POSITIVE TECHNOLOGIES

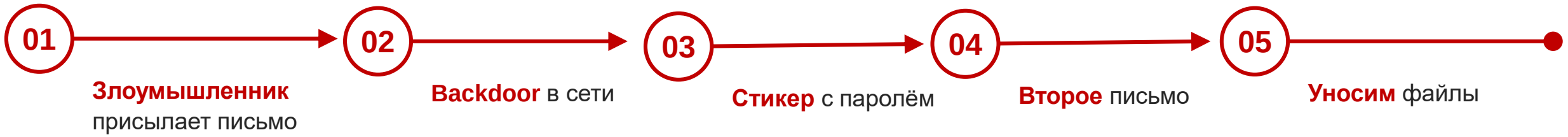
Ваша защита VS наши услуги

ptsecurity.com

Действие первое
камера наблюдения

ptsecurity.com

Банк


01
Злоумышленник присылает письмо
02
Backdoor в сети
03
Стикер с паролём
04
Второе письмо
05
Уносим файлы

Сервисы?
Зачем?

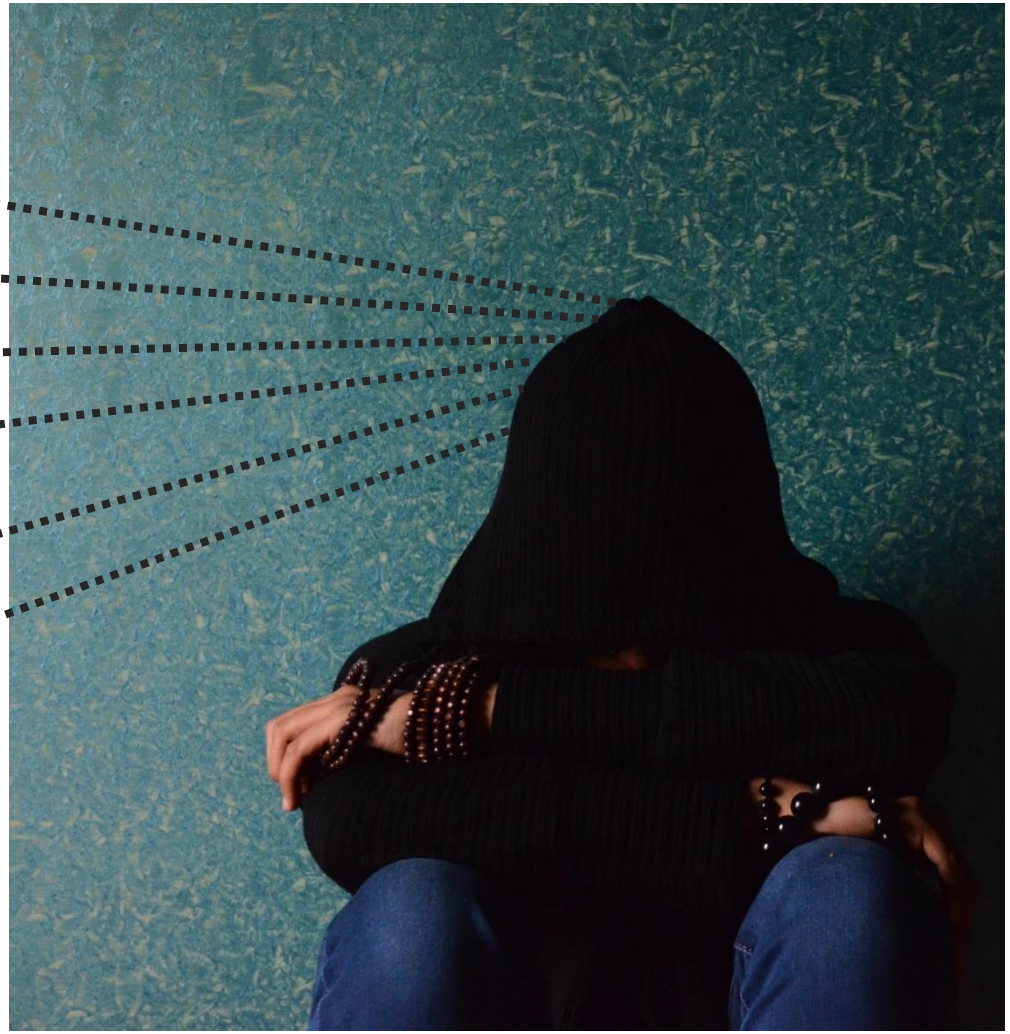
Ответить на вопрос: «Где я сейчас?»

А так же:

- На какой стадии находится ИБ в моей компании?
- Оценить эффективность принятых мер и внедренных средств защиты.
- Принять взвешенное стратегическое решение касательно дальнейшего развития.
- Обрести уверенность в завтрашнем ИБ.

