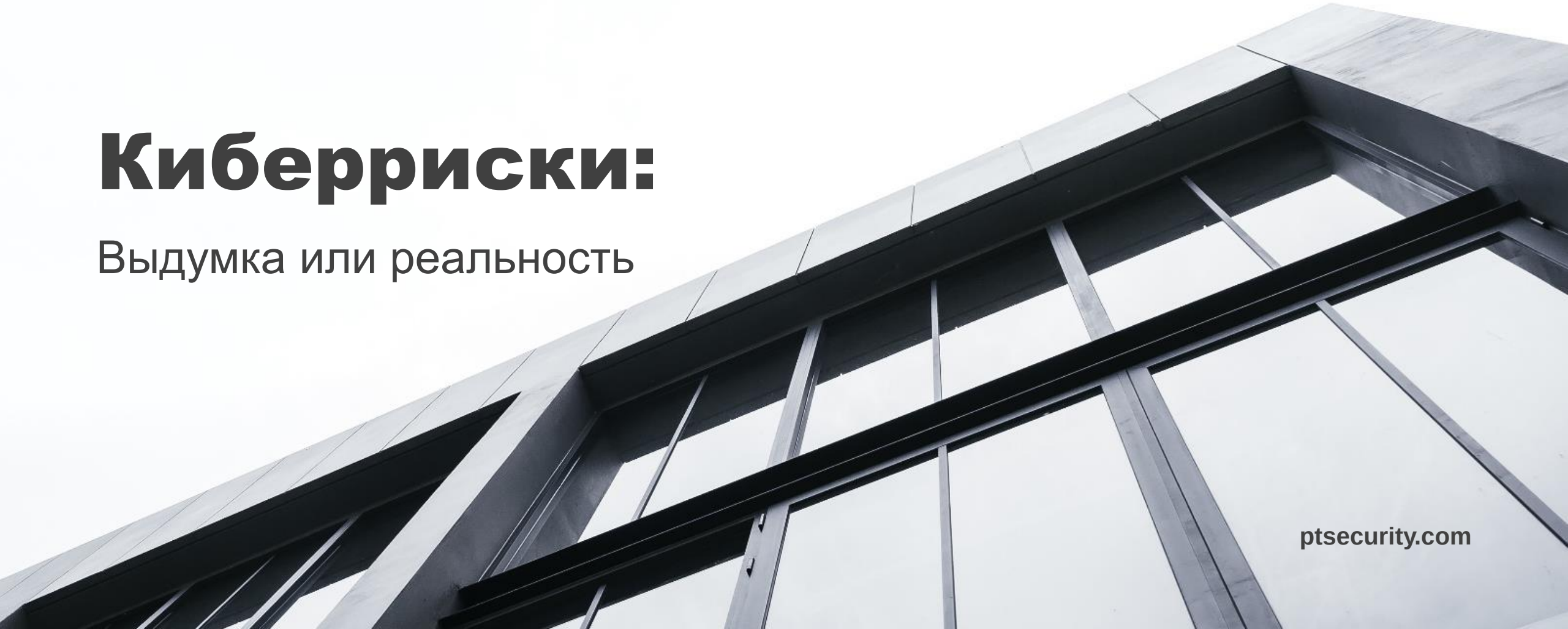
POSITIVE TECHNOLOGIES

Киберриски:

