ИННОВАЦИОННЫЕ ПРОЕКТЫ ДЛЯ ОХРАННОЙ ОТРАСЛИ

Защита автоматизированных систем управления

Патент РФ № 152891

СИСТЕМА ЛОКАЛИЗАЦИИ ИСТОЧНИКА СЕТЕВОЙ АКТИВНОСТИ В ЛИНИЯХ ПЕРЕДАЧИ ДАННЫХ АСУ ТП

Актуальность защиты АСУ определяется ФЗ 187 РФ

Последствия нападений на АСУ

- Нарушение работоспособности ключевых систем на предприятии
- Технологические катастрофы
- Утечки данных

Известные мировые атаки на АСУ

Атака Stuxnet на ядерные объекты Ирана в 2010

Атака на объекты энергоснабжения в США в 2011

Атака на Сирийские государственные газовые и нефтяные компании в 2014

НАШЕ РЕШЕНИЕ

Сценарий защиты

PICS

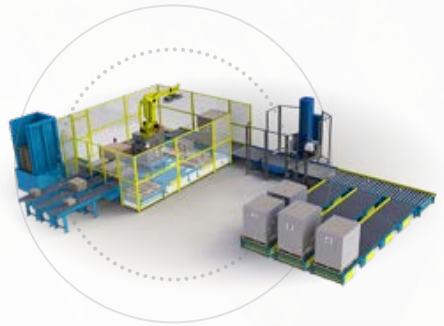
Вирусная атака

Вирус

Предупреждение

Блокировка

Логический контроллер



Предприятие

SCADA

ASAP- это уникальное запатентованное аппаратно-программное решение и первая **система предотвращения вторжений (ASAP)** для систем управления промышленными процессами, которая обнаруживает, предотвращает или блокирует вредоносное ПО в системах информационной инфраструктуры автоматического управления для различных производственных и технологических процессов:

Высший уровень
SCADA, MES

Средний уровень
PLC, HMI

Полевой уровень
Сенсоры, оборудование

ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

ГОТОВЫЙ БИЗНЕС

ПРИМЕНЕНИЕ

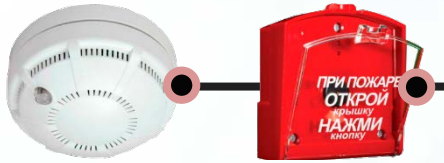
Системы пожаротушения

Системы защиты периметра

Охранные системы

Системы видеонаблюдения

Системы пожарной охраны



Поддержка:
- System sensor
- Аргус-Спектр
- Арсенал безопасности
- Артон
- ВЭРС и др.

Системы видеонаблюдения

Поддержка:
- ЧекТВ
- Линия
- Болид
- БайтЭрг и др.

