статистика уязвимостей веб-приложений (2016)».<sup>2</sup>

Недостатки корпоративных систем, связанные с использованием открытых протоколов передачи данных, занимают вторую строчку рейтинга. Для доступа к интерфейсам управления широко применяются протоколы FTP, Telnet и HTTP-интерфейсы управления. Используя отсутствие защиты данных, передаваемых по этим протоколам, злоумышленник может перехватить чувствительную информацию, в том числе учетные данные привилегированных пользователей, и получить несанкционированный доступ к ресурсам.

Проблема доступности из внешних сетей интерфейсов удаленного доступа, управления оборудованием и подключения к СУБД в 2016 году также актуальна и входит в пятерку наиболее распространенных недостатков.

По сравнению с 2015 годом незначительно (на 9%) улучшилась ситуация с использованием уязвимых версий программного обеспечения на узлах сетевого периметра. При этом увеличилось количество систем, в которых используются уязвимые версии прикладного ПО.



Из интересных тенденций 2016 года можно отметить сокращение с 33% (2015 год) до 18% количества уязвимостей, связанных с использованием избыточных привилегий приложений или СУБД. Во многом это связано с тем, что в новых версиях MS SQL Server по умолчанию не устанавливаются максимальные привилегии в ОС. Ранее нарушитель, подобранный учетную запись СУБД, моментально получал полный контроль над сервером — при условии, если администратор вручную не ограничивал привилегии СУБД. В актуальных версиях MS SQL Server этот недостаток был учтен, привилегии СУБД по умолчанию ограничены. Однако даже эти ограничения часто не обеспечивают должного уровня защиты. С примерами повышения привилегий СУБД можно ознакомиться в исследовании «Тестирование на проникновение корпоративных информационных систем: сценарии атак».<sup>3</sup>

### 3.3. Результаты анализа защищенности внутренних ресурсов

После получения доступа к внутренней сети внешний злоумышленник имеет возможности для развития атаки и получения полного контроля над всей IT-инфраструктурой или отдельными критически важными системами. Более чем в половине работ от лица внешнего нарушителя был получен полный контроль над критически важными ресурсами (системой Active Directory, СУБД, ERP-системой и другими). При этом в 55% случаев удалось получить полный контроль над корпоративной инфраструктурой. Данный показатель увеличился почти в два раза по сравнению с результатами 2015 года.

При тестировании от лица внутреннего злоумышленника (например, рядового сотрудника, находящегося в пользовательском сегменте сети) в 2016 году полный контроль над инфраструктурой был получен в 100% систем — против 82% в 2015 году.

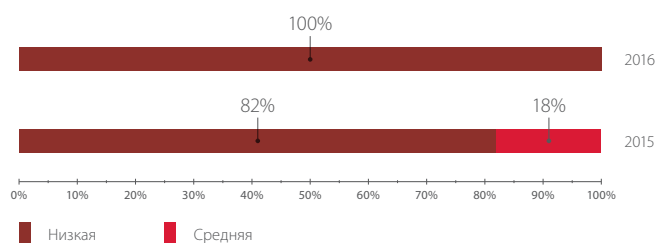
Сложность атак для получения доступа к критически важным ресурсам со стороны внутреннего нарушителя существенно снизилась.

<sup>2</sup> [www.ptsecurity.com/ru-ru/research/analytics/](http://www.ptsecurity.com/ru-ru/research/analytics/)

