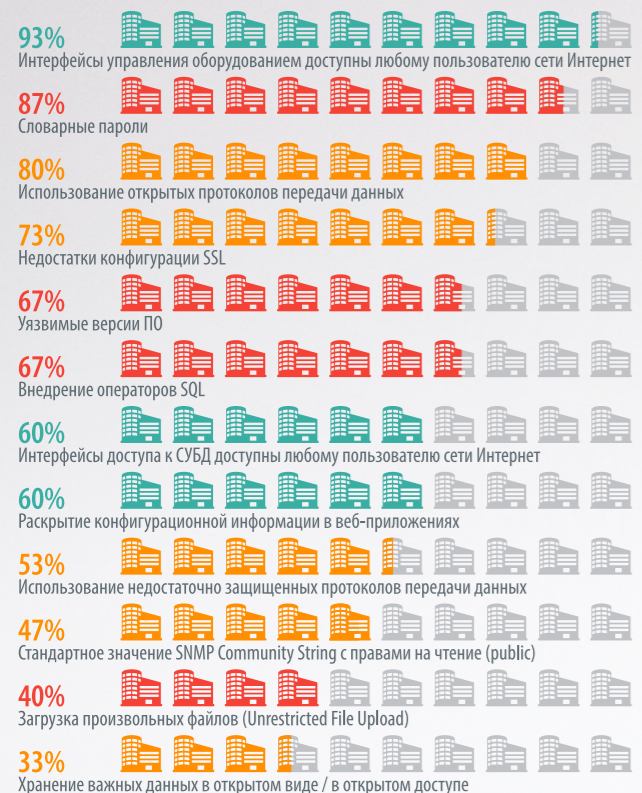




# СТАТИСТИКА УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ – 2014

## Наиболее распространенные уязвимости на сетевом периметре



## Векторы атак для преодоления сетевого периметра



## Сложность преодоления периметра

13%

Не удалось преодолеть периметр в заданных границах работ

13%

Средняя (с использованием социальной инженерии)

13%

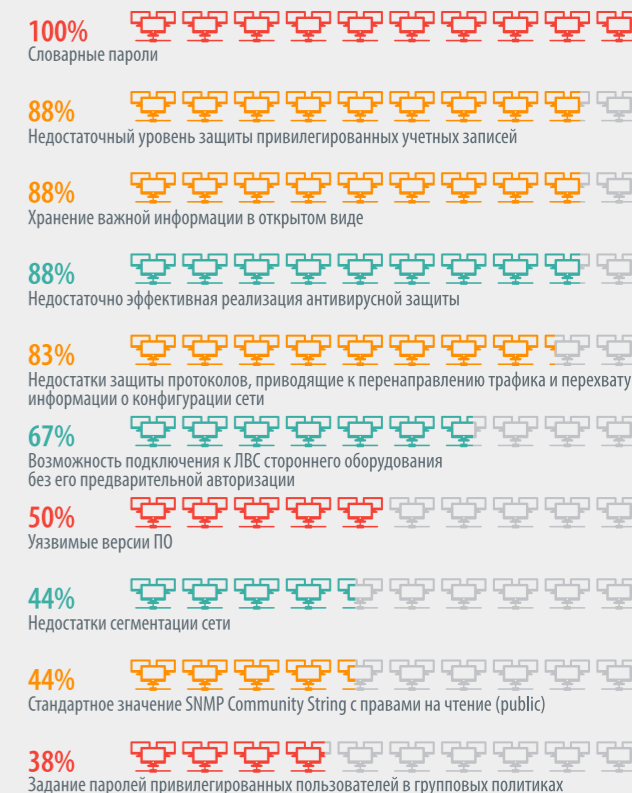
Средняя (без использования социальной инженерии)

## Критически важные ресурсы

Сложность получения доступа к критическим ресурсам со стороны внутреннего нарушителя

6% Тривиальная  
50% Низкая  
44% Средняя

## Наиболее распространенные уязвимости внутренней сети



## Уровень привилегий, полученных от лица внешнего нарушителя (доли систем)

13%

Доступ к расширенной конфигурационной информации



Уязвимости, получившие наибольшую известность в 2014 г., – Heartbleed и Shellshock, на практике оказались не столь распространены, как изначально опасались СМИ: во многом благодаря широкому распространению информации большинство крупных компаний оперативно устанавливали обновления. Однако эти действия зачастую были выборочными: устаревшее ПО, содержащее критические уязвимости, было выявлено в 78% систем.

27%

Максимальные привилегии в критических системах

53%

Полный контроль над инфраструктурой

54%

Низкая

7%

Тривиальная

## Уровень привилегий, полученных от лица внутреннего нарушителя (доли систем)

22%

Максимальные привилегии в критических системах

78%

Полный контроль над инфраструктурой

3 ШАГА

требуется в среднем для получения доступа к критически важным системам