Шлагбаумы

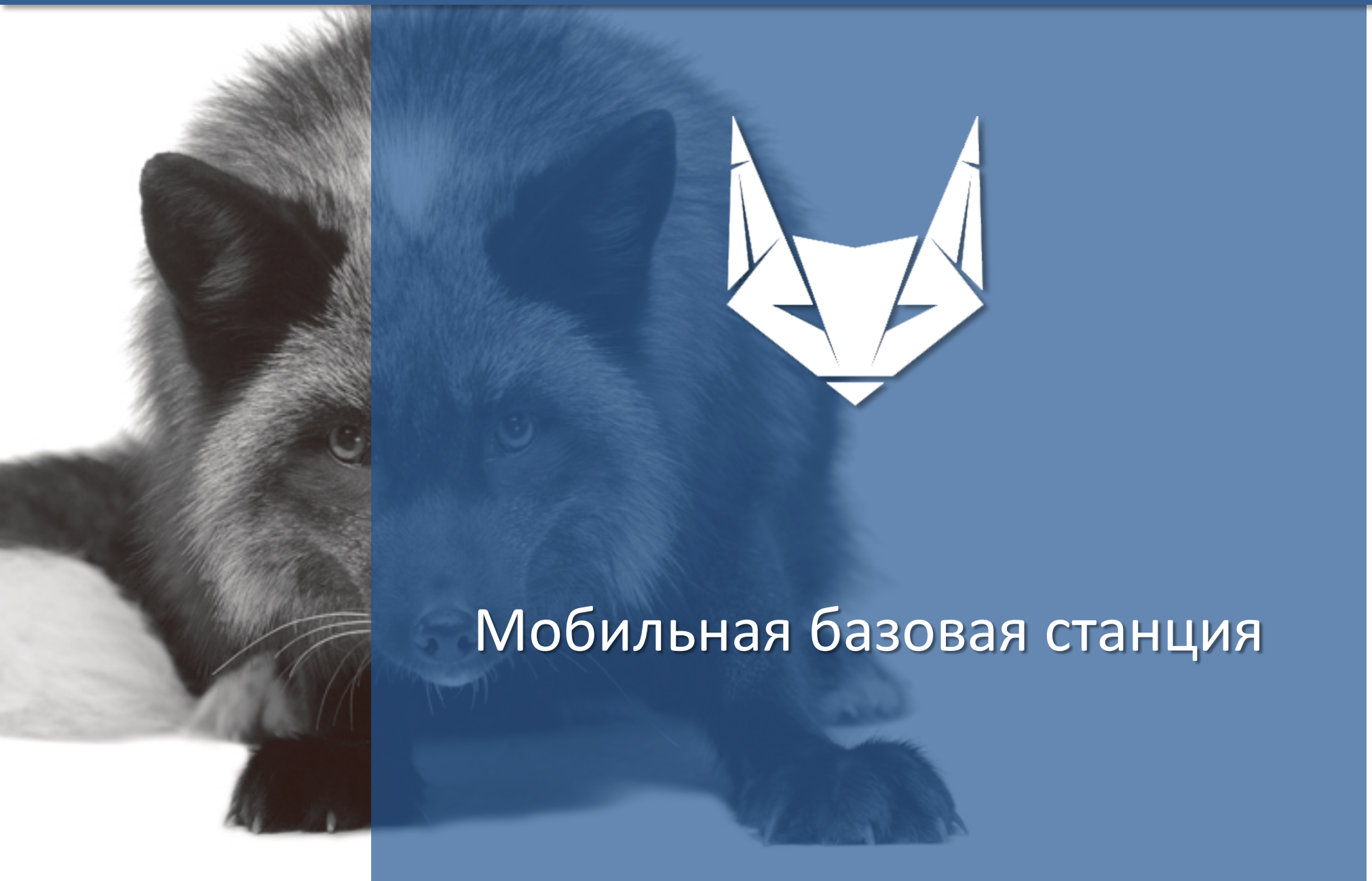
Поддержка:
- Gate
- Parsec
- Perco
- Болид и др

СКУД и турникеты

Поддержка:
- Aler
- IronLogic
- Промикс
- Эликс и др

КОМПЛЕКС ОБЕСПЕЧЕНИЯ КИБЕРФИЗИЧЕСКОЙ ЗАЩИТЫ

Информация о кибербезопасности объекта



Мобильная базовая станция

Способы внедрения

Промышленный корпус

Офисный корпус

Мобильный корпус

Мобильная базовая станция Black Fox

Black Fox - виртуальная мобильная базовая станция, которая позволяет создавать локальную сеть GSM со следующими функциональными возможностями:

- ★ Отслеживание мобильных телефонов в реальном времени в данном районе (IMSI, IMEI, активность)
- ★ Локальные вызовы и локальные текстовые сообщения на телефоны в данном районе
- ★ Локальные звонки между телефонами в данном районе без привязки к реальным мобильным операторам
- ★ Блокирование выборочных мобильных телефонов в данном районе согласно политике белого списка / черного списка

BLACK FOX

ГОТОВЫЙ БИЗНЕС

Предлагаемое решение для правительственных зданий: специальный лифт и категории этажей

АНТИ-ТЕРРОРИСТИЧЕСКАЯ БЕЗОПАСНОСТЬ

СЦЕНАРИЙ ЭВАКУАЦИИ

РАЗВЕРТЫВАНИЕ СВЯЗИ В ЗОНЕ БОЕВЫХ ДЕЙСТВИЙ ИЛИ В РАЙОНЕ КАТАСТРОФЫ

ЛАБОРАТОРНЫЙ ПРОТОТИП

AutoVisor

Новое поколение защиты автомобиля от кибернетических угроз

PATENTED

Патент США № US 8955130

СПОСОБ ЗАЩИТЫ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ ТРАНСПОРТНЫХ СРЕДСТВ ОТ ВТОРЖЕНИЙ

КАК ВАШЕ ТРАНСПОРТНОЕ СРЕДСТВО МОЖЕТ БЫТЬ АТАКОВАНО?

