Результаты анализа защищенности информационных систем

2016

POSITIVE TECHNOLOGIES

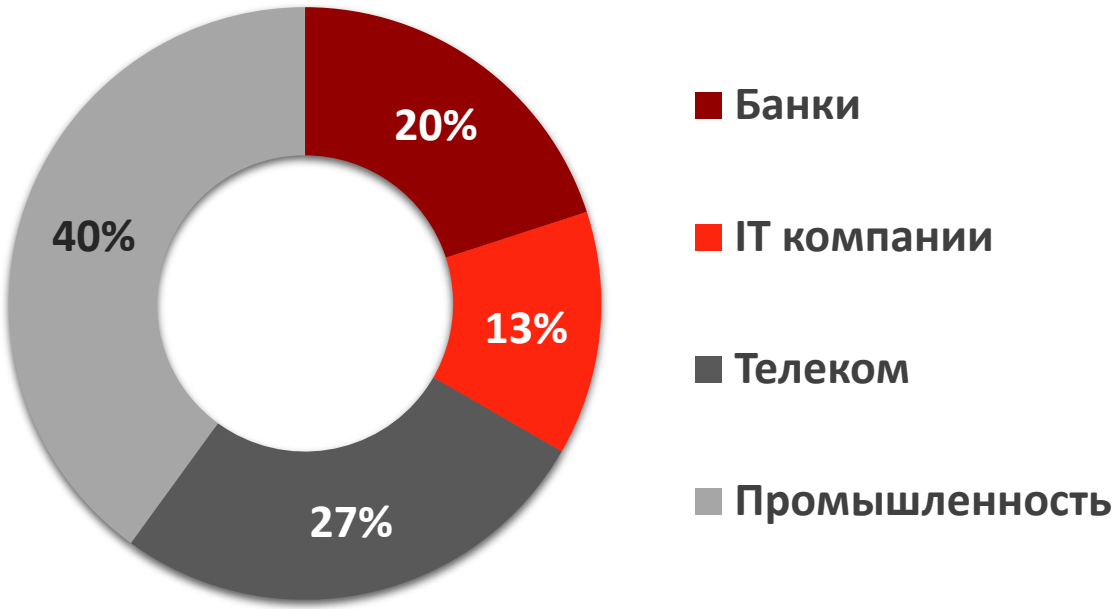
ptsecurity.com

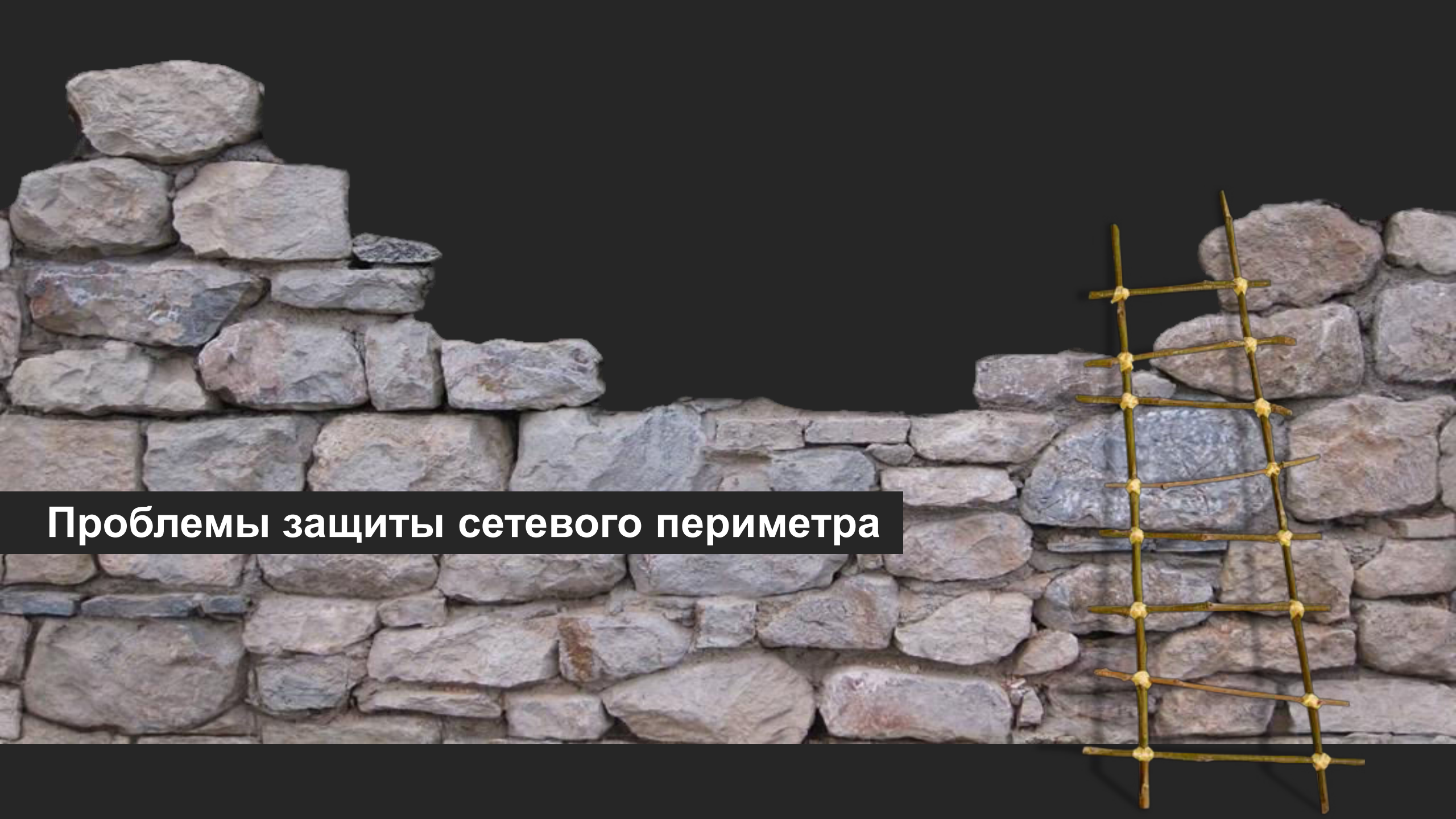
Практика анализа защищенности: объекты анализа

POSITIVE TECHNOLOGIES

Крупнейшие российские и зарубежные компании:

- Территориально распределенная инфраструктура
- Множество дочерних компаний и филиалов
- Сотни узлов на сетевом периметре
- Тысячи устройств ЛВС (серверы, рабочие станции, сетевое оборудование)





