# БИОГРАФИЯ СЕТЕВОГО ПЕРИМЕТРА В КАРТИНКАХ

**Владимир Лапшин**

Решая задачи, связанные с обеспечением информационной безопасности, принято разделять угрозы на внешние и внутренние. Внешние угрозы, как правило, ассоциируются с хакерскими атаками на сетевой периметр. Именно эта активность «темной стороны» часто становится предметом рассмотрения кино и художественной литературе. При этом действия хакера, проникающего в сеть, расположенную на другом континенте, обросли мифами, и понять — где реальность, а где вымысел — бывает очень сложно.

Многие компании сталкиваются со взломом внешнего периметра. Некоторые пытаются оценить стойкость своих границ самостоятельно, другие обращаются к специализированным организациям. Часто стойкость «оценивают» и злоумышленники, и тогда компании приходится выяснять, кто и как осуществил несанкционированное проникновение во внутреннюю сеть. Специалисты нашей компании часто оказывают помощь организациям как в оценке защищенности их сетевого периметра, так и в расследовании инцидентов информационной безопасности, а поэтому мы можем с уверенностью сказать, что задача обеспечения защиты сетевого периметра на сегодняшний день более чем актуальна.

СМИ ведут свою статистику в этой области, и она, увы, также не вызывает оптимизма. Взламывают не только рядовые компании, имеющие скромные возможности в части использования новых технологий и построения полномасштабной системы защиты, но и компании, располагающие передовыми технологиями, с высоким уровнем зрелости процессов ИБ.

В основу настоящей статьи положены результаты исследования, проведенного в отношении компаний с высоким уровнем зрелости процессов ИБ, то есть только таких компаний, где налажены процессы:

+ инвентаризации активов,
+ оценки важности активов и угроз,
+ управления уязвимостями и обновлениями ПО.

Под инвентаризацией активов понимается наличие знаний о системах, которые используются на внешнем периметре: эти знания совпадают с реальным положением дел, а также существует обоснованное понимание необходимости наличия этих систем на периметре.

Когда мы рассматривали результаты этих исследований с коллегами, которые занимаются расследованием инцидентов ИБ, оказалось, что половина инцидентов, которые приходится расследовать, связана со взломом систем, о существовании которых либо никто вообще не знает, либо о которых никто не может сказать, как и зачем они появились именно на периметре сети.

Под оценкой важности понимается оценка степени влияния тех или иных угроз на компоненты системы, которая позволяет ранжировать уязвимости в зависимости от уровня риска и от системы, в которой она обнаружена. Это особенно актуально для больших сетевых периметров.

Под управлением уязвимостями и обновлениями подразумевается здравый уровень бюрократии, позволяющий опираться на документы, регламентирующие процессы устранения уязвимостей. Их основная цель договориться внутри компании о приемлемых уровнях риска и описать зоны ответственности структурных подразделений, участвующих в процессе.

Компании, в которых описанные выше процессы не налажены, в исследование не попали. Очевидно, что уровень защищенности этих компаний невысок, за исследуемый период выявленные уязвимости не были устранены, и, согласно нашим данным, 40% таких систем будут уязвимы, а 30% сервисов — представлять угрозу.

Итак, перейдем к подробностям.