Методы проникновения вредоносного ПО в систему вашего автомобиля аналогичны тем, которые используются для обычных компьютеров

Беспроводное соединение

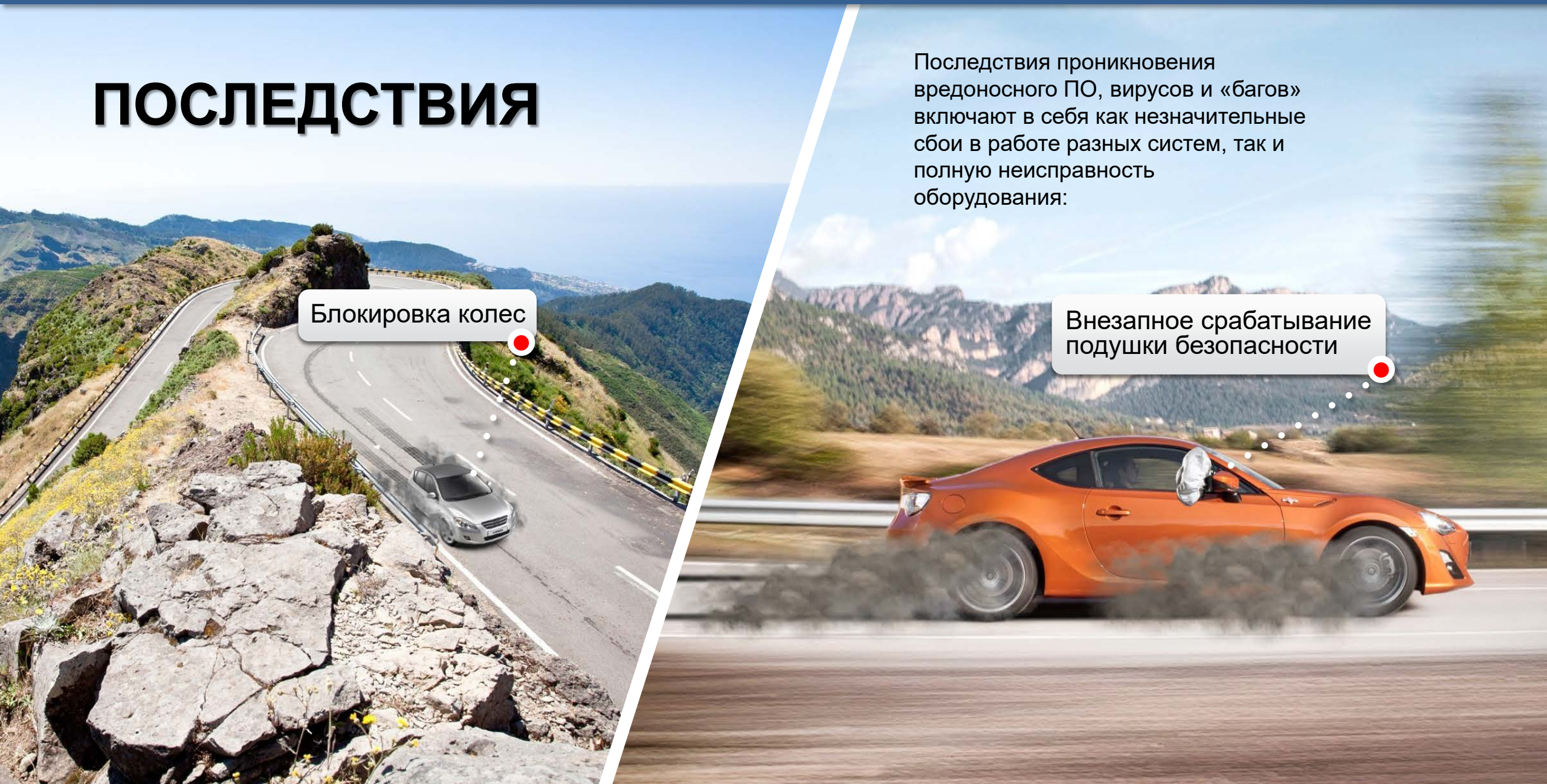
Системы устранения неполадок

Внешние носители данных

Воздействие при сервисном обслуживании

ПОСЛЕДСТВИЯ

Последствия проникновения вредоносного ПО, вирусов и «багов» включают в себя как незначительные сбои в работе разных систем, так и полную неисправность оборудования:



ПОСЛЕДСТВИЯ

AUTOVISOR

ЛАБОРАТОРНЫЙ ПРОТОТИП

AutoVisor обеспечивает максимальную защиту от неожиданных последствий атак на CAN-шину автомобиля

AutoVisor - единственный инструмент, который позволяет владельцу автомобиля самостоятельно контролировать параметры его работы. Он также обеспечивает автоматическую блокировку угроз.

