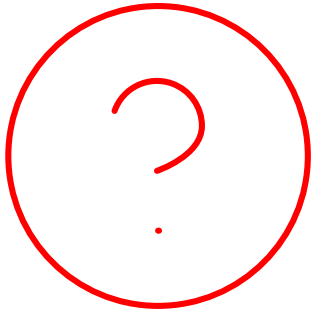
Игорь Протопопов

— Эксперт Центра Компетенций Positive Technologies

Результативная кибербезопасность

- Что делать в условиях парадигмы «всех уже давно взломали»?
- Для чего мы внедряем технические средства защиты?



- Как в результате получить не стопку бумаг, а реальную защиту?
- Чем измерить эффект от инвестиции в кибер-безопасность?

Вопрос не в том, взломают ли вопрос в том – готовы ли мы?

96%

компаний
не защищены
от внешних атак

От часа до пяти дней

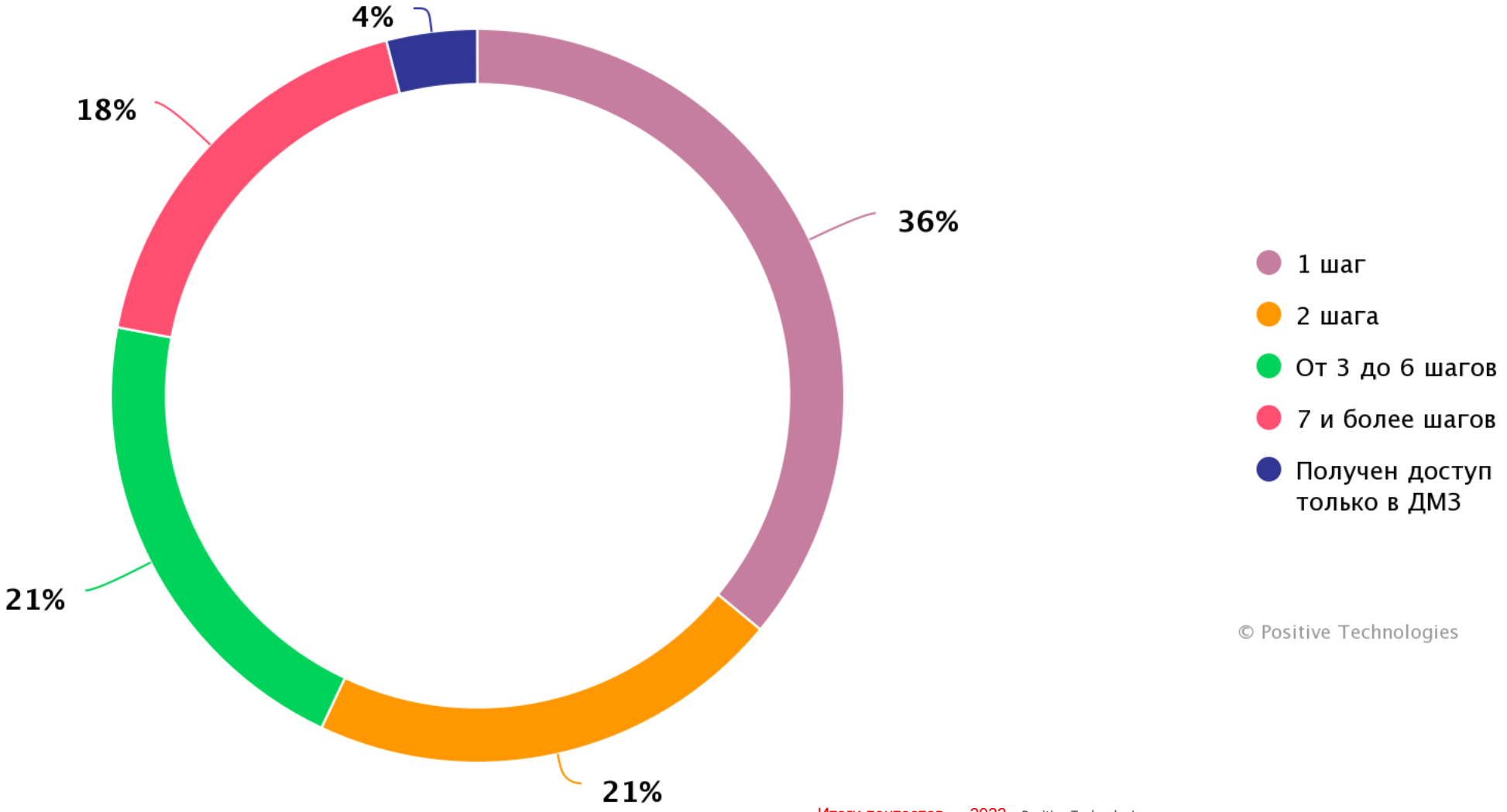
тратят злоумышленники
на проникновение
во внутреннюю сеть