Я беспокоюсь

- Сомнения
- Догадки
- Страхи
- Гипотезы
- Не ясно с чего начать
- Страх неизвестности

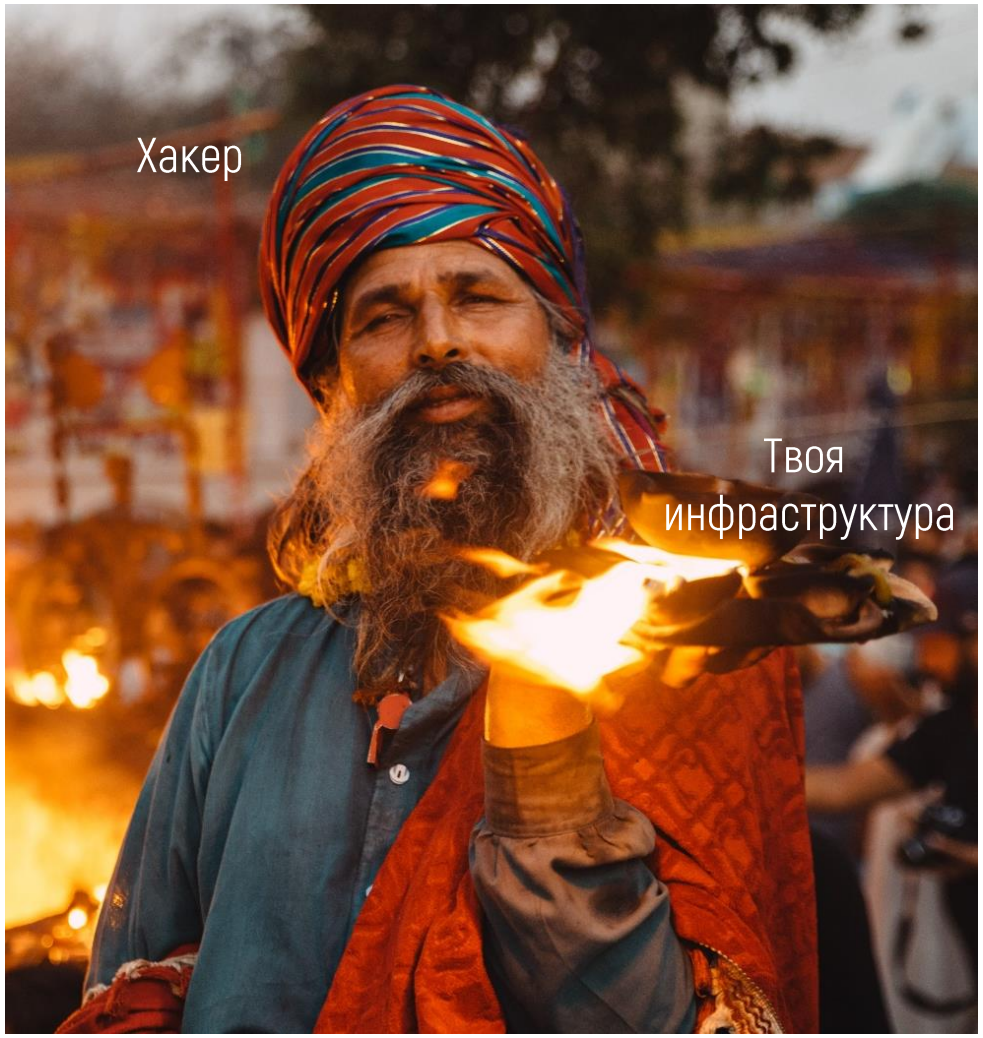


Меня ничего не беспокоит

Абсолютно любой хакер:
- Посмотри на свою инфраструктуру и на меня.
- А теперь снова на меня и на свою инфраструктуру, она в огне.

Тем временем ты:





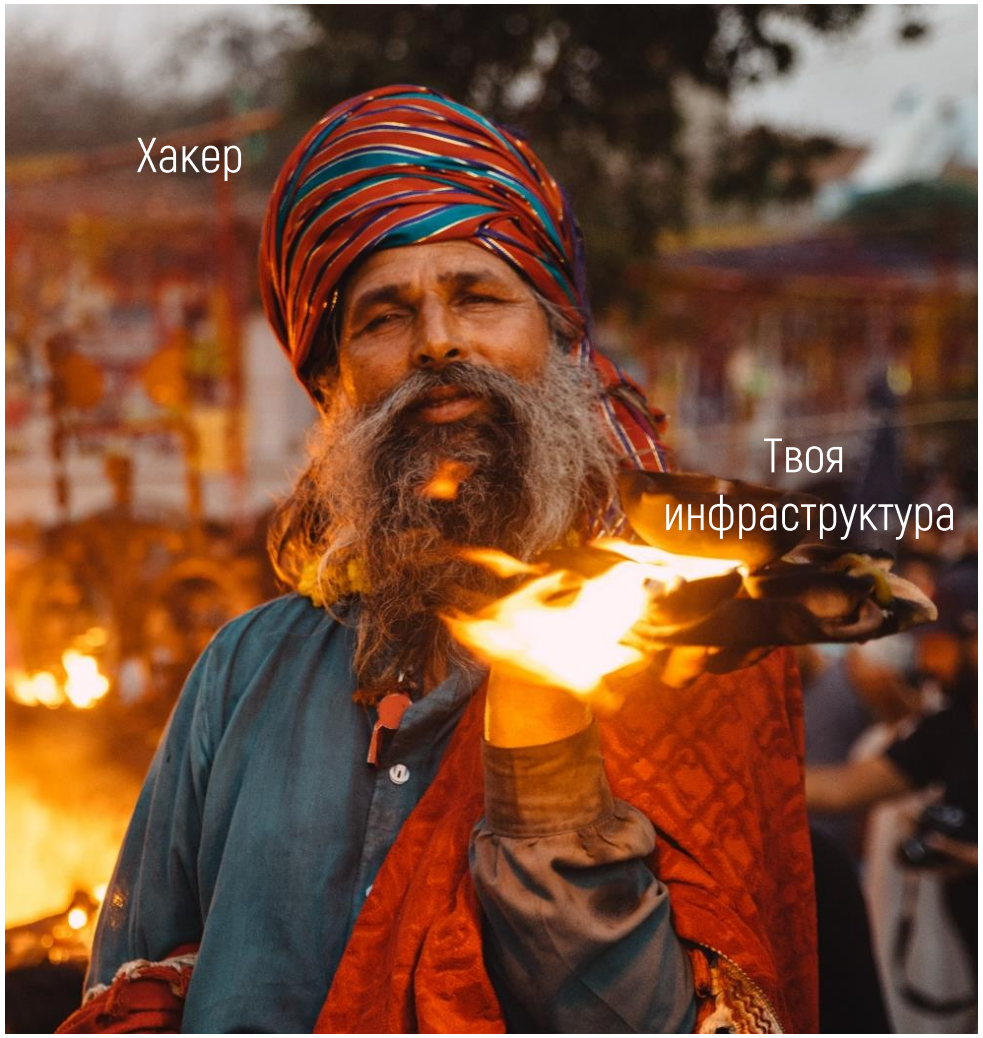
Меня ничего не беспокоит

Абсолютно любой хакер:
- Посмотри на свою инфраструктуру и на меня.
- А теперь снова на меня и на свою инфраструктуру, она в огне.

Тем временем ты:



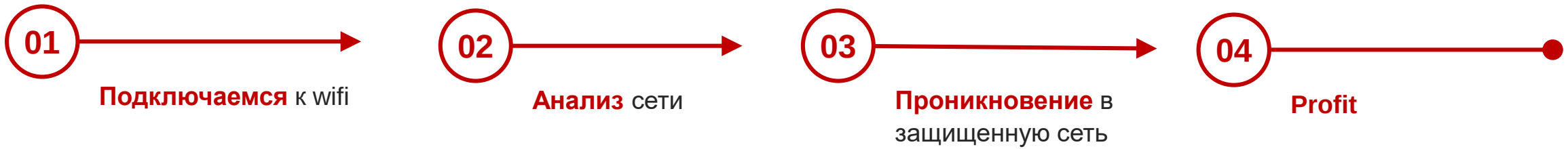
Хватит это терпеть!



Действие второе
wifi есть?