01 Не имеет аналогов в мире

02 Установка в сервисном центре занимает не более 2 часов

03 Вся информация о функционировании защитной системы доступна в мобильном приложении (iOS, Android)

КИБЕРБЕЗОПАСНОСТЬ

ТЕКУЩИЕ ПРОБЛЕМЫ

Актуальные угрозы для мобильных устройств и пользователей

Несанкционированное прослушивание разговоров по мобильному телефону

Несанкционированное включение микрофона и камеры устройства для передачи данных злоумышленникам

Доступ посторонних лиц к файлам с деловой информацией

Определение местоположения человека по мобильному устройству

НАШЕ РЕШЕНИЕ

Устройство для защиты от прослушивания Green Head

Защита от прослушивания

Защита от утечки данных

Особенности

Обнаружение несанкционированной активации мобильного устройства и камеры с микрофоном

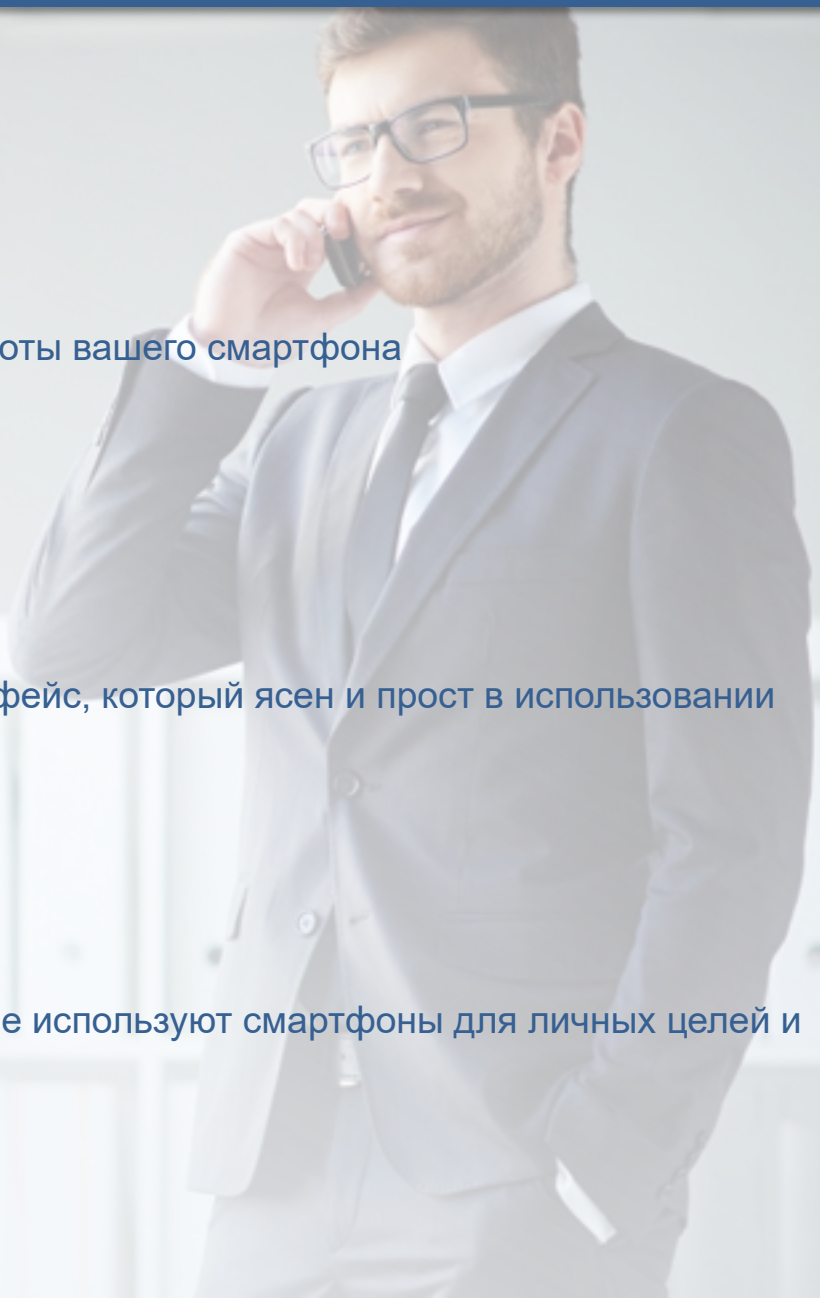
Виджет по одному нажатию блокирует камеру, микрофон и выключает беспроводные коммуникации: Wi-Fi, BT, NFC, мобильный интернет, которые могут стать каналами утечки информации.