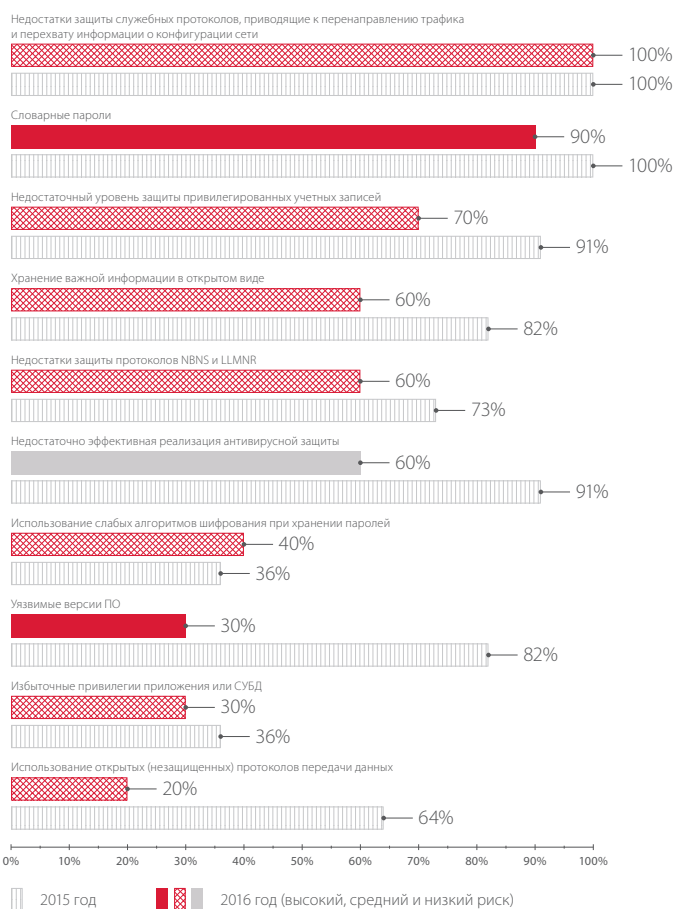
<sup>3</sup> [www.ptsecurity.com/ru-ru/research/analytics/](http://www.ptsecurity.com/ru-ru/research/analytics/)



Уровень привилегий, полученных от лица внешнего нарушителя (доля систем)



Сложность получения доступа к критически важным ресурсам  
со стороны внутреннего нарушителя (доля систем)



Наиболее распространенные уязвимости внутренней сети (доля систем)

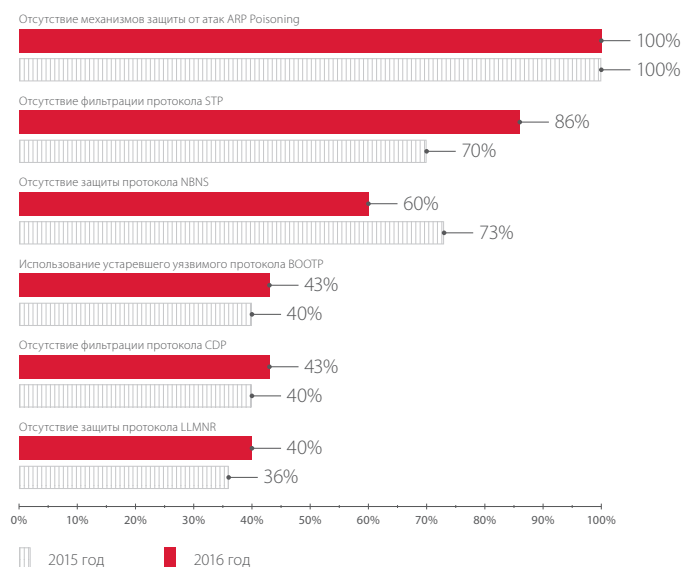
В большинстве работ для получения максимальных привилегий в критически важных системах от лица внутреннего нарушителя достаточно подобрать учетную запись с привилегиями локального администратора на одной из рабочих станций или на сервере ЛВС, запустить

специализированное ПО и получить в открытом виде учетные записи локальных администраторов других узлов. Данный вектор атаки можно развивать вплоть до получения учетных данных администраторов доменов.

В некоторых работах для получения доступа к критически важным системам со стороны внутреннего нарушителя требовалось всего два шага. На первом шаге осуществлялось повышение привилегий до максимальных в ОС с использованием известной уязвимости ОС (CVE-2015-1701) и общедоступного эксплойта. Затем проводился анализ доступных журналов на исследуемом сервере и подбор учетных данных для доступа к критически важной системе.