Проблемы защиты сетевого периметра

Векторы проникновения

POSITIVE TECHNOLOGIES

91% Системы с доступными из Интернета интерфейсами управления

Векторы проникновения

POSITIVE TECHNOLOGIES

91% Системы со словарными паролями для доступа к веб-приложениям

Векторы проникновения

POSITIVE TECHNOLOGIES

73% Системы, где чувствительные данные хранятся в открытом виде

Векторы проникновения

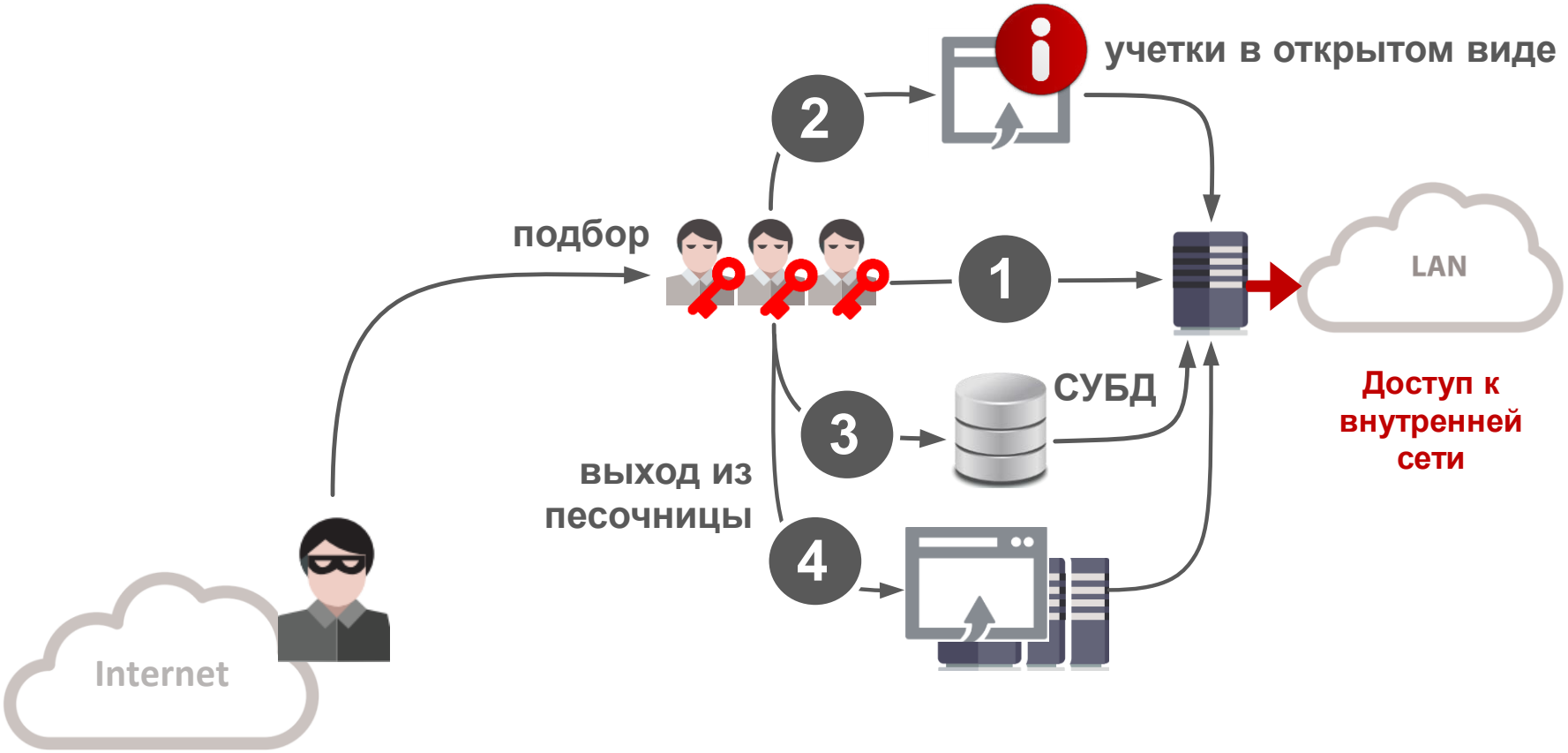
POSITIVE TECHNOLOGIES

27% Системы со словарным паролем к СУБД

45% Системы с доступными для подключения интерфейсами СУБД

Векторы проникновения

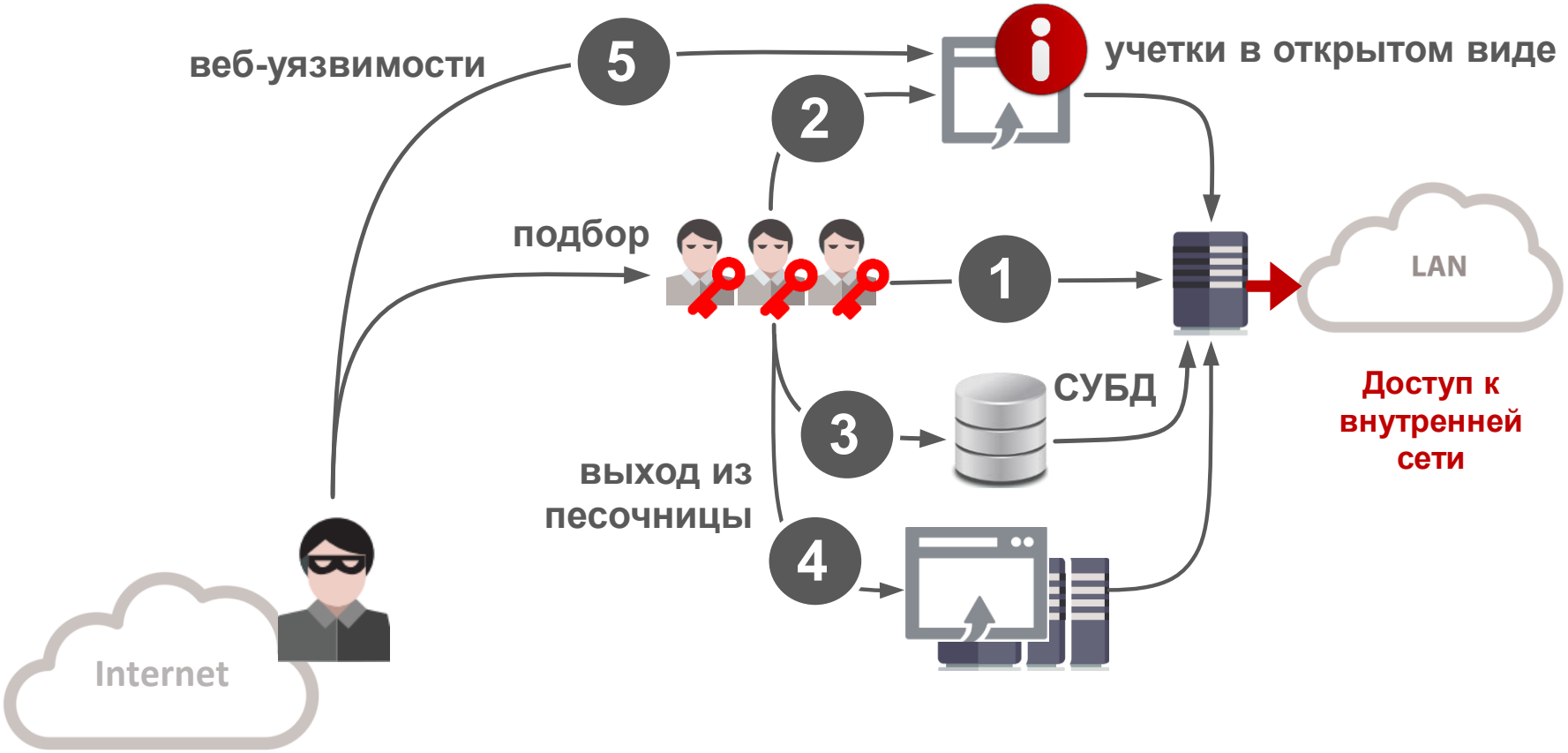
POSITIVE TECHNOLOGIES