## НАШИ ГЕРОИ

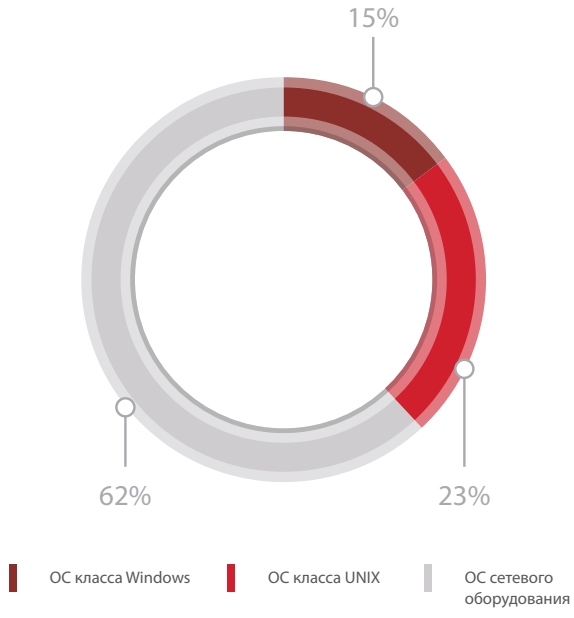
Оценка уровня защищенности проводилась в 10 организациях (одна из них — Positive Technologies, а вот названия остальных мы не раскроем). Адресное пространство исследования включало 130 000 уникальных IP-адресов. Использовались новые технологии сканирования системы MaxPatrol X. Чтобы получить данные об изменениях, сканирование указанного диапазона проводилось на регулярной основе, по возможности раз в неделю.

Исследование проводилось в 2014 и 2015 годах.

## ВАШЕ ДЫРЯВОЕ ВЕЛИЧЕСТВО…

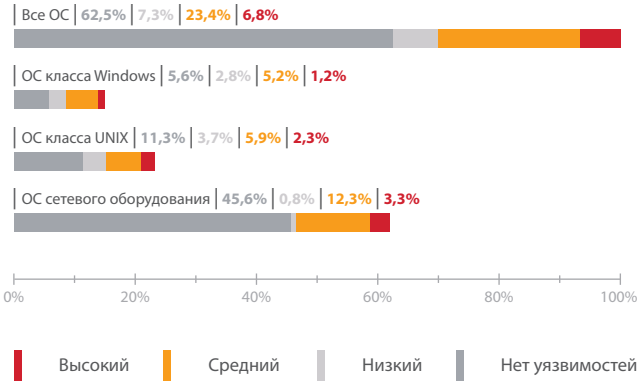
В течение всего двухлетнего периода исследования проводилось регулярное сканирование диапазона IP-адресов. Постоянно были доступны около 10 000 адресов (7,7% от общего количества). Остальные адреса либо не использовались, либо доступ к ним был ограничен на межсетевом экране. За все время проведения работ было выявлено порядка 15 000 уязвимостей.

Все обнаруженные в ходе исследования системы можно разделить на следующие группы.

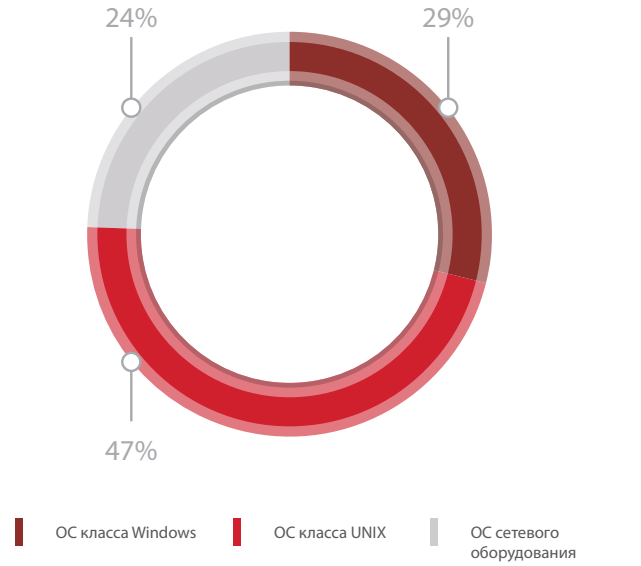


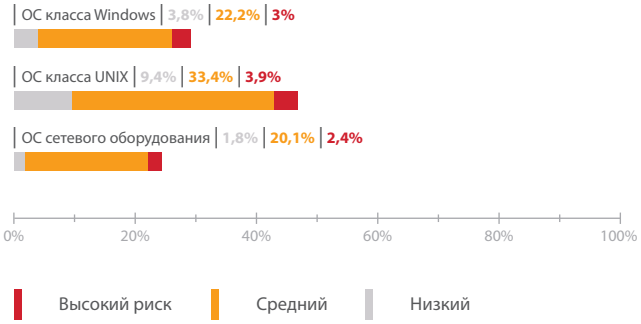
Уязвимости были выявлены на 37% систем. Из них примерно на 7% систем обнаружены уязвимости с высоким уровнем риска по CVSS, а на 23% систем — со средним уровнем риска. Если принять во внимание результаты баннерных проверок, то картина будет еще более удручающей.