Это приложение позволяет записывать разговор в режиме онлайн для последующего воспроизведения

Виджет на экране мобильного устройства уведомляет пользователя о несанкционированном прослушивании

Для ОС Android

ПРЕИМУЩЕСТВА



ВЫСОКАЯ СКОРОСТЬ

Green Head не влияет на скорость работы вашего смартфона

ПРОСТ В ИСПОЛЬЗОВАНИИ

Green Head имеет интуитивный интерфейс, который ясен и прост в использовании

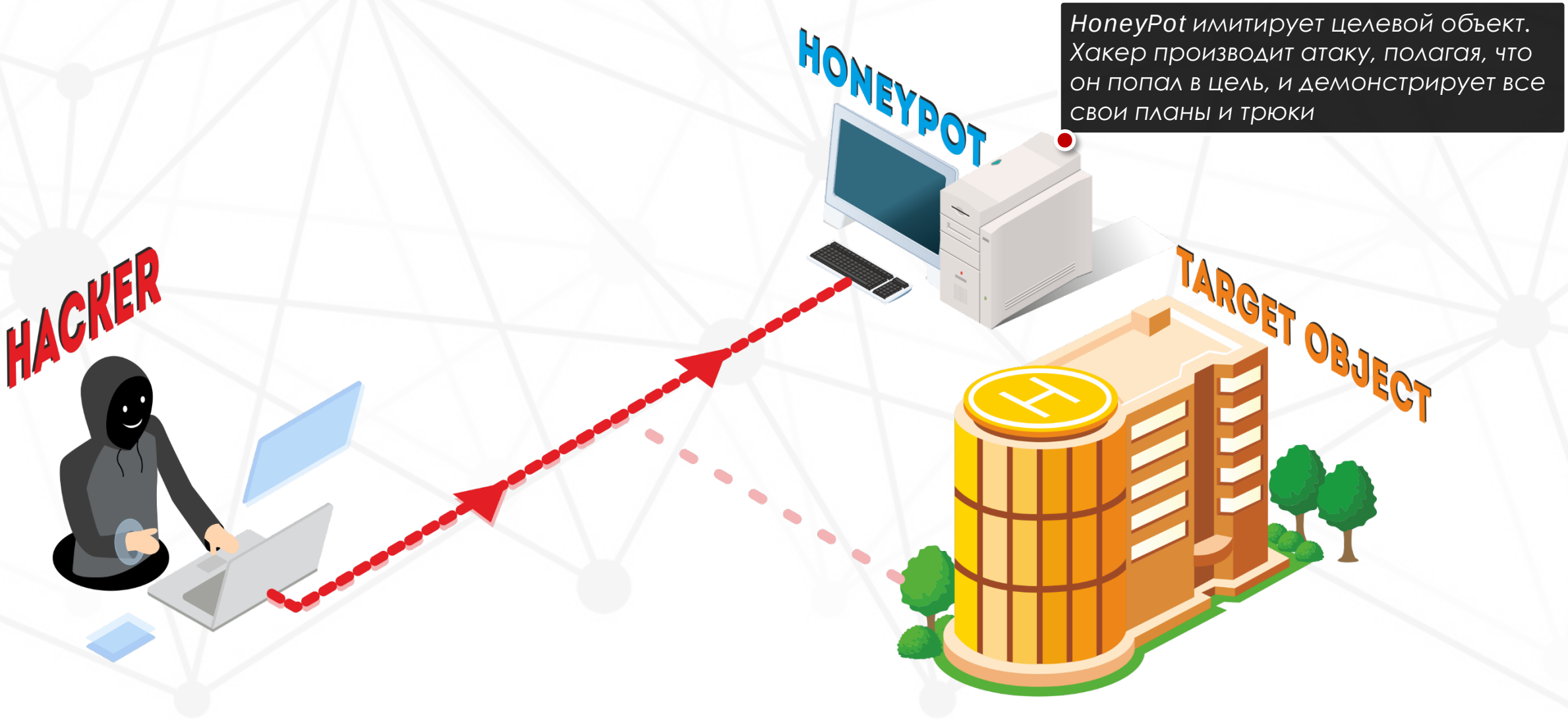
МНОГОФУНКЦИОНАЛЬНОСТЬ

Green Head удобен для людей, которые используют смартфоны для личных целей и для работы

HONEYPOT

эмуляция существующей производственной или телекоммуникационной критической системы инфраструктуры на простом сервере

ПРИНЦИП ФУНКЦИОНИРОВАНИЯ



HoneyPot имитирует целевой объект. Хакер производит атаку, полагая, что он попал в цель, и демонстрирует все свои планы и трюки

HONEYPOT

это механизм компьютерной безопасности, установленный для обнаружения, отклонения и противодействия попыткам несанкционированного использования информационной системы.