ptsecurity.com

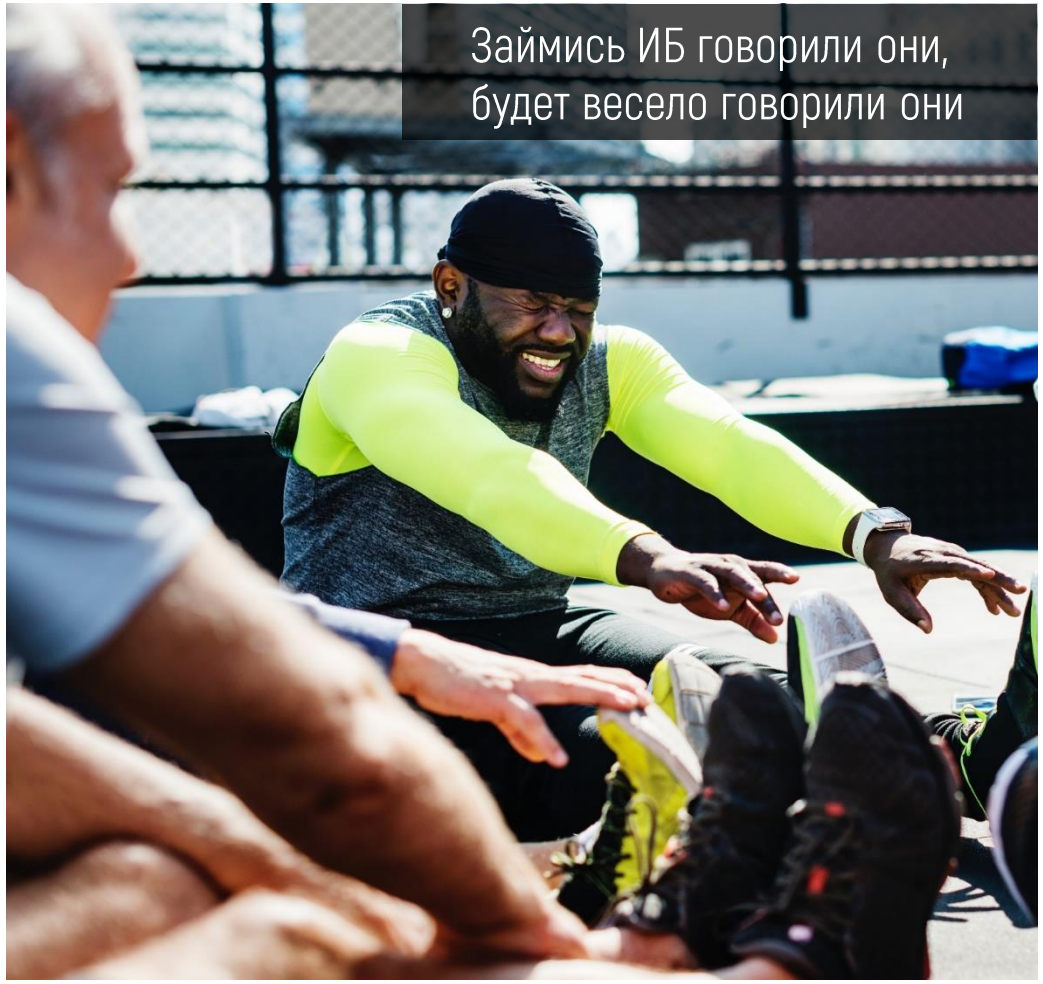
Отель Казино



С чего начать?
Классическая программа

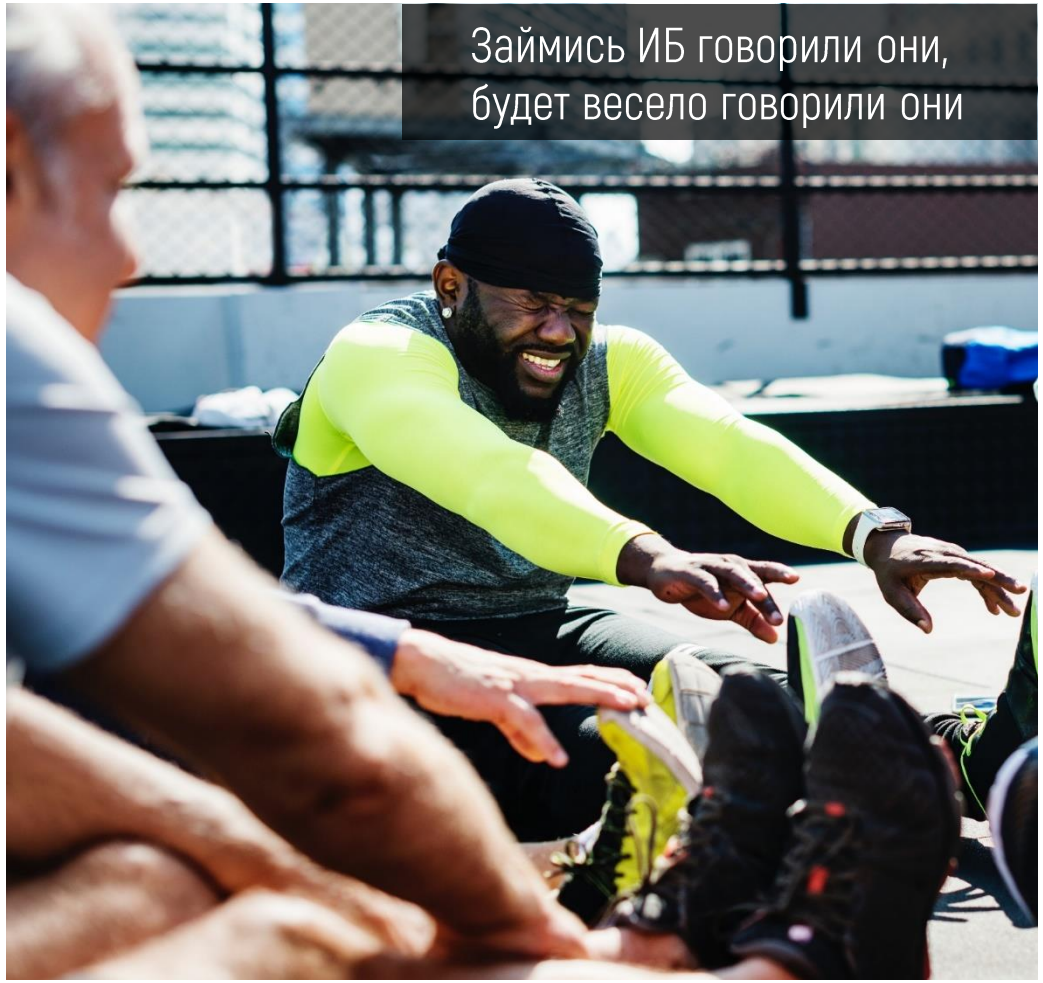
Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