27% Системы с доступными для подключения корпоративными сервисами

Векторы проникновения

POSITIVE TECHNOLOGIES



80% Системы с уязвимыми веб-приложениями

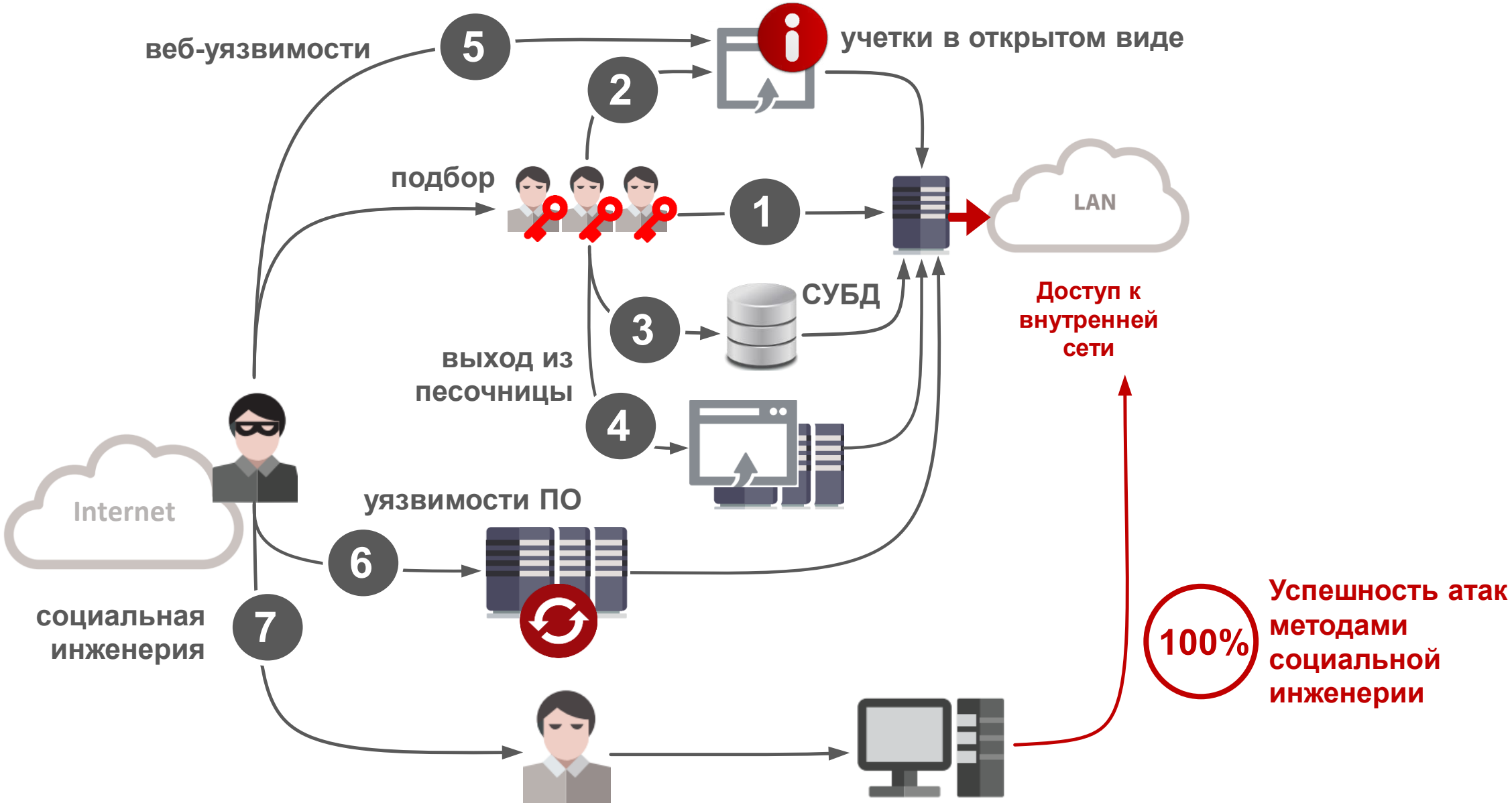
Векторы проникновения

POSITIVE TECHNOLOGIES

91% Системы с уязвимым ПО

Векторы проникновения

POSITIVE TECHNOLOGIES



Векторы проникновения

POSITIVE TECHNOLOGIES

Векторы проникновения

POSITIVE TECHNOLOGIES

Векторы проникновения

POSITIVE TECHNOLOGIES

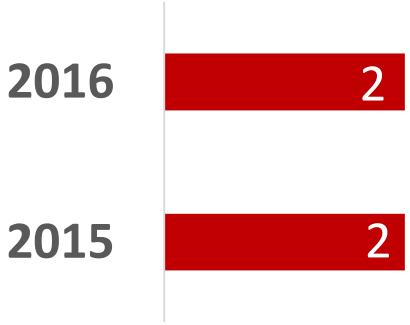
100%

Успешность атак через WiFi сети

Тенденции

POSITIVE TECHNOLOGIES

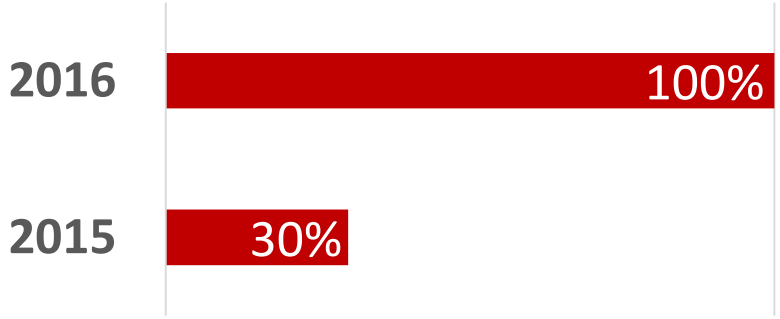
Среднее число шагов к ЛВС



Вектор проникновения (доля систем)