Рассмотрим распределение уровня риска уязвимостей по типам ОС.




Ниже представлена зависимость количества обнаруженных уязвимостей от типа ОС.




В результате мы получили следующую закономерность.

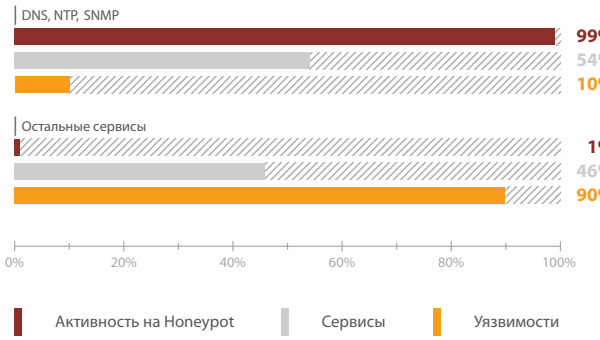
+ Для самой распространенной группы операционных систем сетевого оборудования было обнаружено наименьшее количество уязвимостей, около 25% от общего количества.
+ Для UNIX-систем было обнаружено наибольшее количество уязвимостей — более 45%.
+ И чуть менее 30% уязвимостей было отнесено к системам на базе Windows.

Зависимость количества уязвимостей от категории ОС показывает, что подходы к управлению обновлениями зависят от типа ОС, и для повышения эффективности процессов ИБ на это нужно обращать внимание.

## ЛЮБИМЫЕ МОЗОЛИ ЗЛОДЕЕВ

В ходе исследований была предпринята попытка выявить наиболее популярные у внешних злоумышленников сервисы и связать уязвимости и контекст соответствующих атак. Для этого мы разместили сенсоры PT MultiScanner, реализующие функции классической системы Honeypot, в сети Интернет. Для чистоты эксперимента мы установили их непосредственно в нашем адресном пространстве, рядом с «живыми» системами.

В норме на этих системах не должно было быть никакой активности, так как на них нет ни одного настоящего сервиса, и они не являются частью каких-либо информационных систем. Однако уже в течение первого месяца на этих системах было зафиксировано множество разных активностей, большая часть их них была связана с использованием сервисов DNS, NTP, SNMP. Мы провели анализ захваченного трафика и обнаружили явные попытки использовать сервисы для проведения DDoS-атак. Количество этих событий составило 99% от общего количества. В целом такие результаты предсказуемы: DDoS-атаки могут принести деньги, технология проведения таких атак доступна и проста, уязвимы больше половины сервисов, и они содержат около 10% всех уязвимостей.




На остальную часть сервисов пришелся лишь 1% активности. В рамках этого исследования мы рассматривали только этот процент.

Среди оставшихся сервисов мы выделили семь основных категорий:

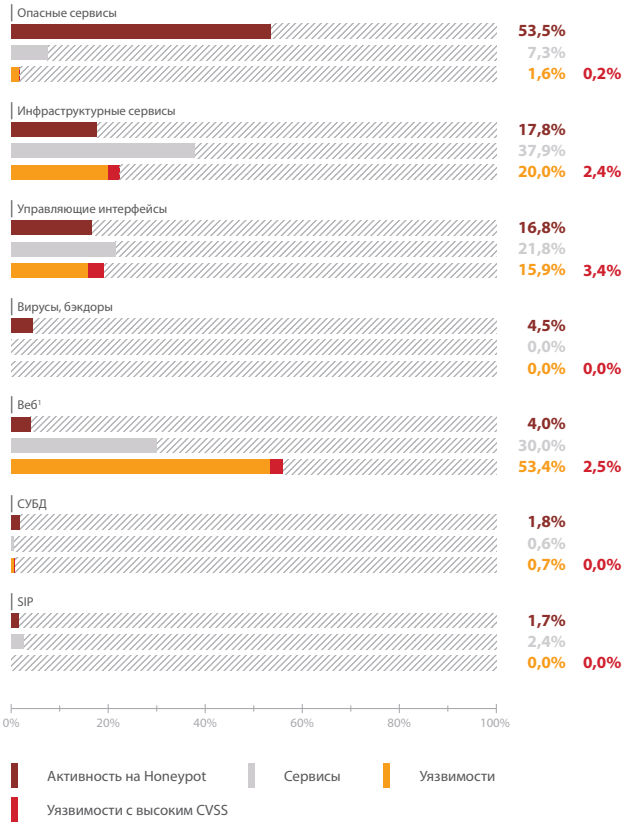
+ опасные сервисы,
+ инфраструктурные сервисы,
+ управляющие интерфейсы,
+ вирусы и бэкдоры,
+ Веб,
+ СУБД,
+ SIP.

К категории опасных сервисов мы отнесли сервисы, размещение которых на периметре может нести повышенные риски: сервисы доступа к файловой системе, RPC, службы каталогов, принтеры, сервисные интерфейсы систем виртуализации и пр.

В категорию инфраструктурных сервисов попали VPN, email- и proxy-серверы, специфичные для исследуемых организаций системы, сервисы сетевых устройств, например BGP-роутеры.

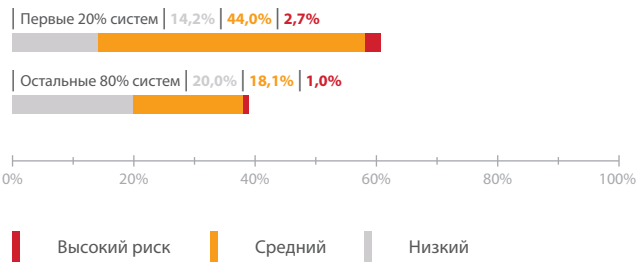
В категорию управляющих интерфейсов были включены Telnet, SSH, RDP, VNC и т. п. Состав остальных категорий очевиден.

Консолидируя информацию о количестве обнаруженных сервисов, уязвимостей и сетевой активности, мы видим, что уровень интереса хакеров к сетевым инфраструктурам весьма высок:




## «СТАТИКА» ПРОТИВ «ДИНАМИКИ»: В ПОИСКАХ ИСТИНЫ

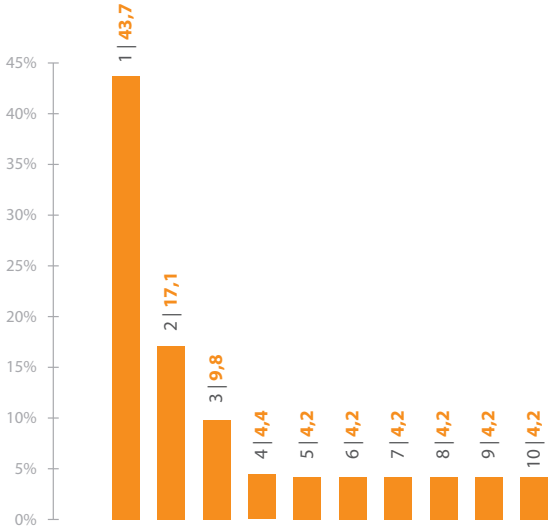
Проверим, работает ли закон Парето в такой формулировке: «20% самых уязвимых систем содержат 80% всех уязвимостей». Мы выбрали результаты сканирования уязвимых систем на случайную дату и отсортировали их по количеству уязвимостей от большего к меньшему:




Самыми уязвимыми оказались первые 20% систем, они содержали около 60% от общего количества уязвимостей. Эти системы содержат большую часть уязвимостей с высоким и средним уровнем риска, ⅔ уязвимостей с высокими значениями CVSS и примерно столько же уязвимостей со средними значениями CVSS.