В 100%

компаний инсайдер
может контролировать
инфраструктуру

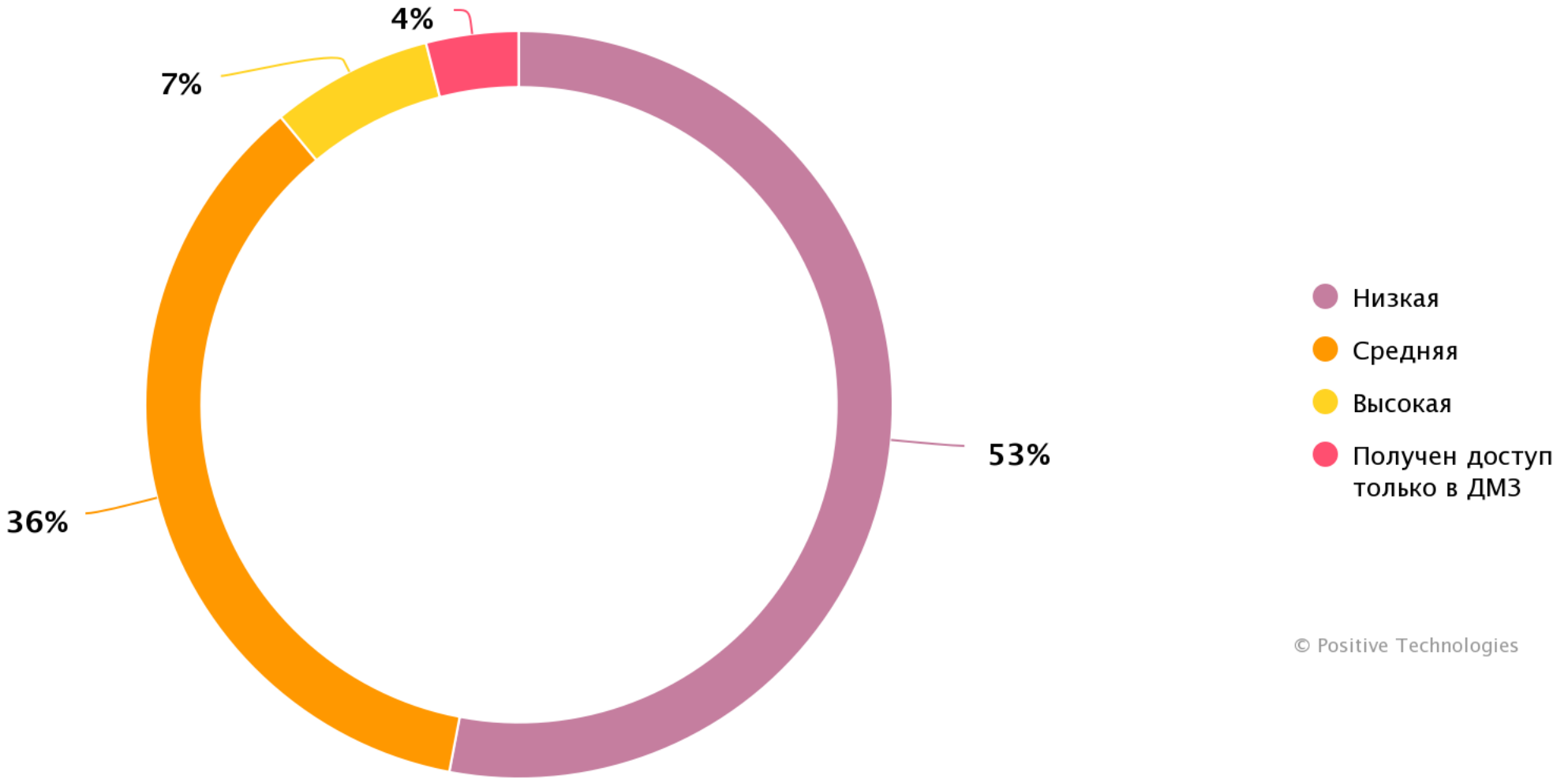
По данным исследования Positive Technologies «Итоги пентестов — 2022»