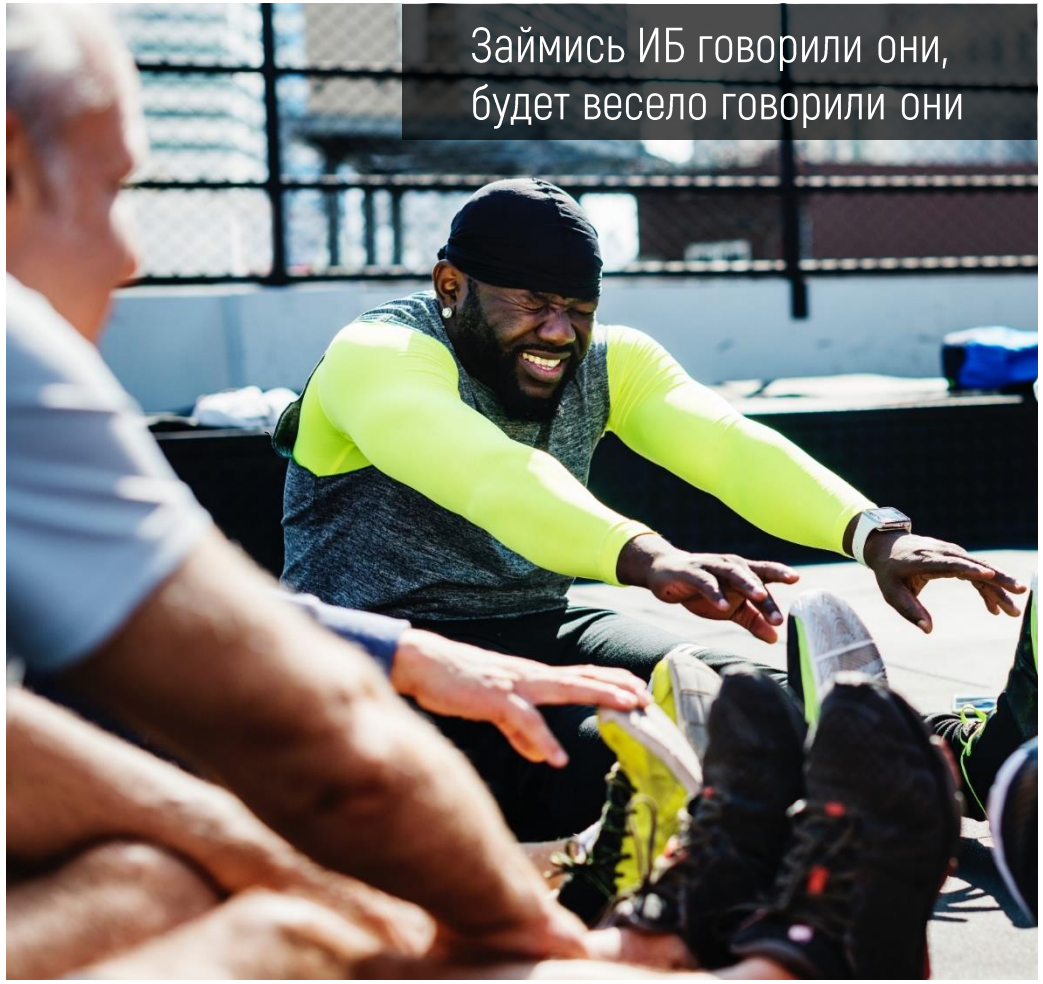
Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



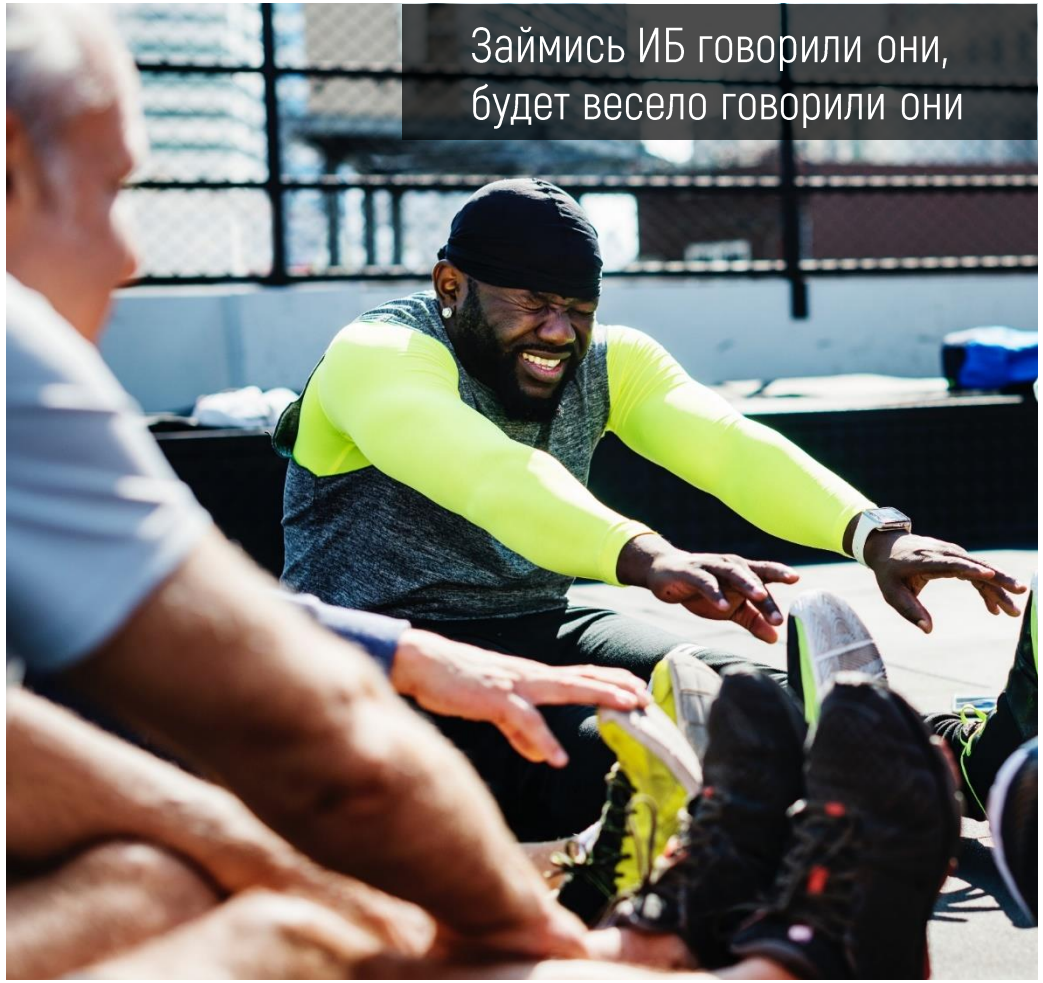
Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