Выдумка или реальность



ptsecurity.com

Наши исследования

Все исследования

Статистика кибератак в 2020 году

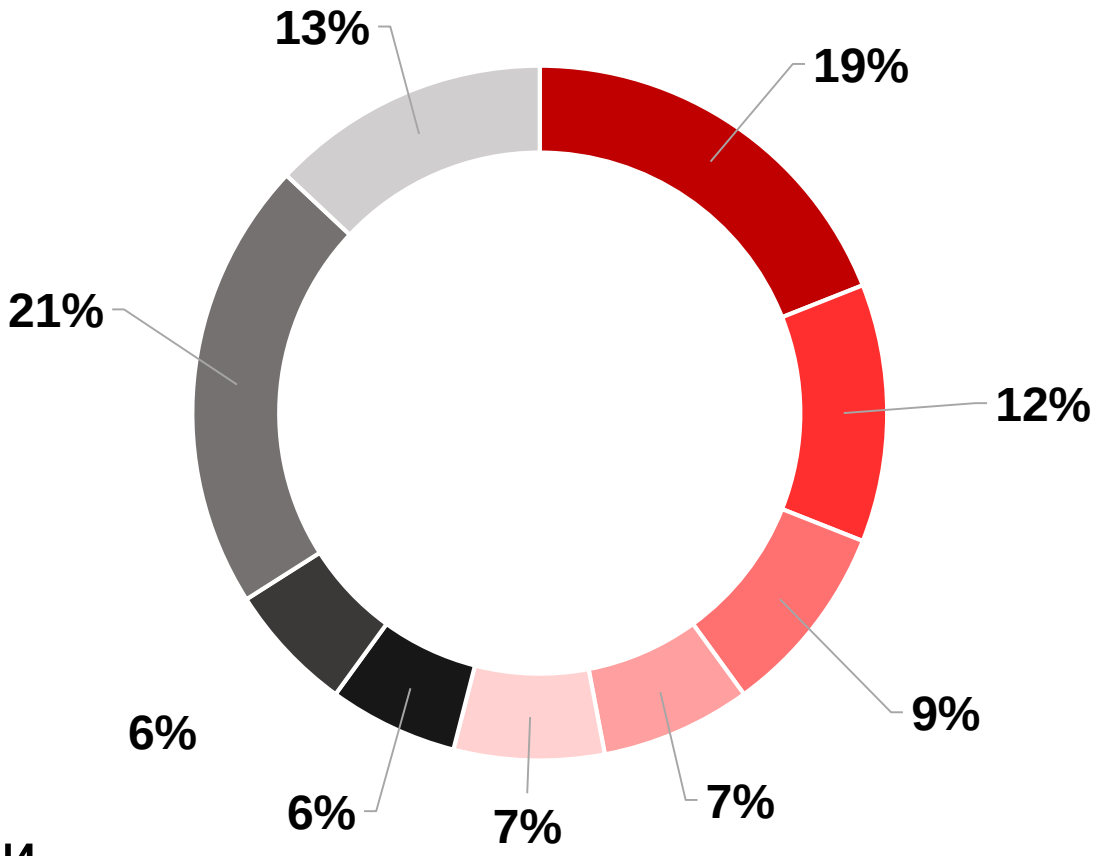
51% рост количества атак в 2020 году по сравнению с 2019

70% атак были целевыми – то есть направленными на конкретную компанию, отрасль или частное лицо

Категории жертв среди организаций

86%

всех атак направлены на организации



Доля атак на организации

- Госучреждения
- Промышленность
- Медучреждения
- Финансовые организации
- Наука и образование
- Торговля
- IT-компании
- Другие
- Без привязки к отрасли

Colonial Pipeline

- **Почти неделя простоя**
  Прекращение работы половины заправок в некоторых штатах юго-востока США
- Повышение оптовых цен на бензин в США
- Повышенный ажиотаж на топливо
- **Финансовые потери**
  Выплата вымогателям $4 400 000
- Репутационный ущерб