Минимальное число шагов для проникновения в локальную сеть



«Итоги пентестов — 2022», Positive Technologies

Минимальная сложность вектора проникновения во внутреннюю сеть



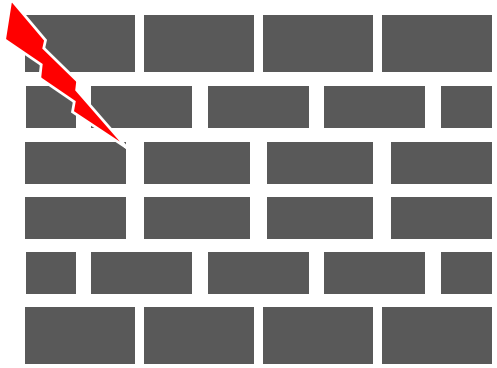
«Итоги пентестов — 2022», Positive Technologies

Цифровая трансформация:

Риск-ориентированный подход

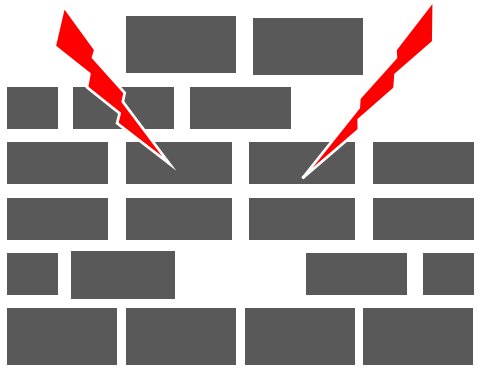
Вся наша жизнь — это выбор между допустимым, нежелательным и недопустимым

В пределах допустимого



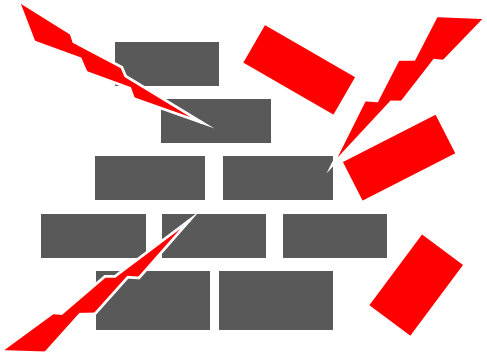
- Превысили скорость на 20 км/ч
- Получили ушиб от удара футбольным мячом
- Потратили 100 рублей на общественный туалет
- Наглотались соленой воды в море

Нежелательно



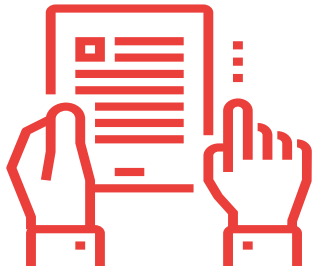
- Поцарапали автомобиль на стоянке
- Сломали ногу во время футбольного матча
- Потеряли кошелек с 10 тысячами рублей
- Поранились в воде о морского ежа

Недопустимо

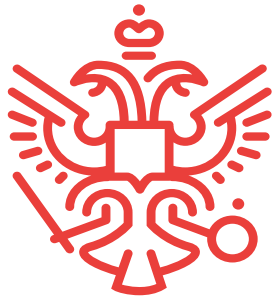


- Попали в ДТП со смертельным исходом
- Получили сотрясение мозга с необратимыми последствиями
- С вашего счета в банке украли все ваши сбережения
- Утонули

Это не новация: вы с этим уже сталкивались



Ключевые риски, описанные в анализе рисков и документах ЦБ



Негативные последствия, описанные в методике оценки угроз ФСТЭК

Ключевые элементы
результативной кибербезопасности

Недопустимые события

Выявляем, какие события действительно являются **недопустимыми** для компании, и проверяем их реализуемость на практике

Активное противодействие киберугрозам

Проектируем и трансформируем кибербезопасность, обеспечивая исключение недопустимых событий