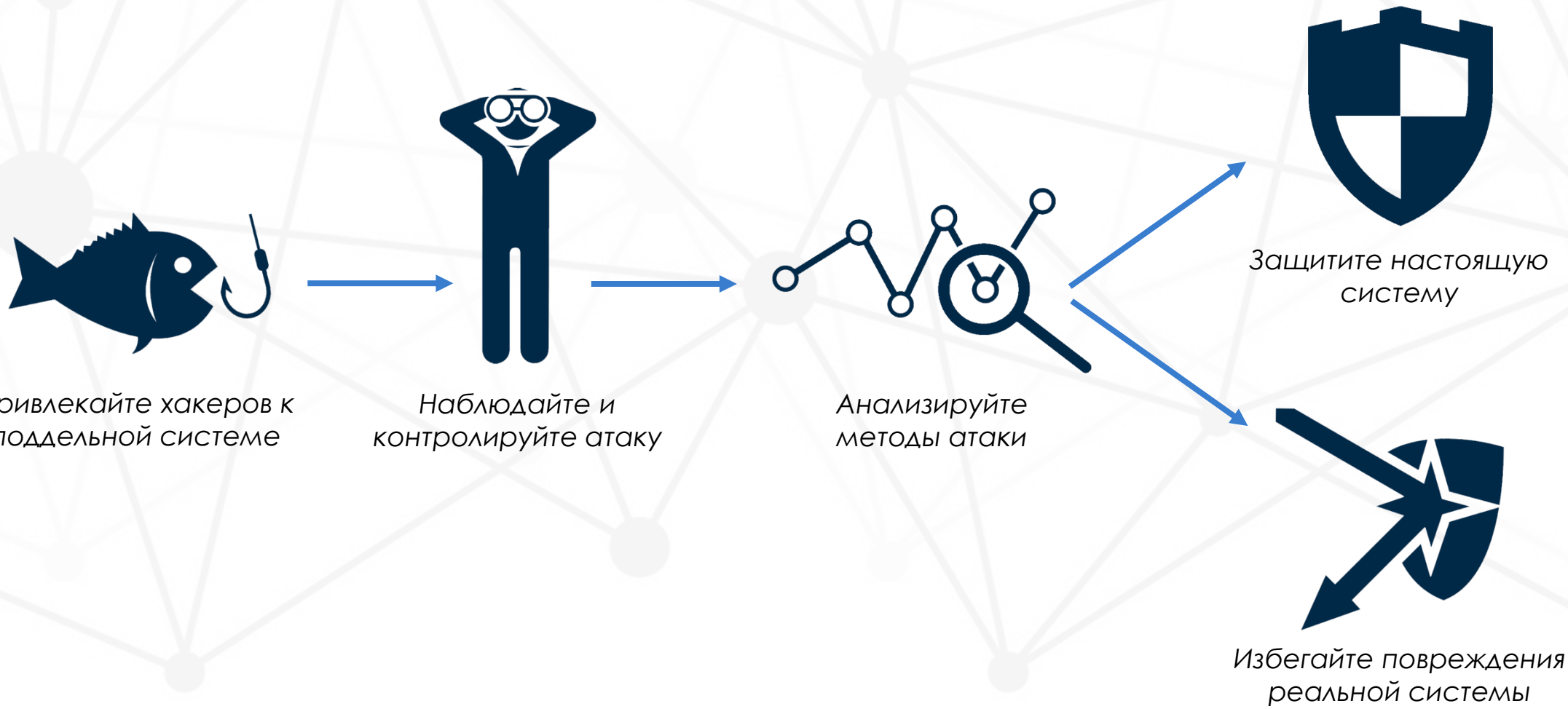
ВИДЫ HONEYPOT

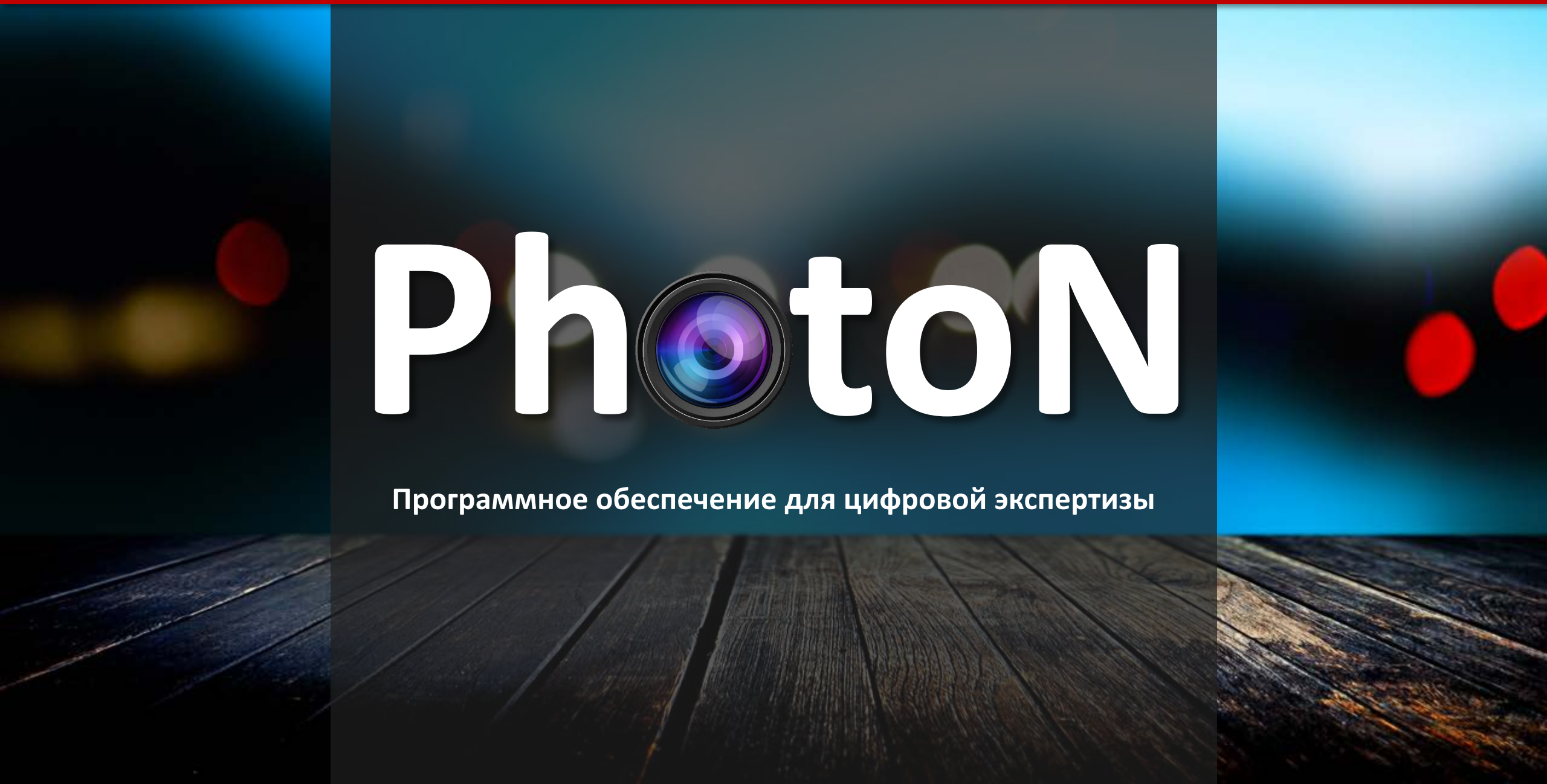
- *Приманки для вредоносных программ*
- *Спам-версии*
- *Ловушки для электронной почты*
- *Приманки для баз данных*

HoneyPot состоит из данных (например, на сайте), которые выглядят настоящей частью сайта, но на самом деле **изолированы** *и* **контролируются,** *и которые содержат информацию или ресурс, который имеет значение для злоумышленников, которые затем блокируются*

ЗАЧЕМ ВАМ НУЖЕН HONEYPOT?

HoneyPot *является эмуляцией реальных промышленных объектов или основных систем телекоммуникационной структуры на сервере. Такой сервер подключен к Интернету и привлекает хакеров как легкая цель.*





PhotoN

Программное обеспечение для цифровой экспертизы

PhotoN

Программный комплекс, который позволяет автоматически и надежно обнаруживать мошенничество любого уровня

Анализ метаданных

Каждое изображение имеет скрытые параметры (метаданные), которые меняются (удаляются) после того как изображение отредактировано

Глубокий цифровой анализ

Предполагает наложение разного рода «фильтров» на изображение, которое позволяет выявить измененные участки

PhotoN обеспечивает обнаружение мошенничества

PhotoN анализирует код изображений вместо применения обычных алгоритмов распознавания