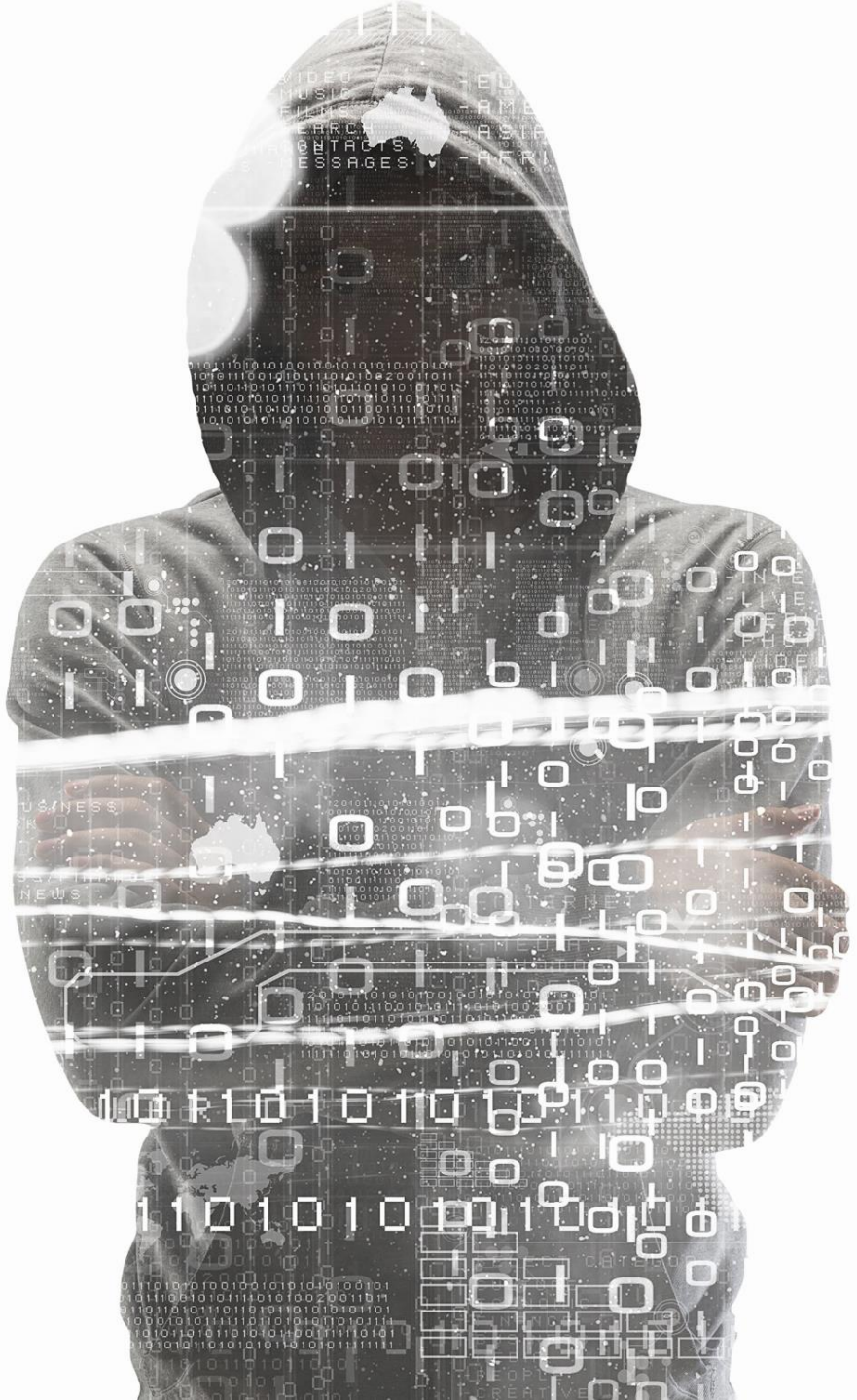
SolarWinds

- Финансовые потери
- Репутационный ущерб
- Утечка конфиденциальных данных

Среди жертв атаки:

- Государственный департамент США
- Министерство финансов США
- Министерство торговли США
- Национальной управление по телекоммуникациям и информации США
- Министерство внутренней связи США
- Microsoft
- Cisco
- FireEye

Для любой компании существуют события, наступление которых может привести к нежелательным для бизнеса последствиям



ptsecurity.com

Нужна результативная кибербезопасность

Прозрачность и измеримость
Уровень защищенности проверяется в любой момент и результаты аудита дают независимую оценку достигнутых KPI

Участие руководства
Результаты ИБ достигаются за счет координации подразделений и участия руководства, а не только за счет преимущественно финансовых инвестиций