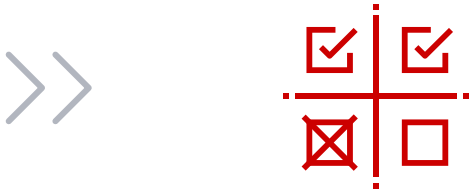
Проведение киберучений

Проверяем достижение результата и невозможность реализации недопустимых событий

Узнаем что недопустимо

ТОП-МЕНЕДЖМЕНТ

Знает, что действительно **недопустимо** для бизнеса



ПЕРЕЧЕНЬ

недопустимых для бизнеса событий

ОПЕРАЦИОННЫЕ РУКОВОДИТЕЛИ

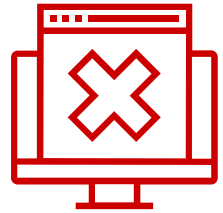
Помогут понять, как **недопустимое** может быть реализовано

СЦЕНАРИИ

реализации недопустимых событий

IT И ИБ-СПЕЦИАЛИСТЫ

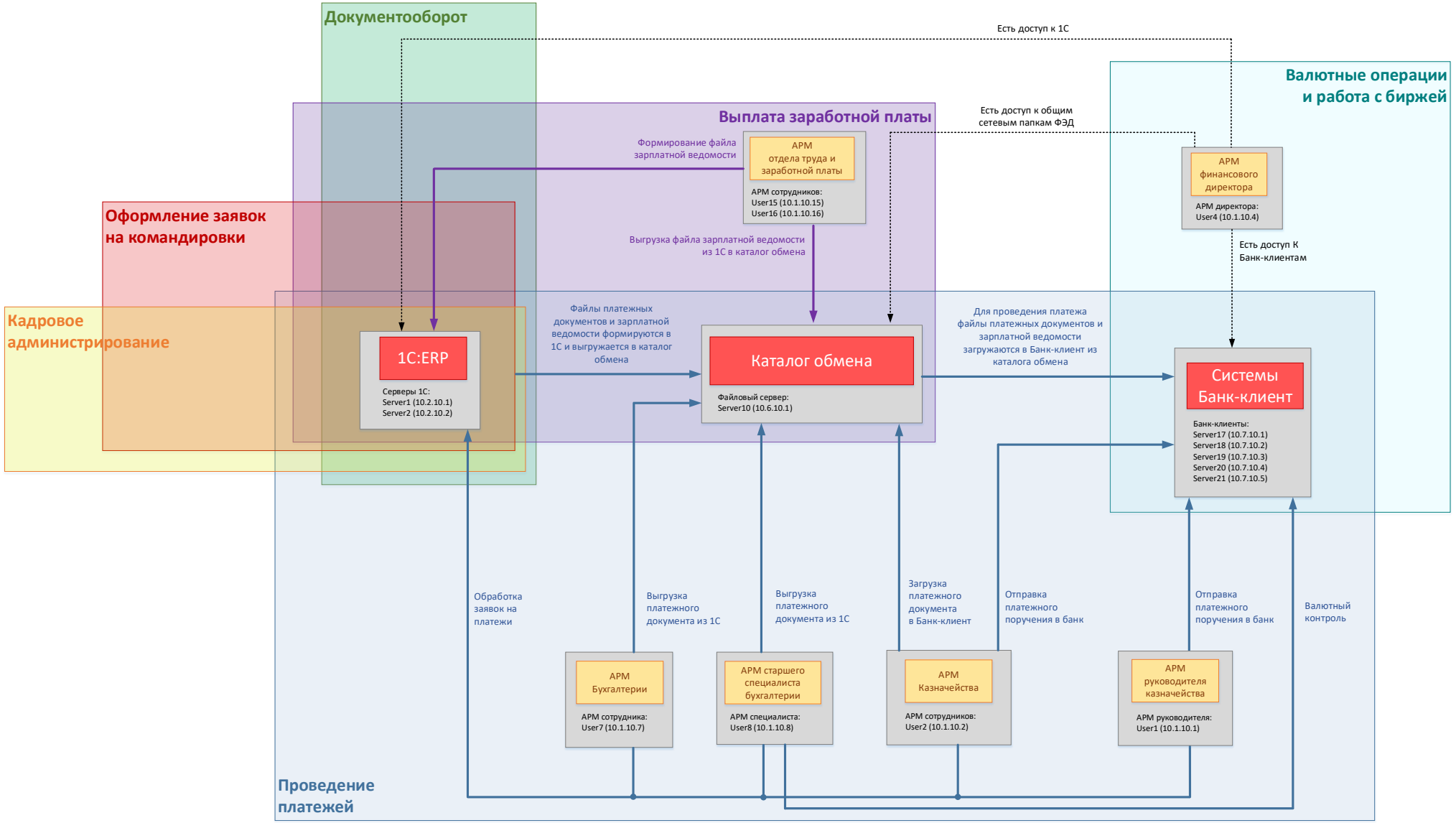
Помогут обозначить системы, на которых **недопустимое** может быть реализовано