Успешность социотехнических атак (доля систем)

Успешность атак через беспроводную сеть (доля систем)



Социальная инженерия

POSITIVE TECHNOLOGIES

Фишинг сегодня это:

- **Первый шаг при целевой атаке**
- **Основной способ распространения ВПО**

Доля сотрудников (в среднем по компаниям)

Недостатки защиты беспроводной сети

POSITIVE TECHNOLOGIES

3/4 систем

- Несанкционированные точки доступа
- Доступность корпоративных WiFi за пределами КЗ

1/2 систем

- Не проверяется сертификат сети
- Слабые ключи


```
                    Aircrack-ng 1.2 rc4

[00:00:00] 304/647 keys tested (948.49 k/s)

Time left: 0 seconds                                    46.99%

                  KEY FOUND! [ 1234qwer ]
```

```
PS C:\Users\chris.admin\Desktop> Invoke-Mimikatz -Command '"lsadump::dcsync /use
r:dev\krbtgt"'
Hostname: WINDOWS4.dev.testlab.local / S-1-5-21-4275052721-3205085442-277024194
2

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 23 2015 23:05:23)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with 16 modules * * */


mimikatz(powershell) # lsadump::dcsync /user:dev\krbtgt
[DC] 'dev.testlab.local' will be the domain
[DC] 'SECONDARY.dev.testlab.local' will be the DC server
```

Недостатки защиты ресурсов ЛВС

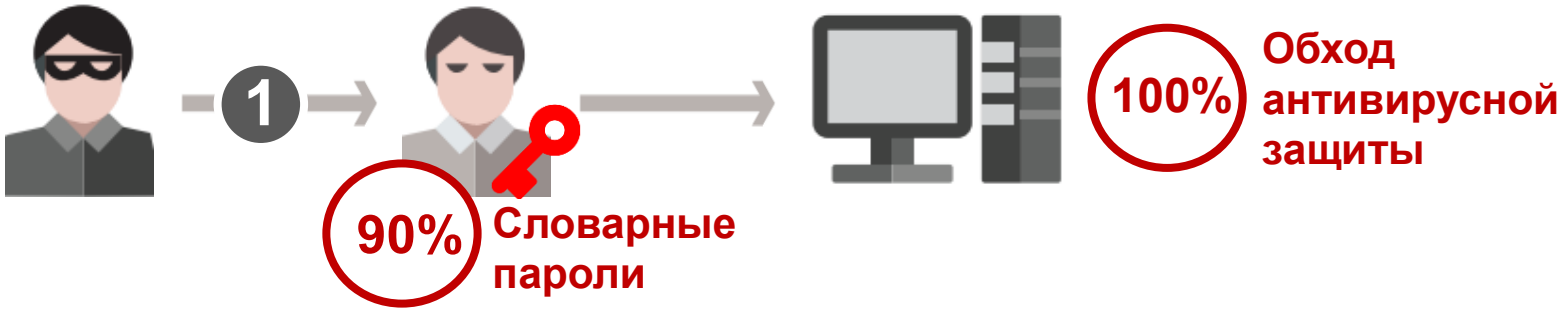
```
Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
```