Модификация процессов
Многие риски закрываются путем отладки процессов ИТ и ИБ , а не только за счет внедрения средств защиты

Результативность и понятность
Работа службы сфокусирована на исключении поистине важных для организации и руководства недопустимых событий, ее результат виден и понятен всем

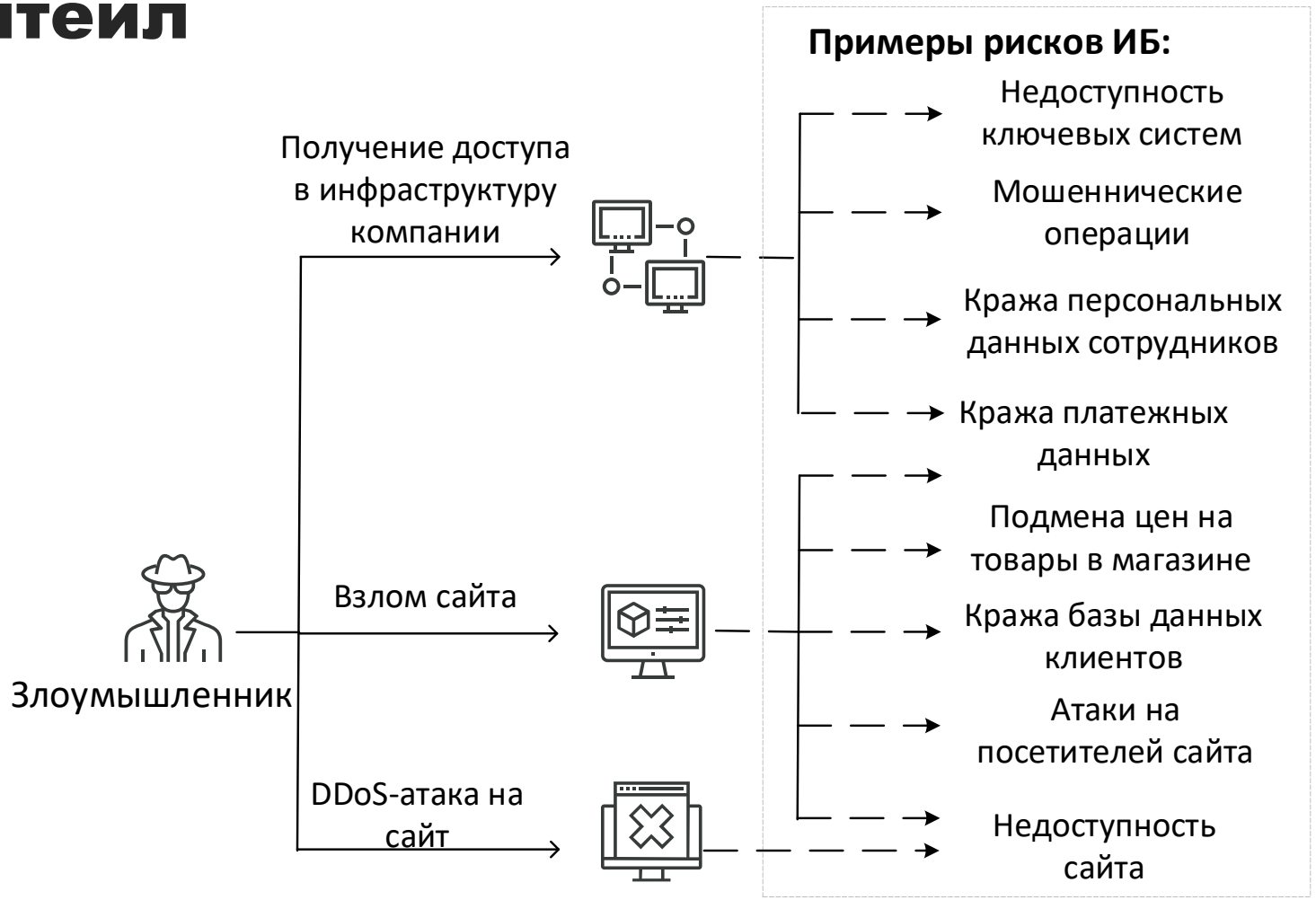
Обоснованность инвестиций
Инвестиции в ИБ соразмеримы с последствиями от недопустимых событий и учитывают текущее состояние и уровень развития ИБ