Первое место в рейтинге наиболее распространенных уязвимостей теперь принадлежит недостаткам защиты протоколов сетевого и канального уровней, приводящим к перенаправлению трафика и перехвату информации о конфигурации сети. Каждая исследуемая система содержала различные недостатки защиты служебных протоколов, таких как ARP, STP, BOOTP, CDP.

В каждом из проектов, где проводился анализ сетевого трафика ЛВС, было выявлено отсутствие механизмов защиты от атак ARP Cache Poisoning. Данный недостаток может быть использован для прослушивания трафика в сети и проведения атак типа «человек посередине». В ходе успешной реализации атаки нарушитель может перехватывать конфиденциальную информацию, изменять данные в процессе передачи и блокировать сетевое взаимодействие.



Недостатки защиты служебных протоколов (доля систем)

Уязвимость, связанная с использованием словарных паролей, переместилась на вторую строчку рейтинга (–10% по сравнению с 2015 годом). Причем во всех тестируемых корпоративных системах, в которых была выявлена данная уязвимость, словарные пароли использовались в том числе и для доступа к учетным записям привилегированных пользователей.

Из положительных тенденций 2016 года можно отметить снижение на 21% количества систем, в которых встречается уязвимость, вызванная с недостаточным уровнем защиты привилегированных учетных записей. Это связано с тем, в процессе работ по анализу защищенности стали чаще встречаться системы, в которых организована двухфакторная аутентификация для привилегированных учетных записей домена, а также для учетных записей ключевых администраторов. Однако специалистам Positive Technologies во многих работах удалось обойти этот защитный механизм. Например, во время одного тестирования на проникновение внутренней сети проводилась эксплуатация уязвимостей механизмов двухфакторной аутентификации в ОС Windows при использовании смарт-карт.



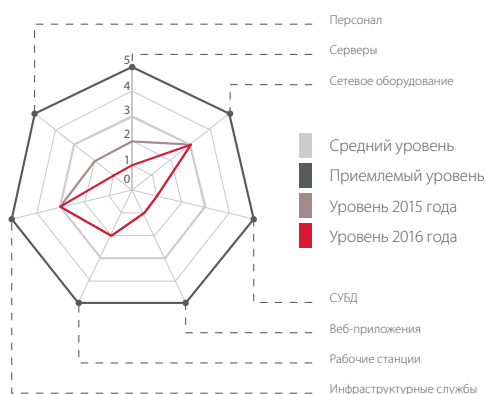
### Интересный факт

Принцип двухфакторной аутентификации подразумевает, что пользователь должен не только знать что-то (например, PIN-код или пароль), но и обладать чем-то (в рассматриваемом случае — смарт-картой с установленным сертификатом). Когда в конфигурации учетной записи домена устанавливается атрибут, отвечающий за аутентификацию по смарт-карте, этой учетной записи присваивается некоторый NT-хеш. Его значение вычисляется случайным образом и неизменно при всех последующих подключениях к ресурсам домена. Уязвимость заключается в том, что злоумышленник может получить этот NT-хеш, присваиваемый пользователю контроллером домена, и использовать его при аутентификации методом pass the hash. Таким образом, злоумышленнику уже не нужно обладать смарт-картой и знать ее PIN-код, и он получает возможность атаковать ресурсы домена с привилегиями скомпрометированной учетной записи неограниченный период времени.

## 4. ОЦЕНКА ЗАЩИЩЕННОСТИ СИСТЕМ

Векторы атак классифицируются в зависимости от компонентов системы, эксплуатация уязвимостей которых позволяет получить несанкционированный доступ к ресурсам.

Механизмы защиты классифицируются в зависимости от выявленных недостатков в реализации системы защиты, которые были использованы в ходе тестирования на проникновение.



Средний уровень защищенности систем: векторы атак



Средний уровень защищенности систем: эффективность механизмов защиты

### Примечание

Оценка 0 на диаграммах соответствует крайне низкому уровню, оценка 5 — приемлемому уровню.