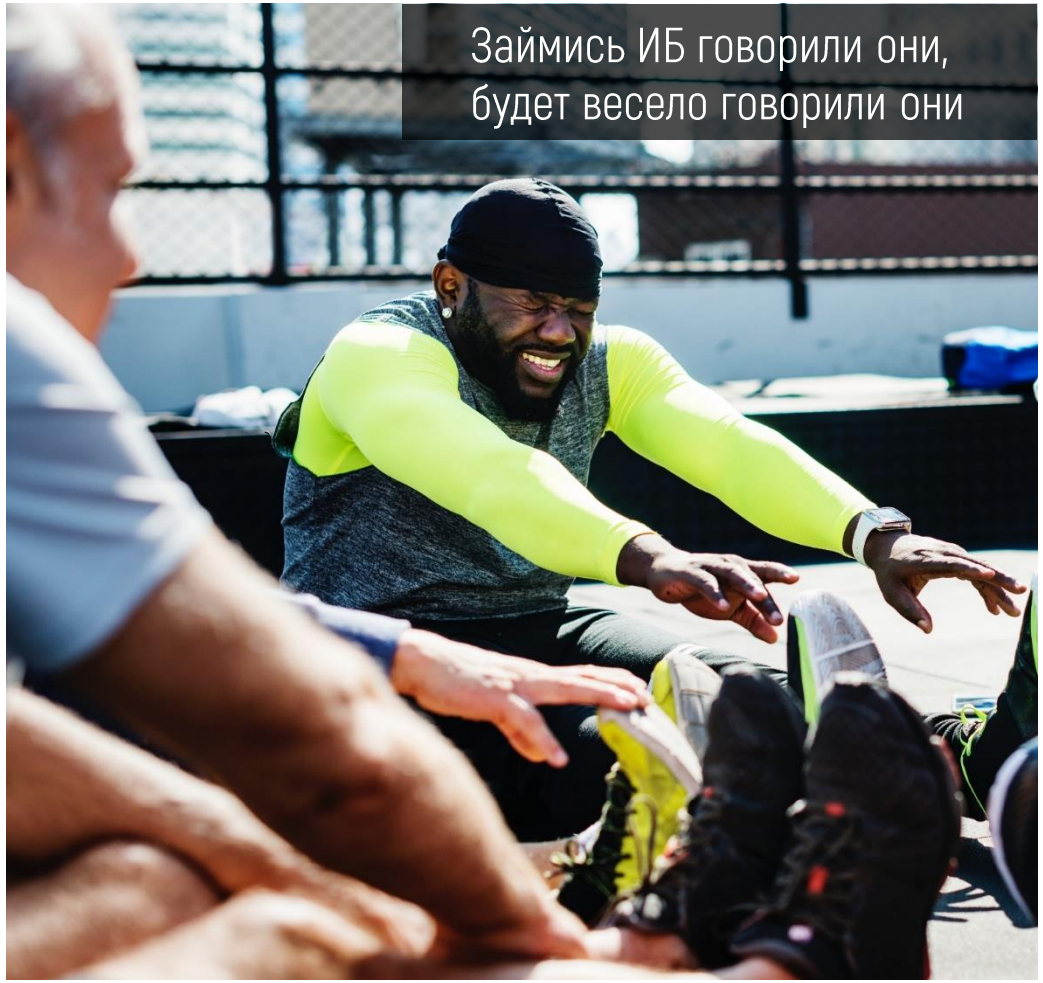
Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



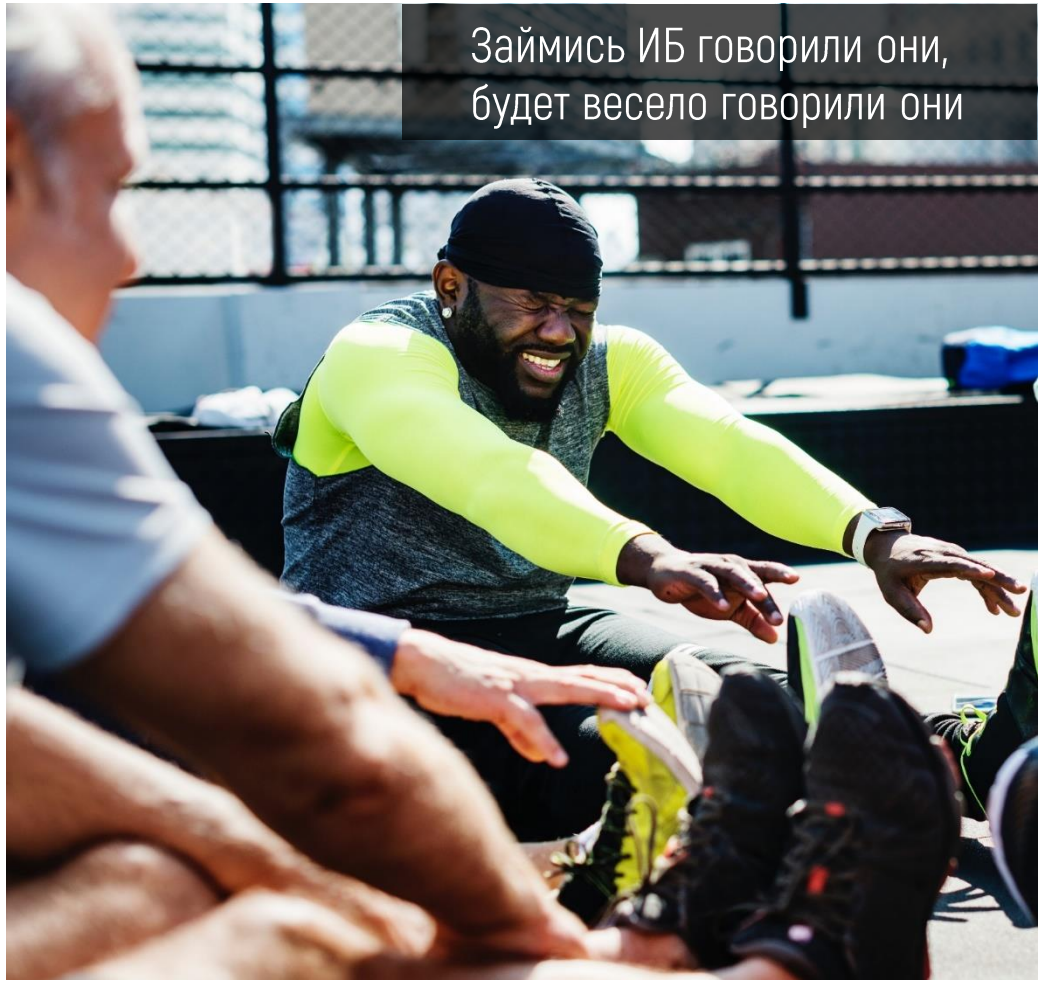
Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