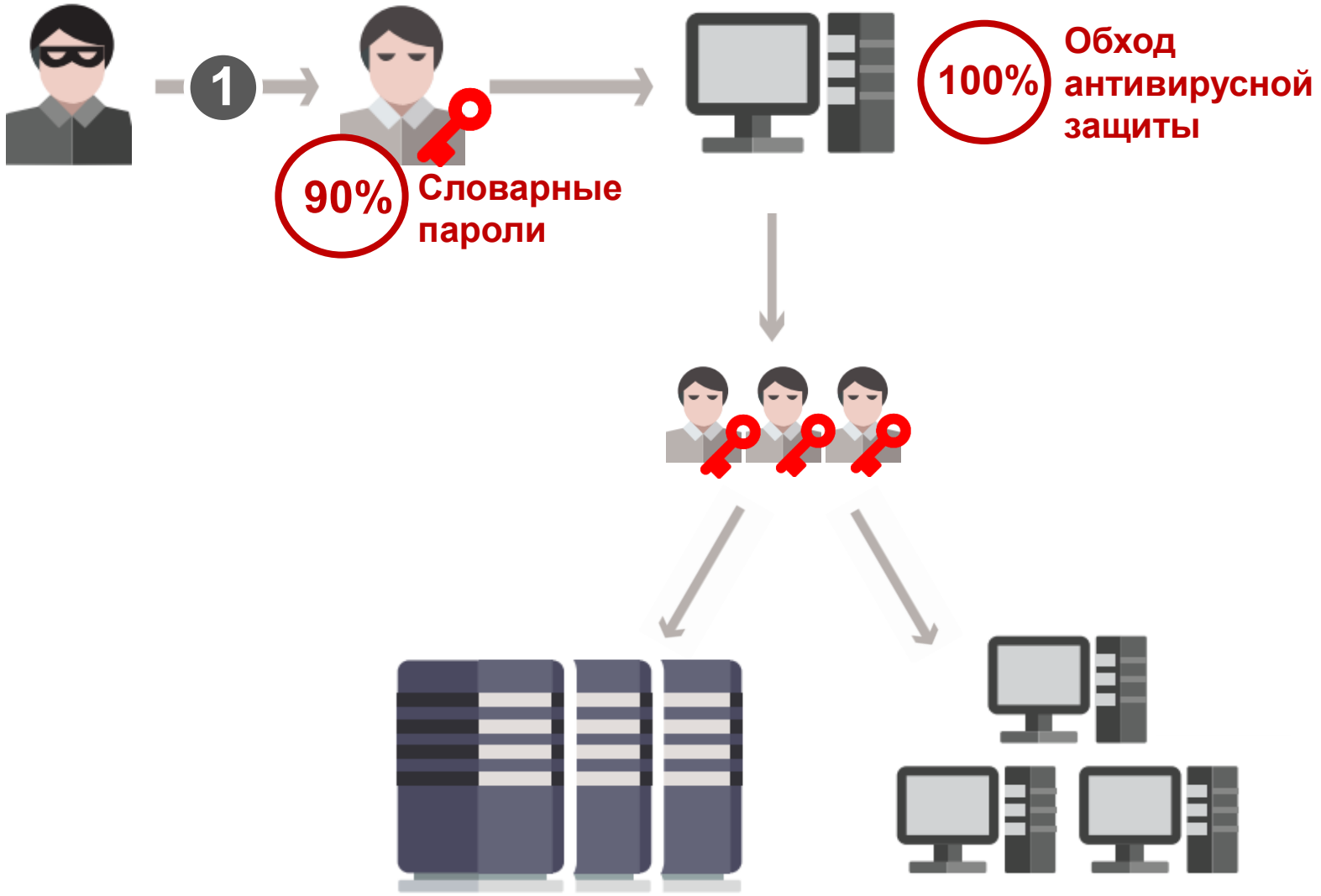
Векторы атаки на ресурсы ЛВС

POSITIVE TECHNOLOGIES



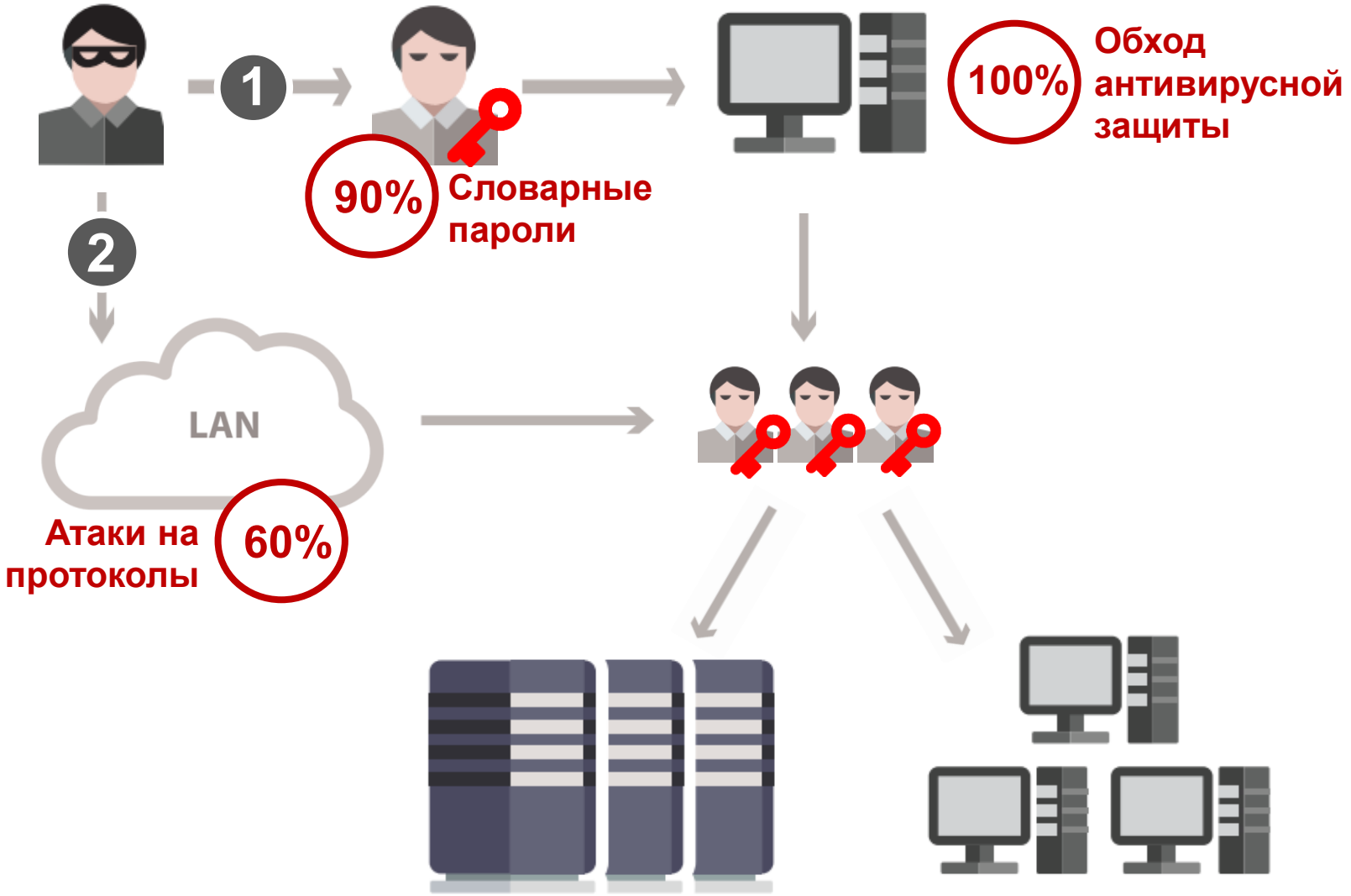
Векторы атаки на ресурсы ЛВС

POSITIVE TECHNOLOGIES



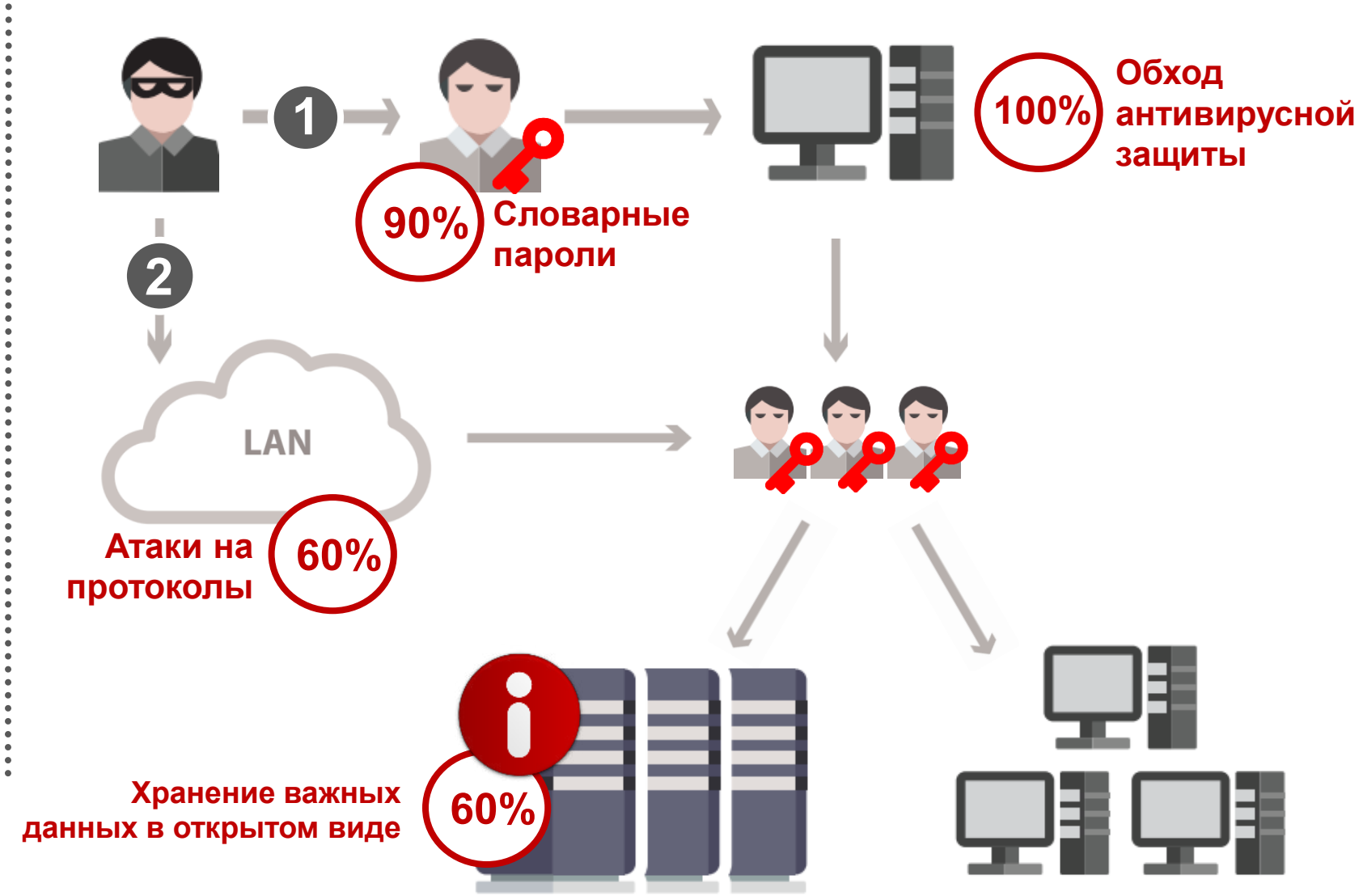
Векторы атаки на ресурсы ЛВС

POSITIVE TECHNOLOGIES



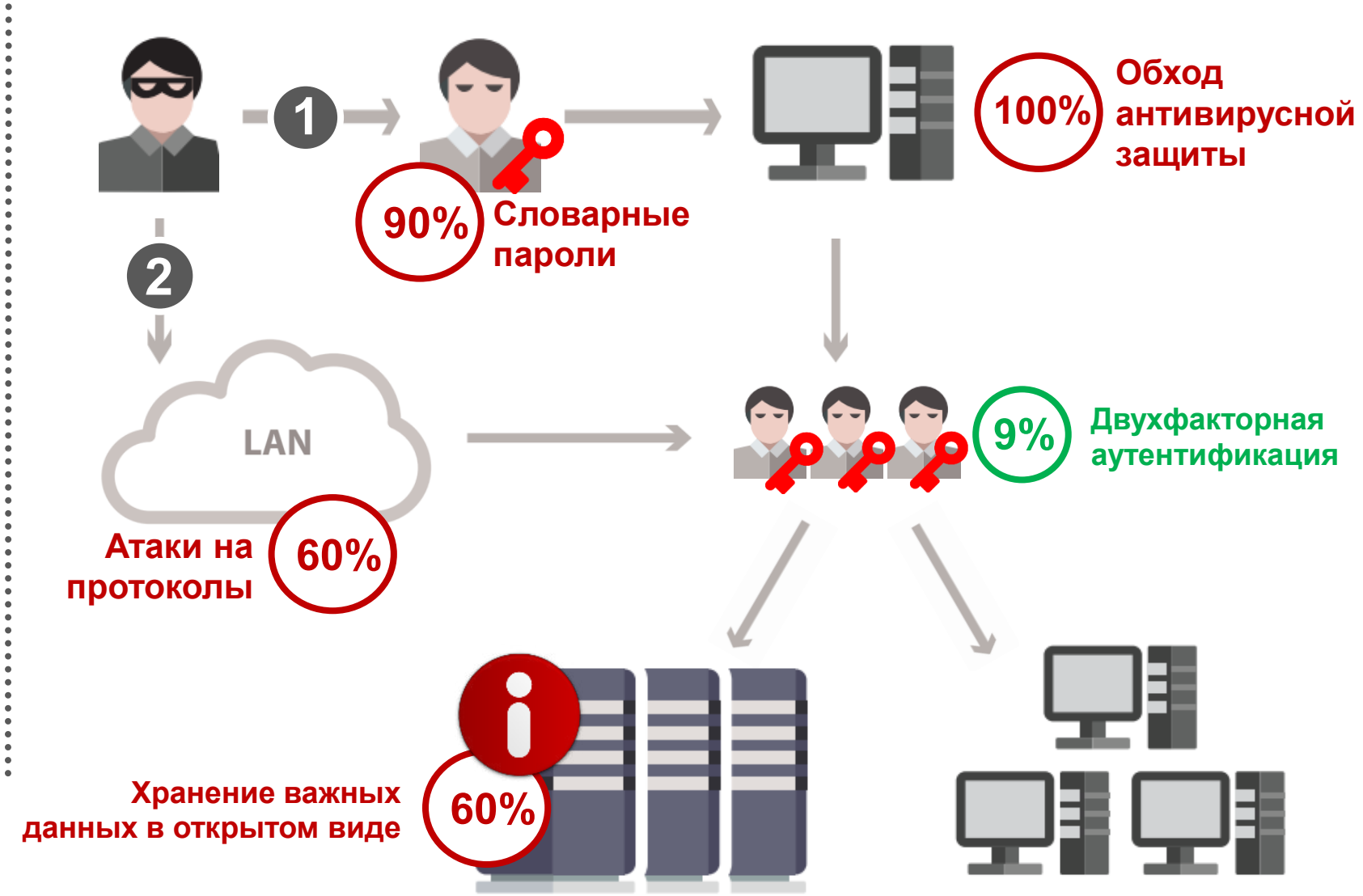
Векторы атаки на ресурсы ЛВС