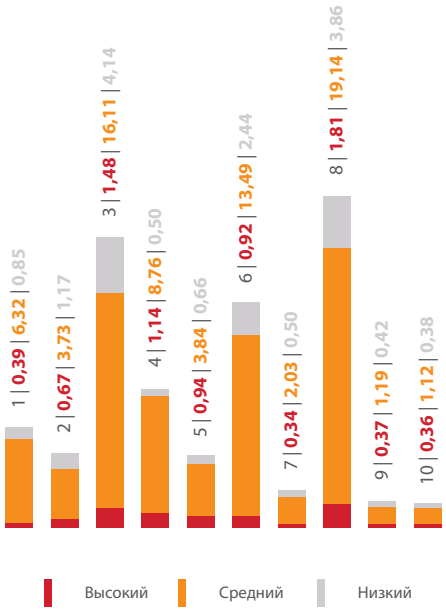
Закон Парето не выполняется. Разобьем те же системы на 10 групп, содержащих одинаковое количество систем. Для каждой группы мы вычислили значения, соответствующие распределению уязвимостей, и построили график.

Видно, что большая часть уязвимостей приходится на первые 30% систем. Остальные уязвимости распределены практически равномерно по остальным системам.




Этот результат дает статическое представление системы на случайную дату. Достаточно ли этого представления для полноценной оценки уровня защищенности сетевого периметра?

Чтобы понять, происходят ли изменения на сетевом периметре, мы разбили результаты исследования на 10 равных временных отрезков. Для каждого выгрузили количество новых сервисов и уязвимостей. Результат показал, что периметр постоянно меняется.

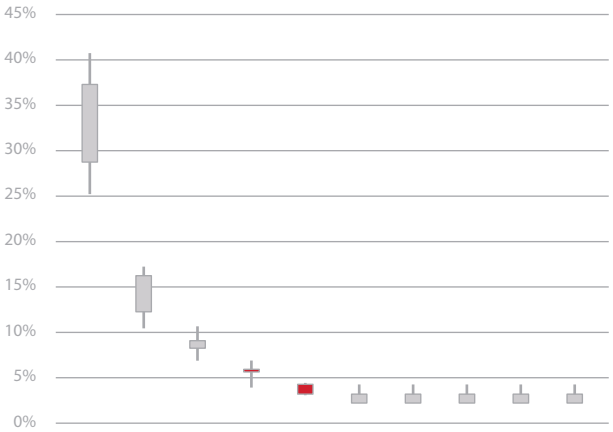




[1] Низкое количество атак на Веб связано с отсутствием на ханипотах сайтов: сервер только устанавливал соединение, но не отдавал контент. На «боевых» сайтах, которые мы защищаем с помощью PT AF, фиксируется значительно большее количество опасной активности.

Поэтому нельзя использовать статическое распределение уязвимостей.