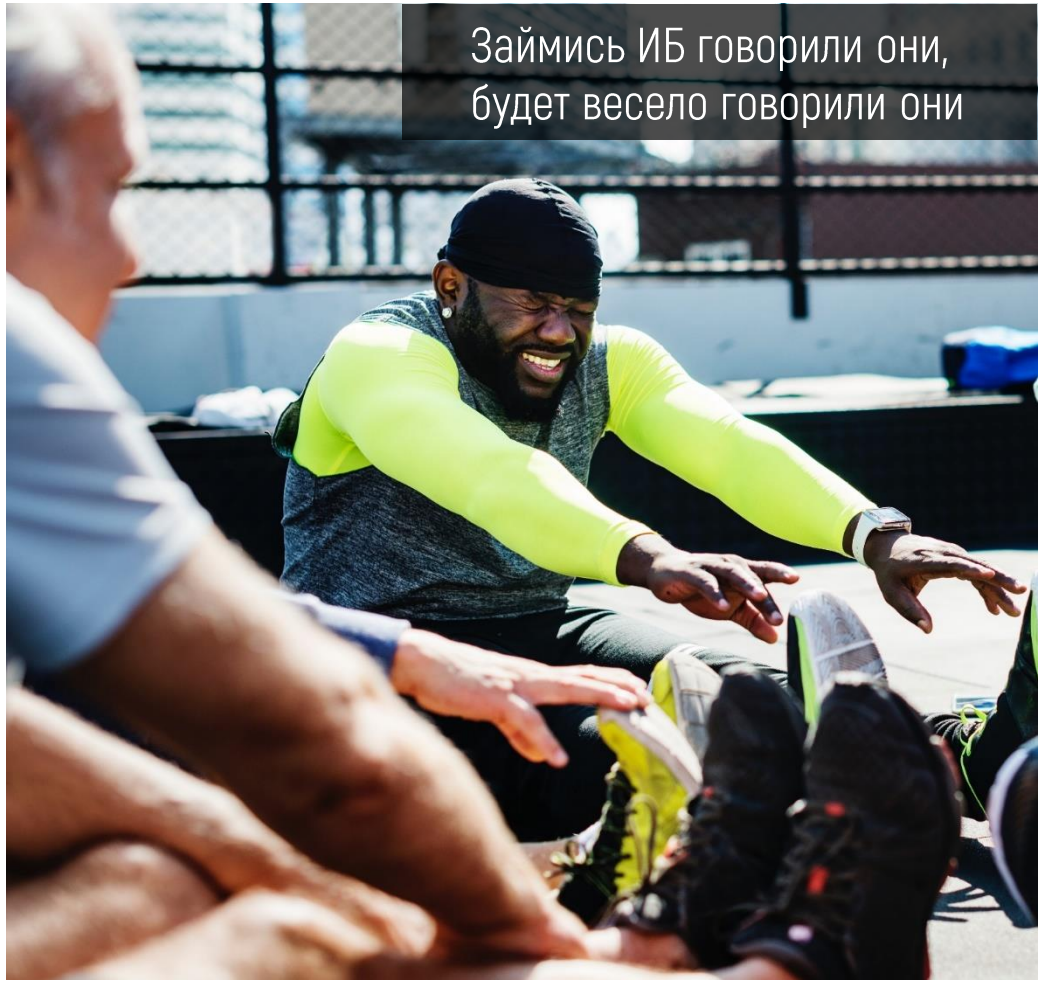
Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