СИСТЕМЫ

взлом которых повлечет недопустимое событие

Сценарии


Документооборот
Есть доступ к 1С
Валютные операции
и работа с биржей
Выплата заработной платы
Есть доступ к общим
сетевым папкам ФЭД
Формирование файла
зарплатной ведомости
АРМ
отдела труда и
заработной платы
АРМ сотрудников:
User15 (10.1.10.15)
User16 (10.1.10.16)
АРМ
финансового
директора
АРМ директора:
User4 (10.1.10.4)
Оформление заявок
на командировки
Выгрузка файла зарплатной ведомости
из 1С в каталог обмена
Есть доступ К
Банк-клиентам
Кадровое
администрирование
Файлы платежных
документов и зарплатной
ведомости формируются в
1С и выгружается в каталог
обмена
Для проведения платежа
файлы платежных документов и
зарплатной ведомости
загружаются в Банк-клиент из
каталога обмена
1С:ERP
Серверы 1С:
Server1 (10.2.10.1)
Server2 (10.2.10.2)
Каталог обмена
Файловый сервер:
Server10 (10.6.10.1)
Системы
Банк-клиент
Банк-клиенты:
Server17 (10.7.10.1)
Server18 (10.7.10.2)
Server19 (10.7.10.3)
Server20 (10.7.10.4)
Server21 (10.7.10.5)
Обработка
заявок на
платежи
Выгрузка
платежного
документа из 1С
Выгрузка
платежного
документа из 1С
Загрузка
платежного
документа
в Банк-клиент
Отправка
платежного
поручения в банк
Отправка
платежного
поручения в банк
Валютный
контроль
АРМ
Бухгалтерии
АРМ сотрудника:
User7 (10.1.10.7)
АРМ старшего
специалиста
бухгалтерии
АРМ специалиста:
User8 (10.1.10.8)
АРМ
Казначейства
АРМ сотрудников:
User2 (10.1.10.2)
АРМ
руководителя
казначейства
АРМ руководителя:
User1 (10.1.10.1)
Проведение
платежей