POSITIVE TECHNOLOGIES



Векторы атаки на ресурсы ЛВС

POSITIVE TECHNOLOGIES



Векторы атаки на ресурсы ЛВС

POSITIVE TECHNOLOGIES

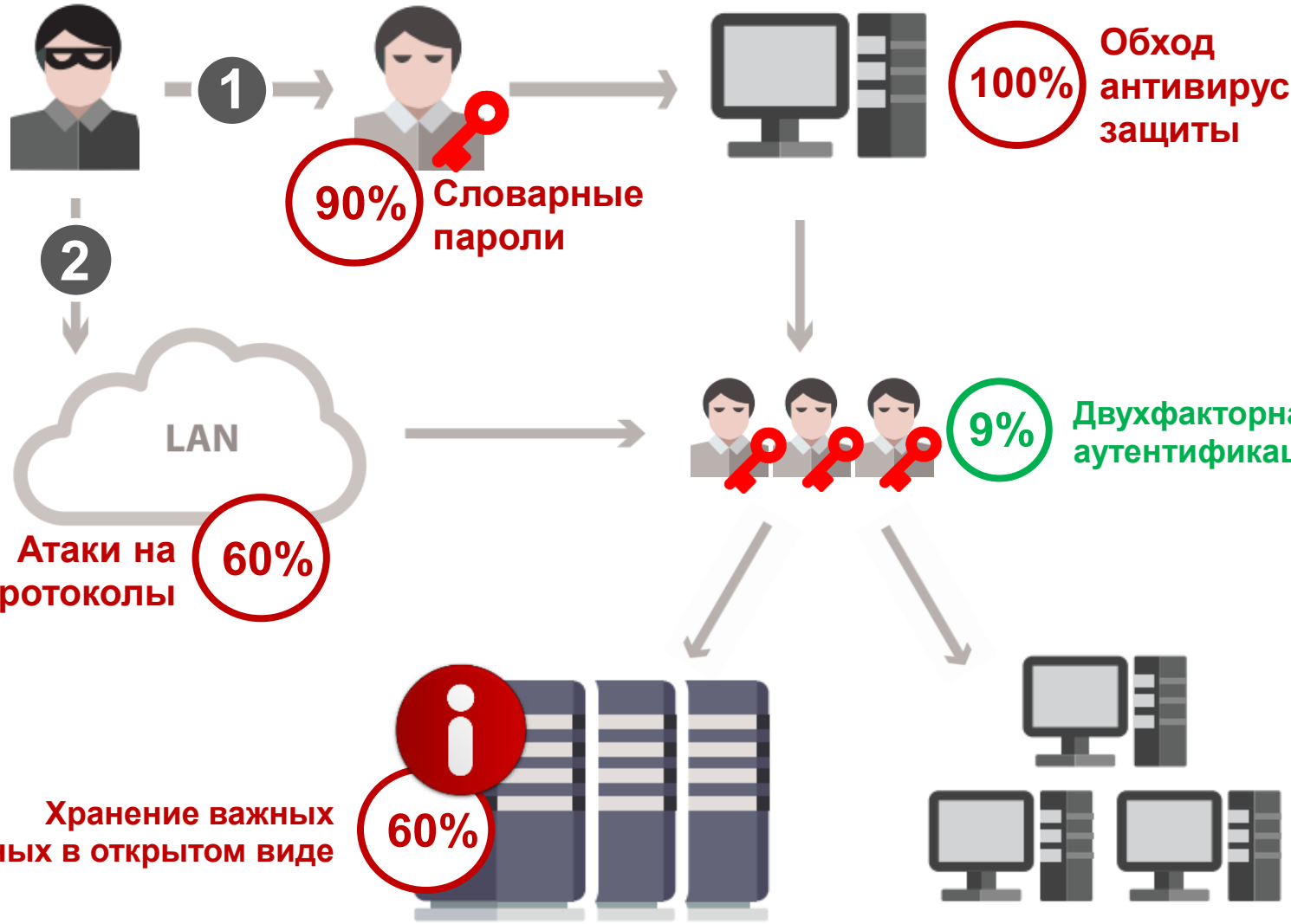
100% систем

Полный контроль над инфраструктурой

Независимо от типа нарушителя

Атака в 4 шага

Ничего не изменяется



Прогнозы

POSITIVE TECHNOLOGIES