Недопустимые кибер-события: примеры

	Промышленность	Банки	Здравоохранение	ИТ	Гос. органы
Финансы	Искажение и утечка финансовой отчетности	Кражи денег со счетов и из банкоматов	Невозможность своевременной закупки специальных препаратов	Невозможность выплаты заработных плат	Неэффективное использование субсидий
Деятельность	Техногенные аварии с экологическим ущербом и угрозой жизни	Длительная недоступность банковских сервисов	Нарушение работы оборудования диагностики и жизнеобеспечения	Уничтожение всех операционных и резервных данных	Недоступность государственных услуг и сервисов
Конкуренция	Утечка НИР и планов развития	Утечка персональных и карточных данных	Утечка сведений о препаратах и их испытаниях	Утечка исходных кодов и планов развития ПО и сервисов	Утечка информации, ведущая к отставке первых лиц
Репутация	Шпионаж за первыми лицами	Кража данных о VIP-клиентах	Подмена медицинских данных пациентов (диагноз, лечение)	Взлом клиентов через уязвимости в продуктах и сервисах	Подмена отчетной информации и данных о показателях деятельности

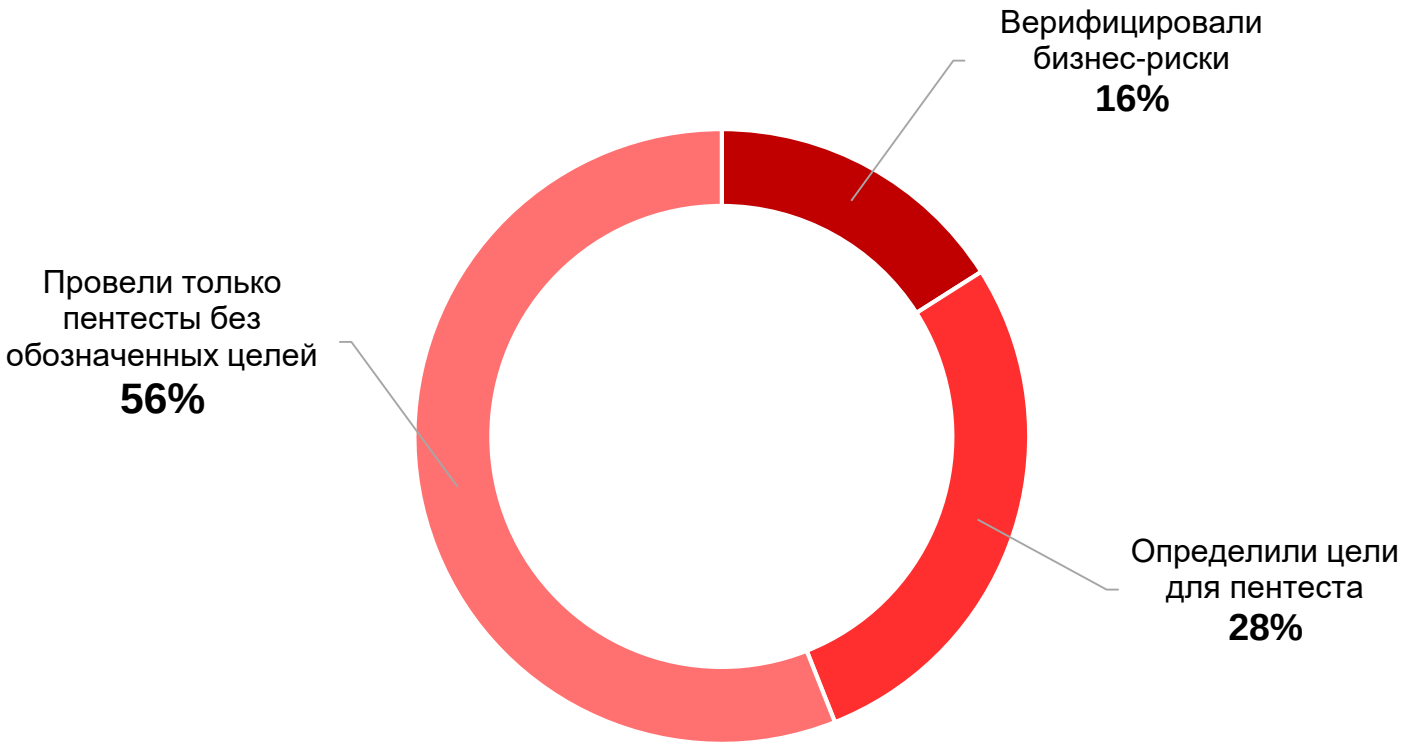
Пример реализации недопустимых событий

Ритейл



Упрощенная схема кибератаки

Типовой подход к оценке защищенности



Доля компаний, выполнявших работы по анализу защищенности и верификации рисков в 2019-2020 годы

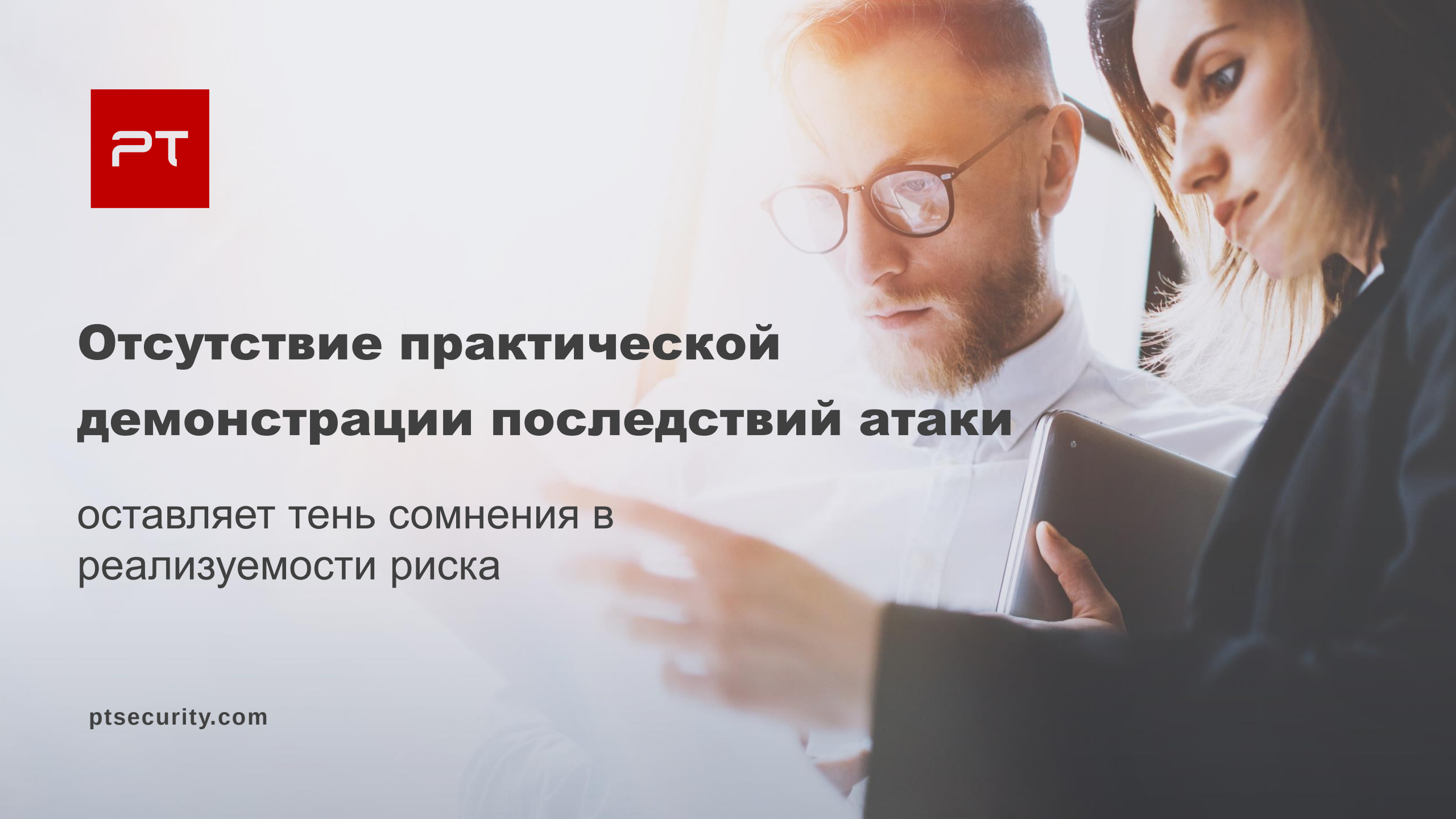
В 75% промышленных компаний злоумышленник может проникнуть в технологическую сеть