Целевые и ключевые системы

СЕТЬ 2

1C:ERP

Тестовый сервер 1с

Резервные копии 1с

СЕТЬ 7

БАНК-КЛИЕНТЫ

Контроллеры домена

СЕТЬ 6

КАТАЛОГ ОБМЕНА

Серверы Exchange

Контроллеры домена

Центр управления антивирусным ПО

СЕТЬ 1

Компьютеры бухгалтерии и казначейства

СЕТЬ 3

Компьютеры разработчиков и системных администраторов

СЕТЬ 4

Сервер системы мониторинга

СЕТЬ 5

Серверы виртуализации

Целевая система

Ключевая система

+ Сценарии

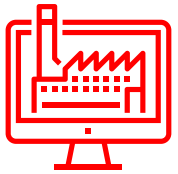
Целевой результат

РИСКОВЫЕ БИЗНЕС-ПРОЦЕССЫ

- Изолированы от других бизнес-процессов

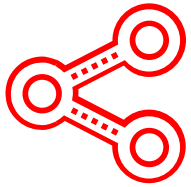
ТОЧКИ ПРОНИКНОВЕНИЯ

- Количество сведено к минимуму
- Безопасно настроены и усиленно мониторятся



ЦЕЛЕВЫЕ СИСТЕМЫ

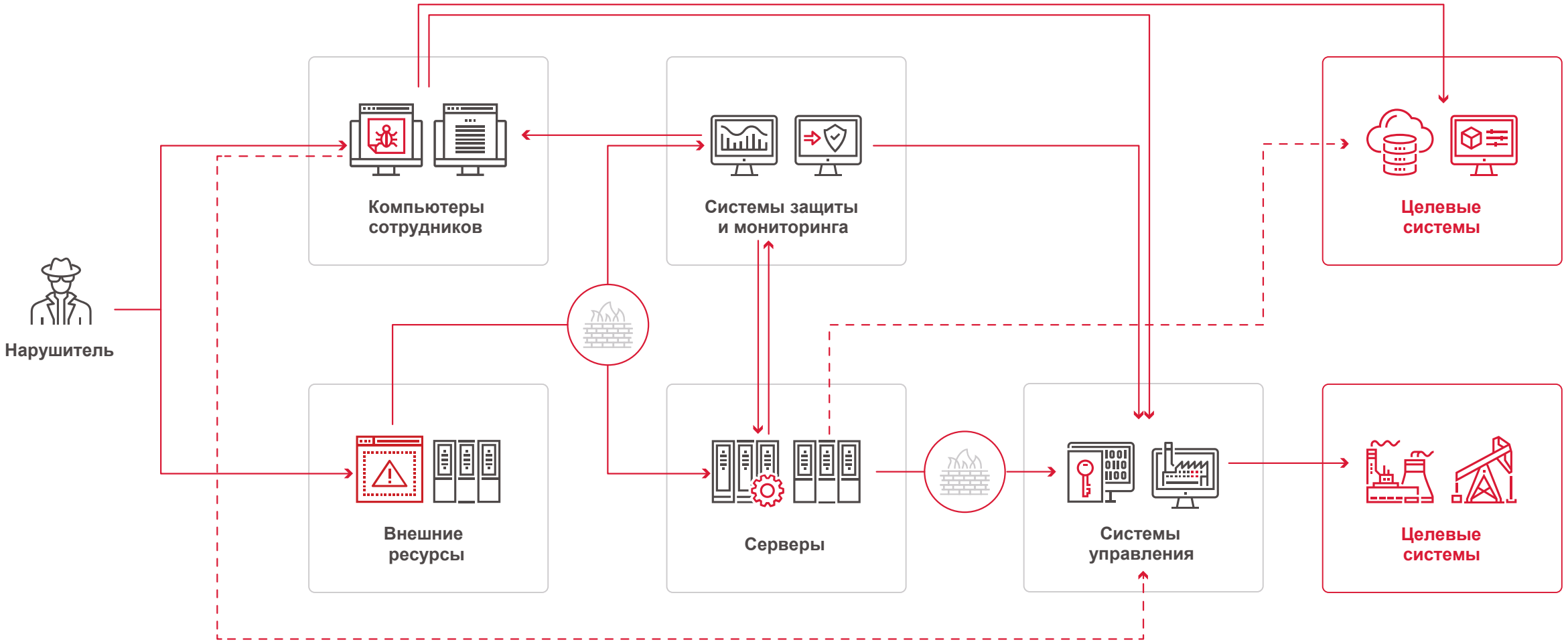
- Расположены в сетевых сегментах, максимально удаленных от точек проникновения
- Безопасно настроены и усиленно мониторятся