Рост числа целевых атак

Рост атак на КИС банков

Рост атак на веб-ресурсы государственных организаций

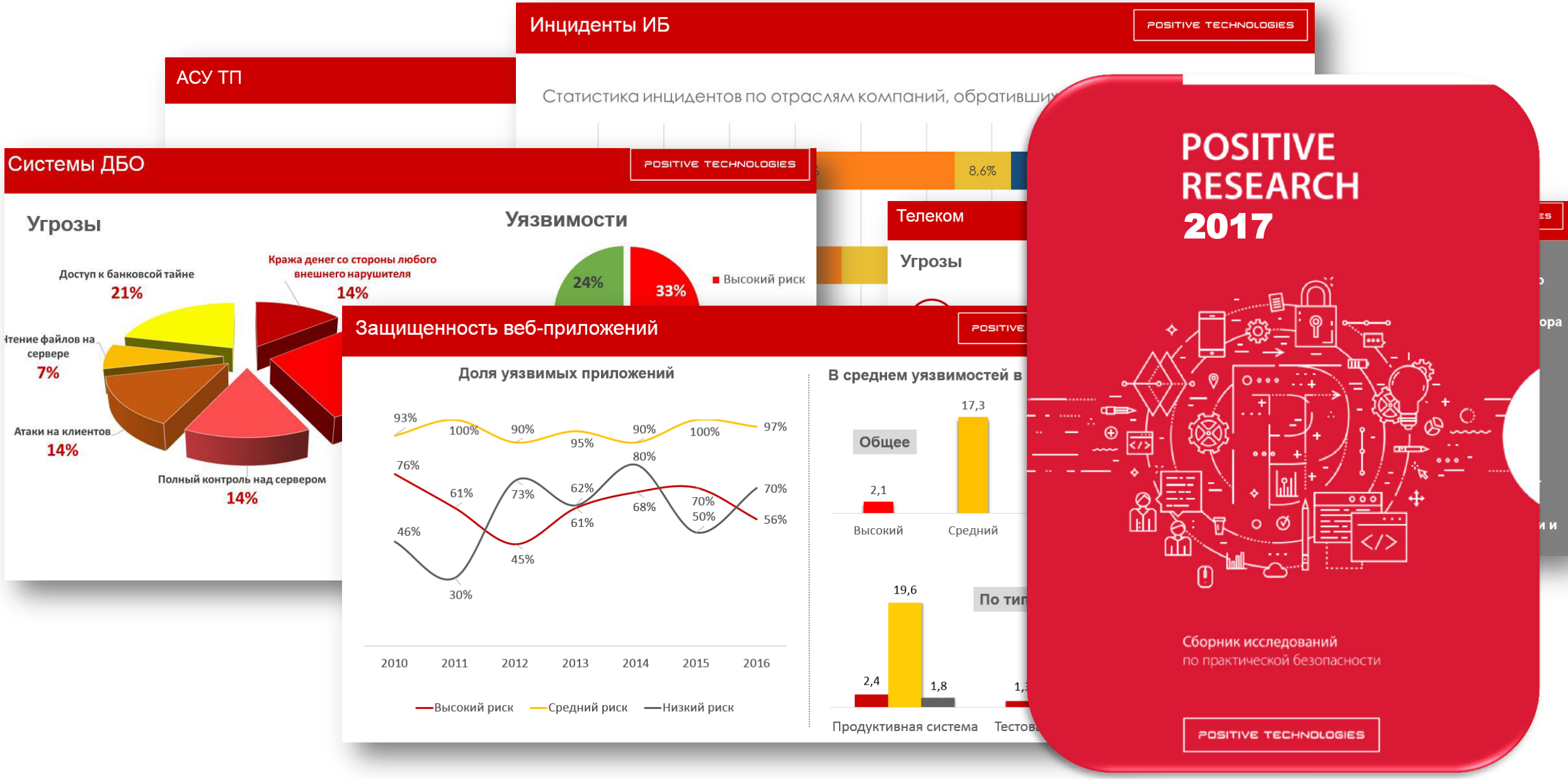
Экспертиза

POSITIVE TECHNOLOGIES

Индустрия	Максимальное покрытие по всем направлениям работ			
Финансовые организации	✓	✓	✗	✓
Промышленность	✓	✓	✓	✓
Транспорт	✓	✓	✓	✓
ИТ	✓	✓	✗	✓
Телеком	✓	✓	✗	✓