В каждом пятом банке возможно получить доступ к управлению банкоматами из внутренней сети

Типовой подход к оценке защищенности

Потенциальные риски:

- Остановка производства
- Вывод из строя промышленного оборудования
- Порча продукции
- Авария



Отсутствие практической демонстрации последствий атаки

оставляет тень сомнения в реализуемости риска

Контроль эффективности: Киберучения

The Standoff

Управление киберполигоном заказчика

Портал управления киберучениями
Портал управления скриптами-чекерами

Кастомизация и управление киберполигоном

Позволяет реконфигурировать полигон заказчика:
изменить количество сегментов,
изменить состав сервисов и сегментов

Мониторинг ИБ

Решения Positive Technologies: PT NAD, MaxPatrol SIEM,PT AF, PT MultiScanner
Решения других вендоров
Blue teams: ведущие команды из России, Европы, США

Инфраструктура The Standoff

Enterprise
Telecom
Bank
SCADA
Red teams:
ведущие пентестеры со всего мира,
участники bug bounty,
победители CTF,
исследователи промышленных систем

Доступ к мероприятиям Standoff

Подключение инфраструктуры заказчика к открытым и закрытым мероприятиям The Standoff

Канал для подключения к The Standoff

Киберполигон

RED TEAM

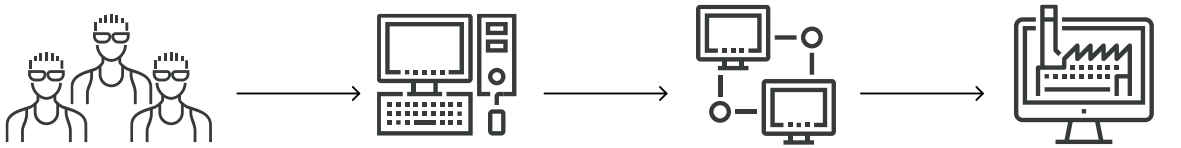
- ведущие пентестеры со всего мира,
- участники bug bounty,
- победители CTF,
- исследователи промышленных систем.