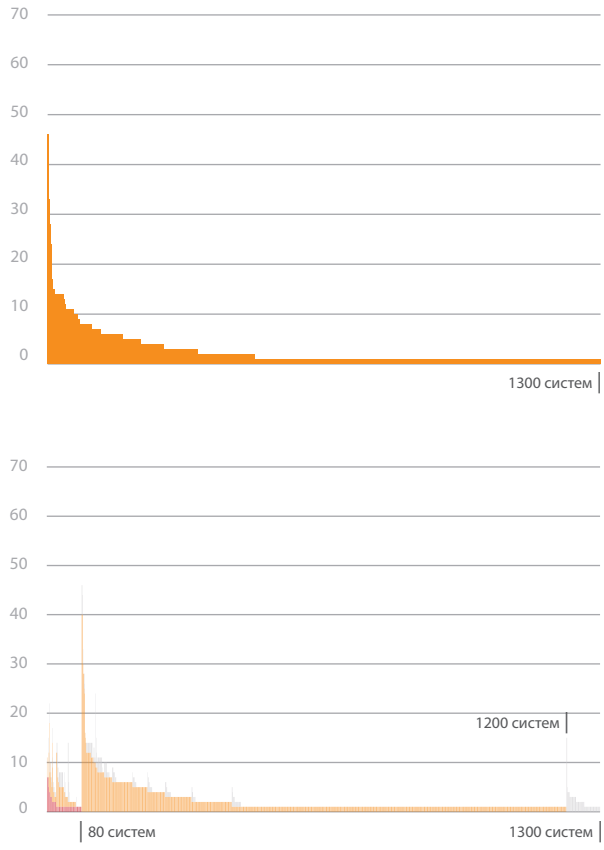
Лучший вариант отображения изменений во времени удалось найти в финансовой сфере. Для отображения колебаний используется специальная диаграмма — японские свечи: в тело свечи мы поместим начало и завершение исследуемого периметра, а фитили будут отображать минимальное и максимальное значение распределения уязвимостей. Снижение параметров — признак улучшения: серая свеча обозначает уменьшение доли уязвимостей, красная — увеличение доли.

Эти результаты подтверждают предположение о распределении большей части уязвимостей на 30% самых уязвимых систем:




## ДВЕРИ ОТКРЫТЫ, ПОЕХАЛИ?

В первый временной интервал попало около 1300 уязвимых систем. Распределение уязвимостей на этих системах будет выглядеть следующим образом:

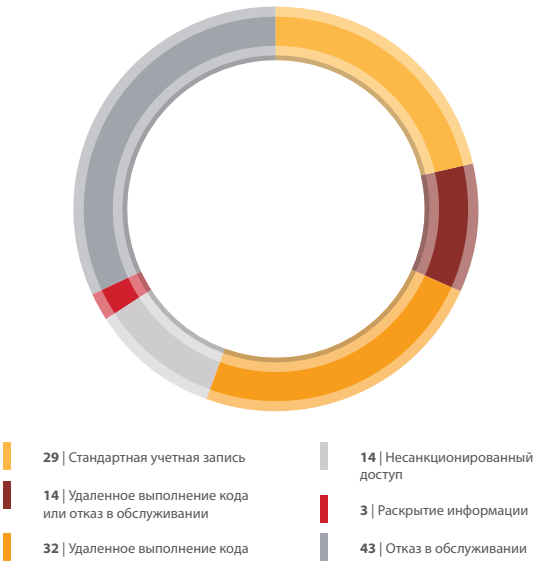



Из 1300 уязвимых систем 80 содержали уязвимости с высокими значениями CVSS и четверть этих систем — более одной уязвимости с высоким значением CVSS. Мы считаем этот участок самым опасным, поэтому сопоставили их с информацией об эксплуатации уязвимостей в базе знаний PT KB.

По завершении этой проверки мы получили:

1. Информацию о доступности инструментов для эксплуатации уязвимости:


2. Тип влияния уязвимости на компоненты системы:

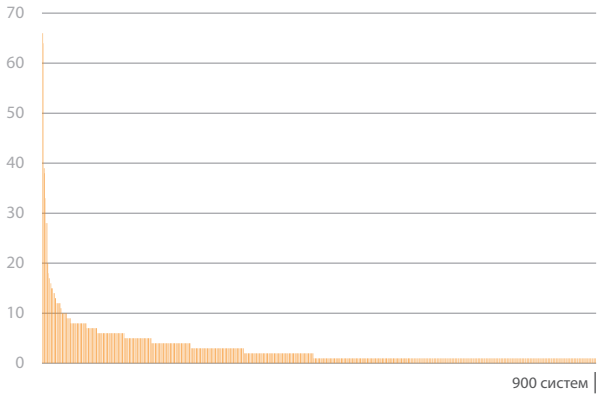



Уровень опасности рассматриваемых уязвимостей на начало исследования был весьма высок: более чем для половины уязвимостей существуют общедоступные инструменты, а четверть позволяет удаленно выполнить код. Для 46 уязвимостей удаленного выполнения кода (RCE) было обнаружено 36 эксплойтов, из них для 6 имеются готовые инструменты в открытом доступе, а 16 могли быть использованы с применением стандартных хакерских инструментов:

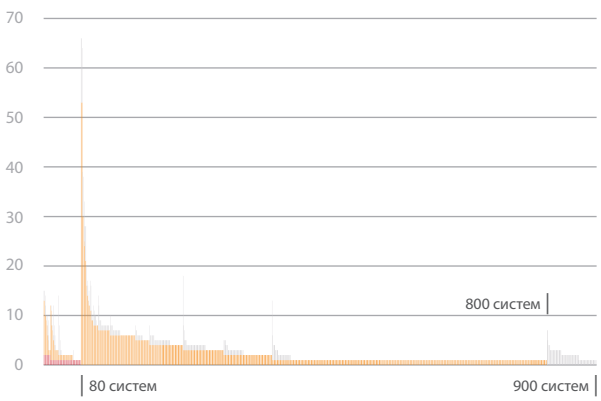

Уровень злоумышленника, который может воспользоваться такой уязвимостью, весьма низкий: достаточно иметь базовые знания и доступ к Metasploit.

Максимальное количество уязвимостей было зафиксировано в одном из временных периодов: 1700 систем уязвимы, из них 120 содержали уязвимости с высоким уровнем CVSS.

Благодаря повышению уровня защищенности на момент завершения исследования количество уязвимых систем уменьшилось до 900.




Систем, содержащих более двух уязвимостей с высоким CVSS, не осталось: остались только новые уязвимости.



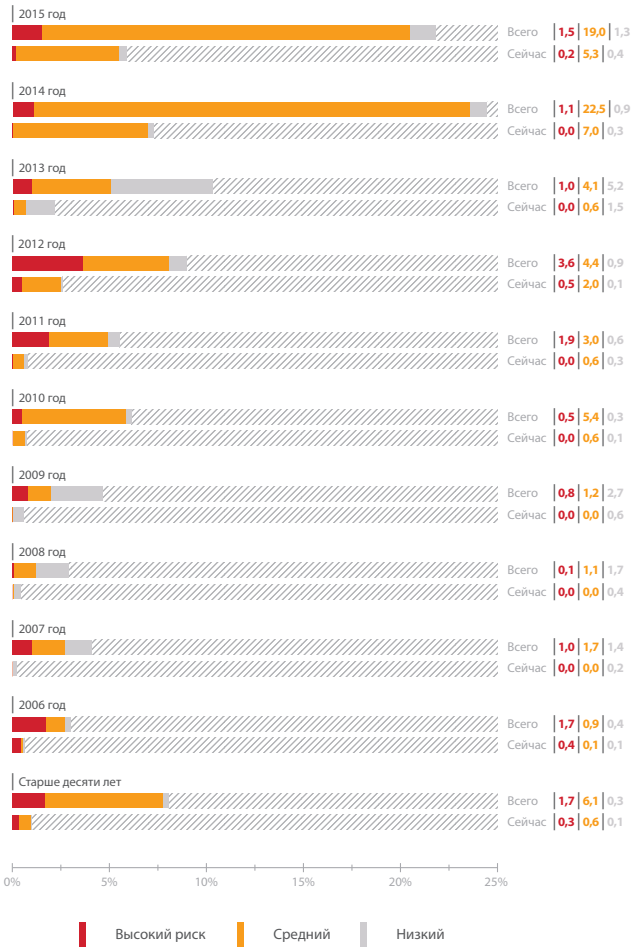

Ниже приведена информация о доступности эксплойтов для этих уязвимостей.


И тип влияния уязвимости на компоненты системы.