Государственные организации	✓	✓	✓	✓
Другие	✓	✓	✓	✓
Работы	Пентест	Анализ защищенности веб-приложений	Анализ защищенности АСУ ТП	Расследование инцидентов

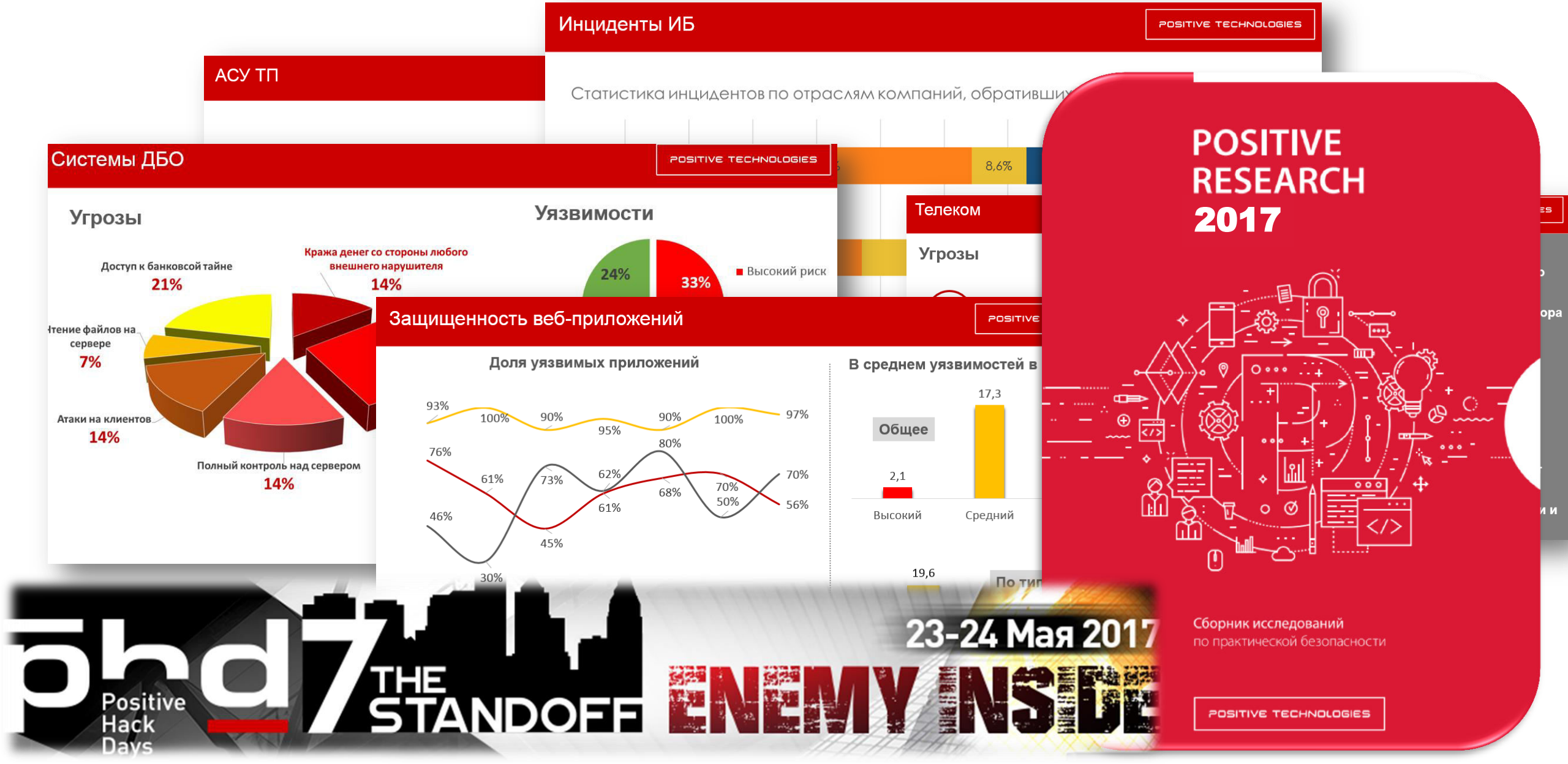
И еще очень много интересного

POSITIVE TECHNOLOGIES



И еще очень много интересного

POSITIVE TECHNOLOGIES



Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.ru