Общий уровень защищенности систем по сравнению с 2015 годом снизился за счет изменения компетенций персонала в вопросах информационной безопасности и уровня защищенности серверного оборудования со значения «ниже среднего» на «низкий». Уровень защищенности СУБД и веб-приложений по-прежнему остается низким. Эффективность механизмов защиты также снизилась, причем сразу по четырем параметрам. При этом повышение эффективности механизмов защиты зафиксировано только по одному параметру «управление уязвимостями и обновлениями». Максимальные уровни защищенности отдельных компонентов и эффективности механизмов защиты не превышают среднего.

## 5. РЕЗУЛЬТАТЫ ОЦЕНКИ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как и в прошлые годы, кроме работ по тестированию на проникновение корпоративных информационных систем в 2016 году для ряда компаний проводились проверки осведомленности сотрудников в вопросах информационной безопасности. Проверки представляли собой серии согласованных с заказчиком атак, эмулирующих реальную деятельность злоумышленников, и отслеживание реакции пользователей на них. Тестирование проводилось по сценариям, адаптированным под конкретного заказчика услуг, методом рассылки по электронной почте сообщений, содержащих вложения в виде файла либо ссылку на внешний источник. Как правило, рассылка писем по электронной почте осуществлялась якобы от лица сотрудника организации, но применялись также сценарии, при которых письма отправлялись от какого-либо стороннего лица или организации. Также в некоторых работах проводилось телефонное взаимодействие с рядовыми сотрудниками компаний, вступившими в переписку, в подписи которых были указаны внутренние телефонные номера.

### Пример сценария тестирования осведомленности пользователей



**Шаг 1.**  
**Рассылка сообщений  
по электронной почте**



**Шаг 2.**  
**Сбор статистических  
данных**



**Шаг 3.**  
**Телефонное  
взаимодействие\***



**Шаг 4.**  
**Подведение итогов**

#### Виды эмулированных атак:

- + атаки типа «фишинг»;
- + целевое заражение системы троянской программой;
- + использование уязвимостей ПО

#### Подсчет:

- + % перехода по ссылке;
- + % запуска приложенных файлов;
- + % ввода учетных данных;
- + % пользователей, вступивших в диалог с нарушителем

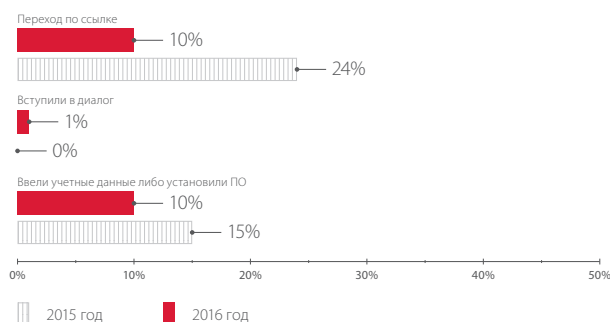
#### В результате:

- + получение чувствительной информации, в том числе учетных записей пользователей;
- + возможность планирования дальнейших атак на систему

#### Что в итоге?

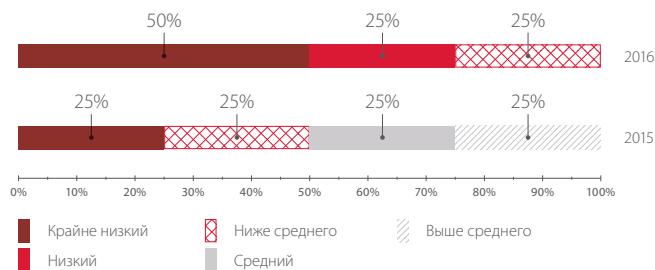
- + общая оценка осведомленности пользователей;
- + рекомендации по повышению уровня осведомленности пользователей

\* При дополнительном согласовании работ



Усредненные данные по результатам тестирования осведомленности сотрудников

Важно отметить, что в среднем в рамках всех проектов зафиксированное количество контролируемых событий оказалось ниже, чем в предыдущем году, но при этом средний уровень осведомленности пользователей в 2016 году ниже, чем в 2015 году. Это объясняется тем, что в 2015 году большинство контролируемых событий зафиксировано в одном проекте и значительно превосходит количественные значения, полученные в 2016 году.