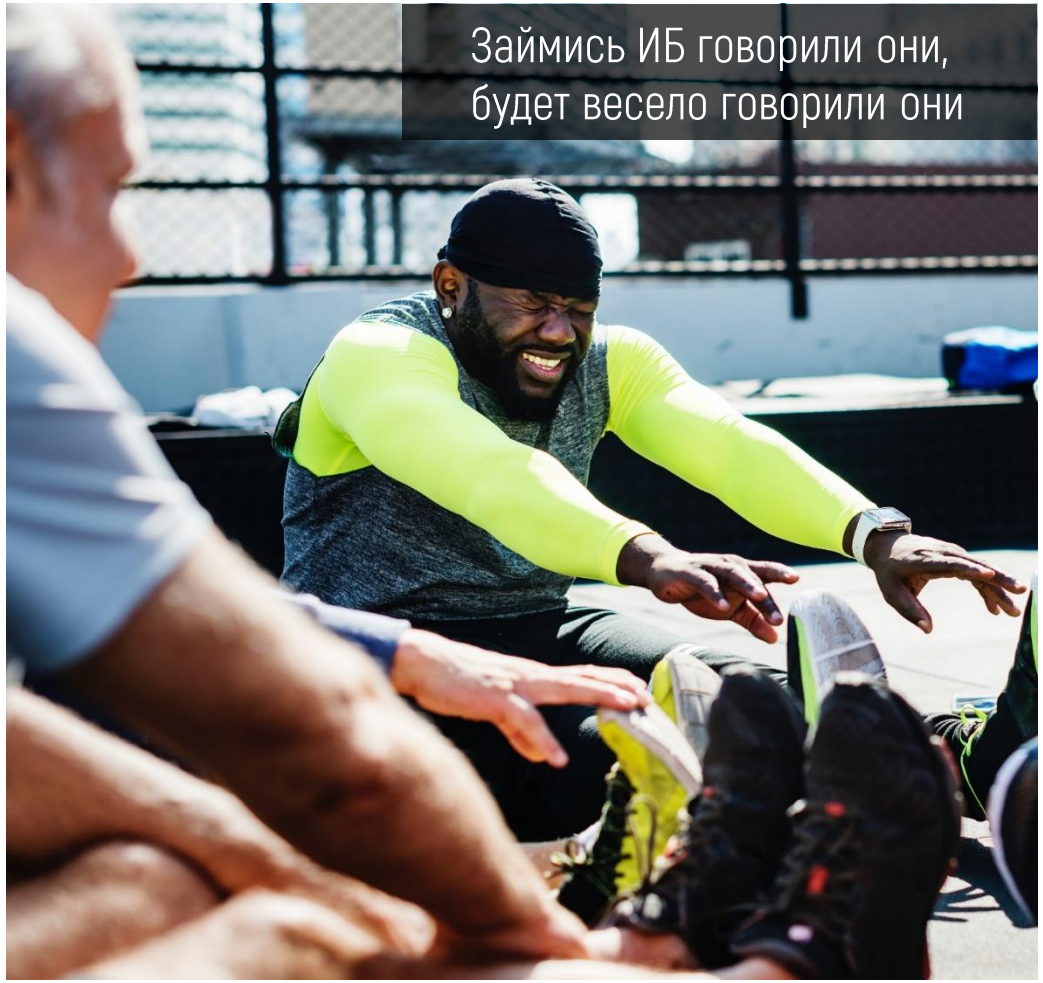
Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



Классическая программа

- Тесты на проникновение:
  - Внешний
  - Внутренний
- Оценка осведомленности сотрудников
- Анализ защищенности Wi-Fi
- Анализ приложений:
  - Веб
  - Мобильные
  - ERP-системы
- Анализ защищенности АСУ ТП
- Усиленный контроль периметра (АВС)
- Мониторинг и расследование инцидентов



Действие третье
Какой VPN?

ptsecurity.com

Транспортная компания

Чем продолжить?
Продвинутая программа

ptsecurity.com

Точечная ретроспектива

Этап 1. Тест на проникновение

Этап 2. Выявление попыток реализации найденных векторов атак

Этап 3. Глубокий анализ и расследование выявленных инцидентов:

- Выявление границ инцидента;
- Анализ артефактов и (или) выявление образца вредоносного программного обеспечения (ВПО), связанных с инцидентом;
- Формирование перечня потенциально зараженных узлов инфраструктуры.

Этап 4. Ранжирование выявленных инцидентов по уровню критичности:

- Классификация инцидента;
- Оценка уровня опасности инцидента;

Total Intelligence Service

- OSINT
- Поиск информации в dark web
- Таргетированный фишинг сотрудников

PT RvB

Сила RED и BLUE team в одном флаконе

Red Team

Этап 0. Разведка и планирование атаки
Этап 1. Проникновение в ЛВС
Этап 2. Закрепление в инфраструктуре
Этап 3. Достижение целей

Blue Team

1. Оценка эффективности мер реагировании команды ИБ Заказчика
2. Подготовка рекомендаций по модернизации средств защиты и мониторинга
3. Разработка рекомендаций по отражению реальных атак

ИБ 2.0

Верификация бизнес рисков

Этап 1. Уточнение перечня критичных бизнес рисков

Этап 2. Оценка возможности реализации рисков разными типами внешних злоумышленников

Этап 3. Идентификация и первичная оценка состояния защищенности внешнего периметра

Этап 4. Выявление взломанных узлов и фактов компрометации объектов инфраструктуры

Этап 5. Анализ эффективности реакции службы ИБ на возникшие инциденты

Этап 6. Разработка дорожной карты трансформации системы ИБ

ATR 365

Advanced Threat Realization 365

Pentest круглый год

- Имитация APT-атак
- Комплекс услуг по анализу защищенности периметра
- Эксплуатация уязвимостей
- Эмуляция последствий атак

24/7

- Без выходных
- Без перерывов на обед

Действие четвертое
Квадрокоптер

ptsecurity.com

Завод


01
Нашли wifi
02
Взяли квадрокоптер
03
Получили доступ
04
Вооруженная охрана
05
Грустим

Продолжим общение?

По вопросам стоимости:

Григорий Тимофеев
Руководитель направления продаж
+7 937 625 26 46