BLUE TEAM

- ведущие команды из России, Европы, США,
- собственная команда заказчика,
- заказчики, вендоры

Реализация рисков на The Standoff

Промышленность. Пример 1



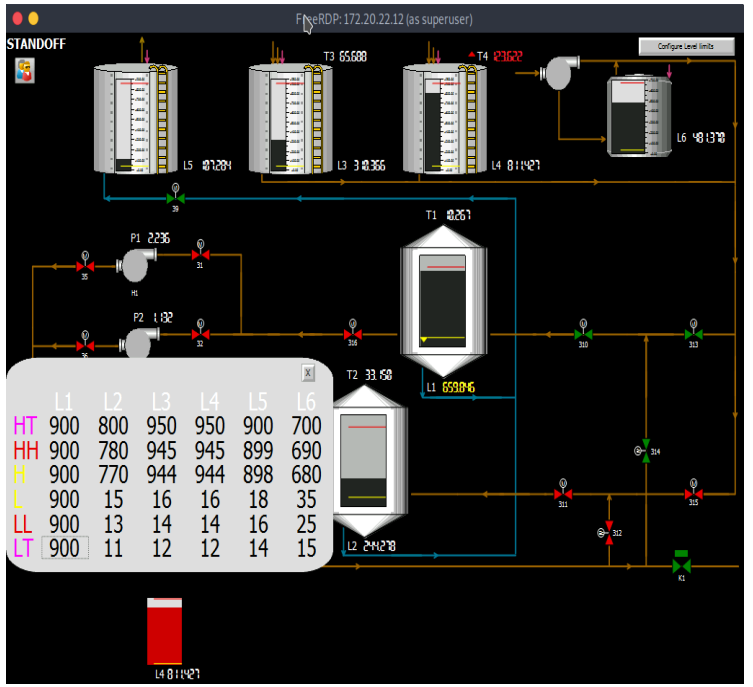
Реализованы риски ИБ

Нарушение технологического процесса. Переполнение нефтехранилища

Закрытие клапана на выкачку нефти

Остановка процесса транспортировки нефтепродуктов в нефтехранилища

Упрощенная схема сценария реализации рисков ИБ для нефтедобывающего предприятия в рамках The Standoff 2020



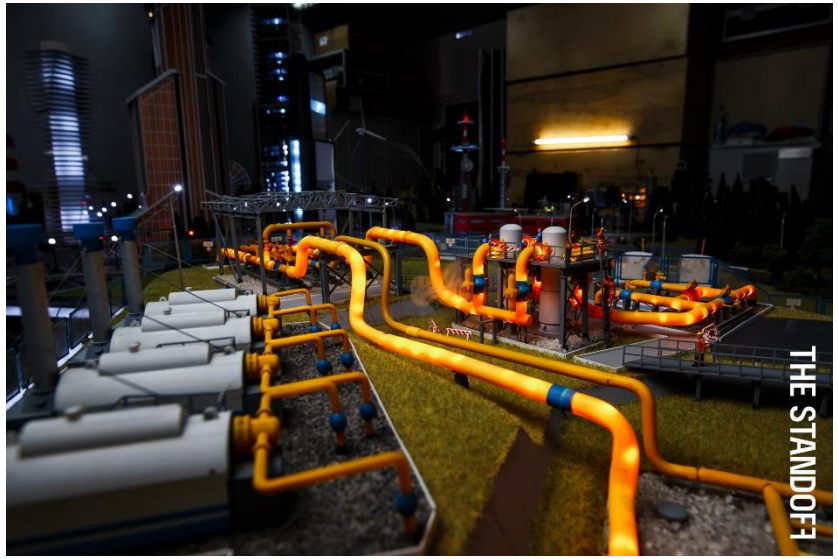
За несколько секунд до аварии

Реализация рисков на The Standoff

Промышленность. Пример 2

Реализованы риски ИБ

- **Нарушение технологического процесса. Остановка подачи газа**
- **Подмена данных о транспортировке газа**
- **Взрыв на газораспределительной станции**



Упрощенная схема сценария реализации рисков ИБ для газораспределительной станции в рамках The Standoff 2021

За несколько секунд до взрыва

4 шага к практической кибербезопасности

01 Выбрать отправную точку и способ кибер-трансформации

02 Обеспечить ресурсную, технологическую и методологическую базу

03 Реализовать основную фазу кибертрансформации и сформировать потенциал защиты

04 Выстроить процессы и цикл совершенствования системы кибербезопасности

Спасибо
за внимание!

ptsecurity.com