Уровень осведомленности сотрудников в вопросах ИБ (доля систем)



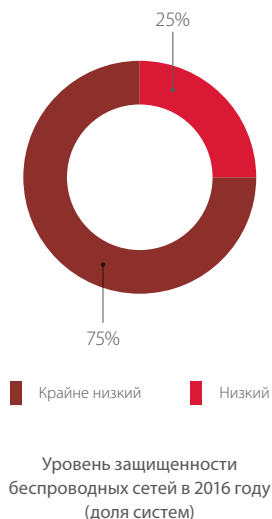
### Интересный факт

В 2016 году по результатам массовой рассылки сообщений по электронной почте некоторые сотрудники вступили в переписку со специалистами Positive Technologies, приняв их за администраторов корпоративных информационных систем. В ходе дальнейших работ был выбран один рядовой сотрудник компании, в подписи которого указан внутренний телефонный номер. Из телефонного разговора, длившегося около 4 минут, специалистами Positive Technologies были получены сведения об используемом общесистемном и прикладном программном обеспечении, а также данные доменной учетной записи сотрудника. Такая информация может быть использована злоумышленником для дальнейшей атаки на внутреннюю сеть с привилегиями пользователя системы.



## 6. РЕЗУЛЬТАТЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ БЕСПРОВОДНЫХ СЕТЕЙ

Общий уровень защищенности беспроводных сетей по сравнению с 2015 годом значительно снизился и оценивается как **«крайне низкий»**



### Во всех тестируемых системах

точка доступа не изолирует пользователей, прошедших аутентификацию, между собой. Злоумышленник, обладающий доступом в гостевую сеть, может атаковать других пользователей сети.

### В 3 из 4 систем

выявлены следующие уязвимости и недостатки:

- 1) уязвимые протоколы аутентификации (MS-CHAPv2, EAP);
- 2) словарные ключи беспроводной сети;
- 3) отсутствие механизмов защиты беспроводной сети;
- 4) несанкционированные беспроводные точки доступа;
- 5) подключение к корпоративным точкам доступа из-за границ контролируемой зоны

### В каждой второй системе

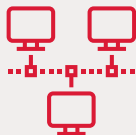
выявлены следующие уязвимости и недостатки:

- 1) недостаточно эффективные механизмы аутентификации;
- 2) из беспроводной сети возможен доступ к ЛВС;
- 3) одинаковые учетные записи для доступа к различным беспроводным сетям;
- 4) отсутствие проверки сертификатов сети;
- 5) слабая парольная политика

### Для отдельных систем

выявлены следующие уязвимости и недостатки:

- 1) отсутствие пароля для доступа к интерфейсу администрирования сетевого оборудования;
- 2) использование механизма WPS;
- 3) использование внутреннего DNS-сервера в гостевой сети



В каждой второй системе из беспроводной сети возможен доступ к ЛВС. Внешний нарушитель, используя различные уязвимости\*, может осуществлять атаки на пользователей корпоративной беспроводной сети и затем получить доступ к критически важным ресурсам ЛВС, находясь при этом за пределами контролируемой зоны.

\* Например, отсутствие проверки сертификатов сети, использование уязвимого протокола EAP или автоматическое переключение корпоративных пользователей на незащищенную сеть.