Если мы сопоставим эти результаты, то увидим, что все еще остается много RCE-уязвимостей с готовыми эксплойтами (32). Более того, 29 из указанных уязвимостей — повышенного риска, так как инструментарий для их эксплуатации размещен в открытом доступе.

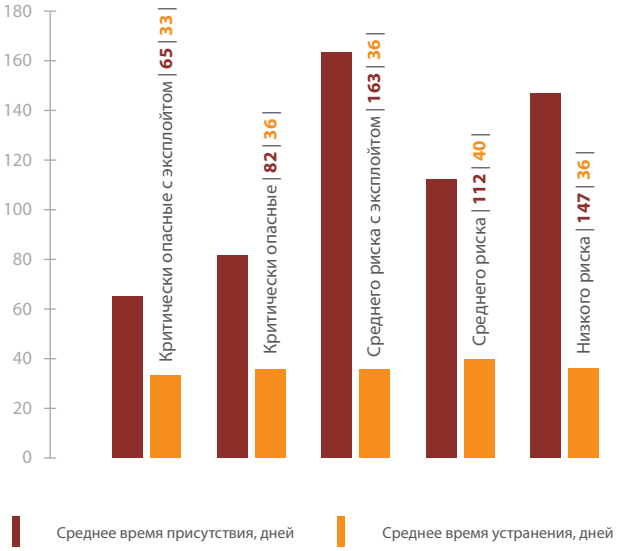

## ПОДВЕДЕМ ИТОГИ

Рассмотрим другие параметры уязвимостей, которые могут повышать риск эксплуатации, и сопоставим их с результатами, приведенными выше.




В отчетах Verizon 2015 года приводится статистика, согласно которой 99% успешных атак использовали уязвимости, информация о которых была доступна более года. Судя по результатам проведенного нами исследования, количество таких уязвимостей на сетевых периметрах весьма велико. При этом информация о 50% уязвимостей стала доступной за анализируемый период времени, остальные уязвимости известны уже более двух лет. На графике представлено процентное соотношение уязвимостей за весь исследуемый период (верхний столбец) и уязвимостей на момент окончания исследования (нижний столбец).

Очевидно, чем дольше известно об уязвимости, тем больше времени могло быть потрачено на разработку средств ее эксплуатации. Кроме того, Verizon сообщает, что если для уязвимости существует эксплойт, то эта уязвимость будет проэксплуатирована с вероятностью 50% в первый месяц существования эксплойта и с вероятностью 100% в первый год его существования. Поэтому крайне важно время присутствия уязвимости на периметре. В рамках проведенных исследований этот параметр разбит на два: для систем, которые не обновляются, и систем, которые обновляются регулярно.




Темно-красным обозначено общее время присутствия уязвимостей на периметре. Видно, что для критически опасных уязвимостей значения составляют от 60 до 80 дней. Давно появившиеся и незакрытые уязвимости имеются в 5% систем. Это небольшое количество, но защищенность системы равняется уровню защищенности ее самого слабого звена.

Оранжевым обозначено среднее время устранения уязвимости: оно составляет от 30 до 40 дней для любой группы уязвимостей. По нашему мнению, это приемлемый показатель (к системам, расположенным на периметре, предъявляются требования по доступности, поэтому все обновления требуют тщательной предварительной проверки).

Взгляд на систему только изнутри не дает объективной оценки реального состояния безопасности периметра: эффективную систему безопасности построить не получится, поскольку принимаемые меры не релевантны текущей ситуации.

Внедрение процессов контроля внешнего периметра может занять много времени и оказаться очень трудоемким, но позволит повысить уровень зрелости процессов информационной безопасности в организации. Для построения эффективной системы защиты информации необходимо знать — что и от чего мы собираемся защищать.

Первые шаги в этом направлении можно начать даже с минимальным бюджетом, например используя open-source утилиты. Для расширения возможностей используемых инструментов обращайтесь к специалистам Positive Technologies.