КЛЮЧЕВЫЕ СИСТЕМЫ

- Безопасно настроены и усиленно мониторятся

Верифицируем недопустимое



Преимущества подхода

Фокус на целевых и ключевых системах и их НС

Не размывается фокус киберзащиты, минимизируется влияние на инфраструктуру

Итерационный характер внедрения

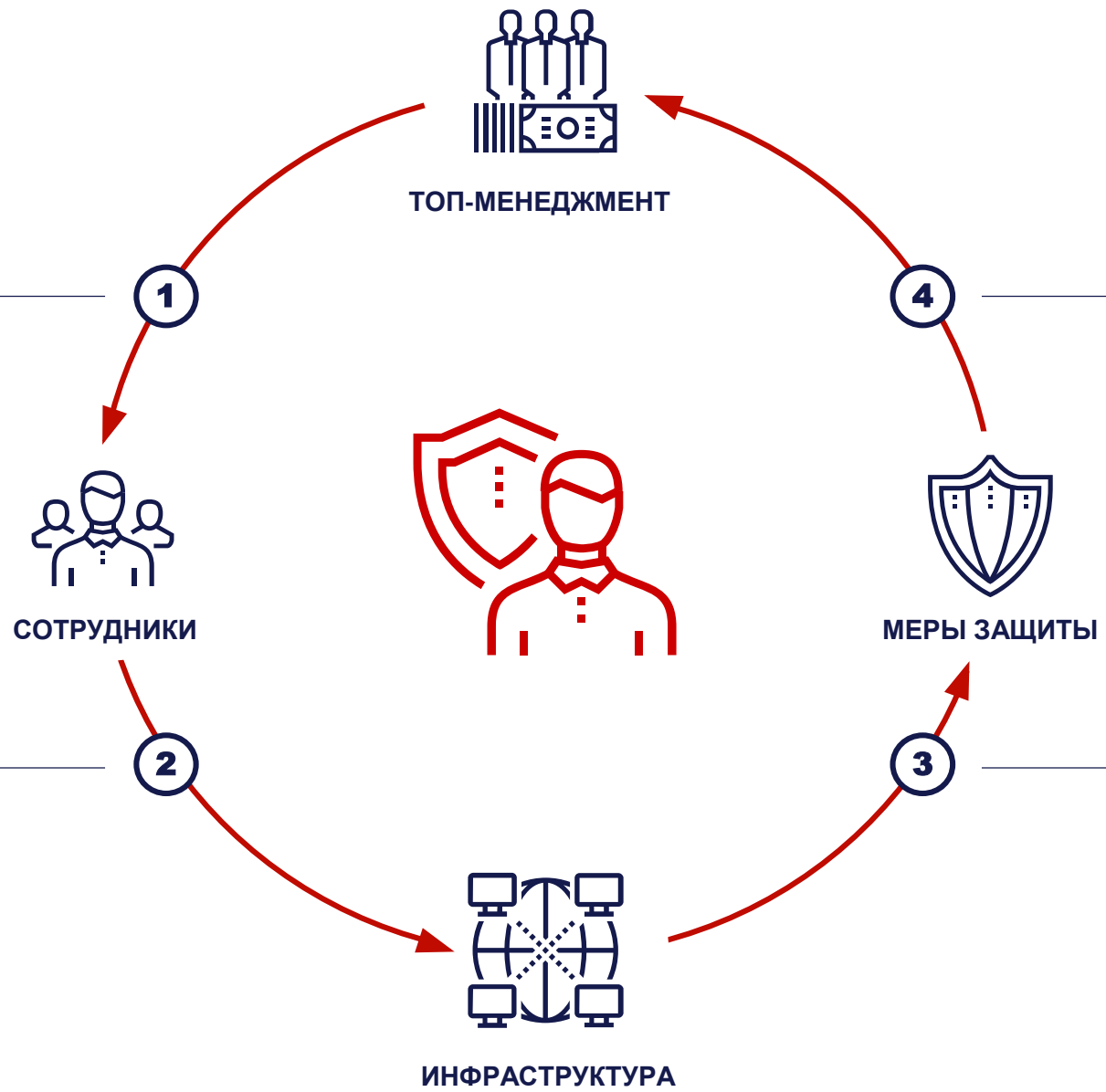
Учет изменений в инфраструктуре по ходу проекта

Эффект сразу

Результаты видны на начальном этапе и усиливаются по мере тиражирования

ПОДТВЕРЖДЕНИЕ РЕЗУЛЬТАТОВ НА КИБЕРУЧЕНИЯХ

Результативный подход к кибербезопасности



Технологии и автоматизация

Корпоративный сегмент

- **VM**
  Мониторинг уязвимостей, инвентаризация
- **SIEM**
  Мониторинг, сбор событий, реагирование
- **PT NAD**
  Выявление хакеров внутри сети
- **PT AF**
  Защита WEB ресурсов
- **Sandbox**
  Блокировка вредоносного ПО
- **XDR**
  Активное противодействие

Промышленный сегмент

- **VM/MP8**
  Мониторинг уязвимостей
- **SIEM**
  Мониторинг, сбор событий, реагирование
- **PT ISIM**
  Выявления аномалий в технологическом сегменте сети
- **Sandbox**
  Блокировка вредоносного ПО
- **XDR**
  Активное противодействие

Спасибо за внимание!

Дмитрий Жилин

Руководитель направления продаж в ЮФО, СКФО

dzhilin@ptsecurity.com

+7 (918) 558-93-05

Игорь Протопопов

Менеджер по продвижению продуктов

iprotopopov@ptsecurity.com

+7 (903) 453-21-11