## 7. ИНТЕРЕСНЫЕ ФАКТЫ О СЛОВАРНЫХ ПАРОЛЯХ

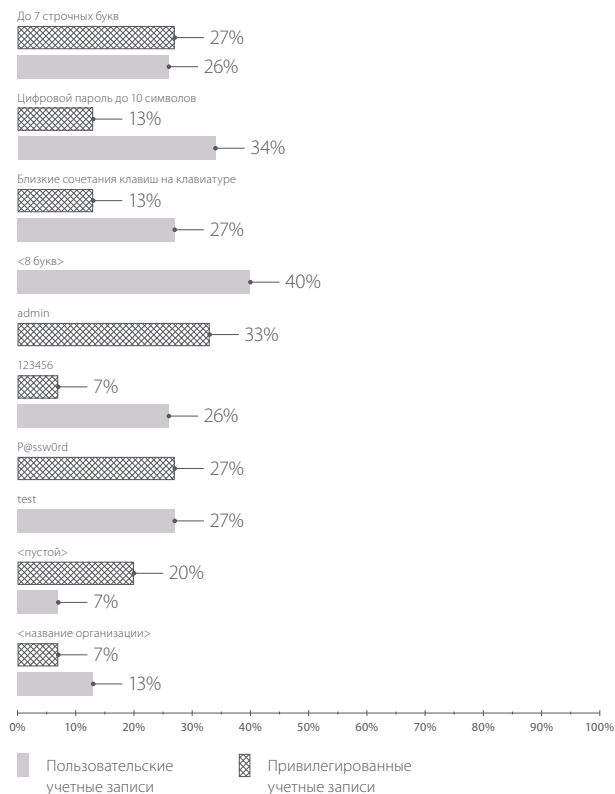
Использование словарных паролей — одна из главных проблем безопасности организаций. Данная уязвимость занимает **первое место** в рейтинге наиболее распространенных уязвимостей, выявленных на сетевом периметре, и **второе место** — во внутренних сетях.



Словарные пароли на сетевом периметре (доля систем)



Словарные пароли во внутренней сети (доля систем)



В 33% корпоративных систем можно найти привилегированную учетную запись с паролем «admin». Этот пароль уже не первый год занимает первую строчку рейтинга самых распространенных паролей администраторов. Второе и третье место поделили «P@ssw0rd» и словарные пароли до 7 строчных букв.

Самые распространенные пароли 2016 года (доля систем)

## ЗАКЛЮЧЕНИЕ

Результаты исследования показали, что современные корпоративные информационные системы стали более уязвимы к атакам со стороны внешних и внутренних злоумышленников, а реализация таких атак не требует серьезной квалификации. По сравнению с прошлым годом значительно снизились уровень защищенности беспроводных сетей и уровень осведомленности пользователей в вопросах информационной безопасности.

Необходимо также отметить, что векторы атак на корпоративные инфраструктуры по-прежнему основываются на эксплуатации распространенных уязвимостей и недостатков, для устранения которых, как правило, достаточно применить базовые принципы обеспечения информационной безопасности:

- 1) использовать строгую парольную политику;
- 2) защищать привилегированные учетные записи;
- 3) не хранить чувствительную информацию в открытом виде или в открытом доступе;
- 4) ограничить число доступных для подключения на сетевом периметре интерфейсов сетевых служб;
- 5) защищать либо отключать не используемые в локальной вычислительной сети протоколы канального или сетевого уровня, разделять сеть на сегменты;
- 6) минимизировать привилегии пользователей и служб;
- 7) регулярно обновлять ПО и устанавливать обновления безопасности ОС;
- 8) для своевременного выявления атак использовать SIEM-системы;
- 9) для защиты веб-приложений использовать web application firewalls;
- 10) проводить регулярные тренинги, направленные на повышение осведомленности пользователей в вопросах информационной безопасности (при этом важно проводить и оценку эффективности таких тренингов);
- 11) для защиты от распространения вредоносного ПО с применением социальной инженерии использовать специализированные антивирусные решения;
- 12) регулярно проводить тестирование на проникновение для своевременного выявления новых векторов атак и проверки принятых мер защиты на практике.

При этом важно обеспечить все эти меры в комплексе, только тогда защита будет эффективной, а затраты на различные дорогостоящие решения окажутся оправданы.

## О компании

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