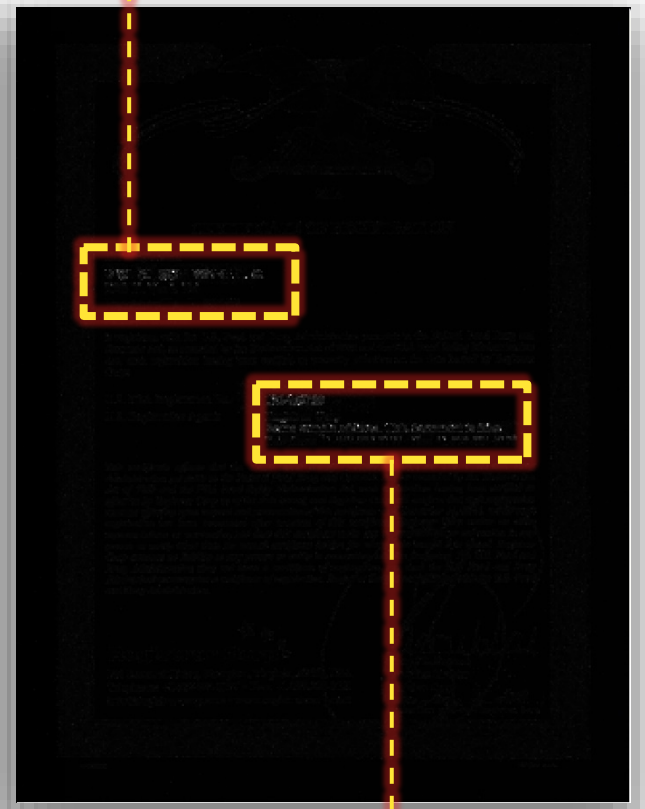
Примеры мошенничества

Поддельное фото паспорта

Результат цифрового анализа

Поддельный скан документа

Результат цифрового анализа



WOW!Mirror

Инновационный рекламный носитель с функцией безопасности

Патент РФ № 116263

СИСТЕМА ДЛЯ РЕКЛАМИРОВАНИЯ

WOW!Mirror

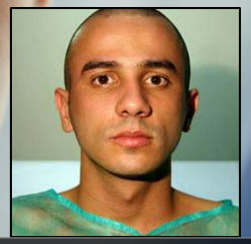
ГОТОВЫЙ БИЗНЕС

Безопасность

Встроенная система анализа скрытого наблюдения в зеркало позволяет сравнивать все полученные изображения лиц с имеющейся базой данных.



Никто не смотрит целенаправленно в камеры наблюдения. С помощью камер трудно получить отчетливое изображение лица



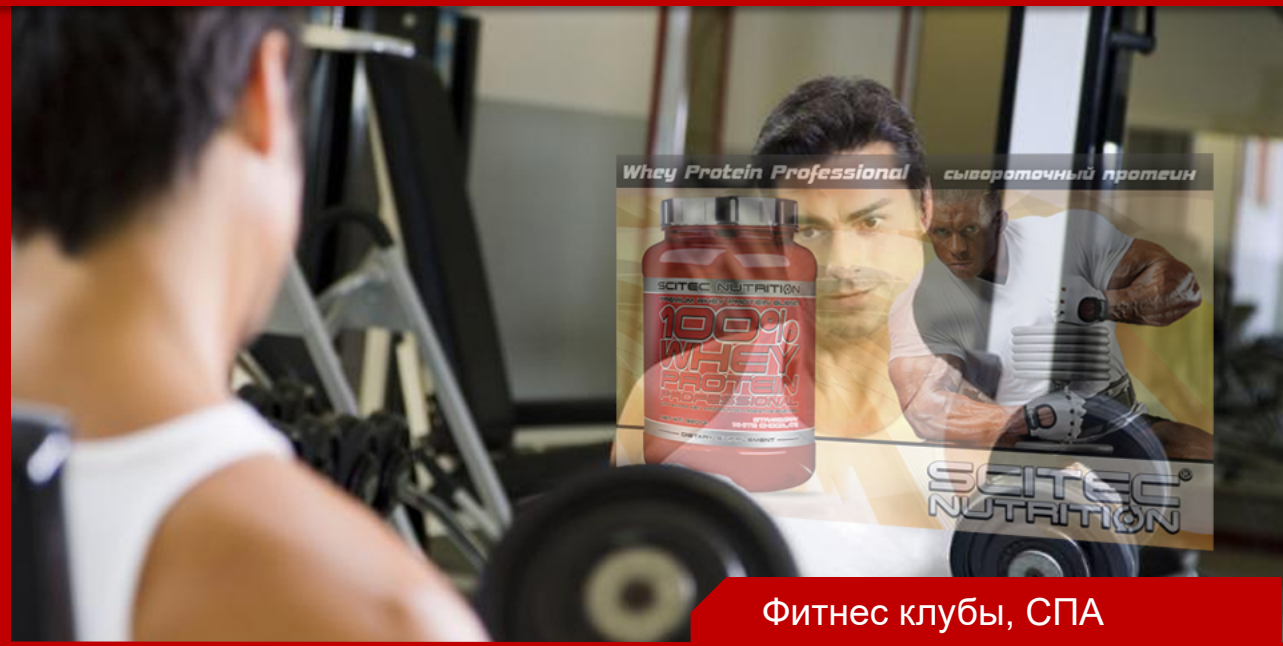
Глядя на свое отражение в зеркале, человек смотрит прямо в объектив камеры. Это позволяет получить отчетливые снимки

WOW!Mirror

ГОТОВЫЙ БИЗНЕС

ПРИМЕНЕНИЕ

Отели, салоны красоты



Фитнес клубы, СПА

Бизнес-центры, аэропорты

Рестораны, ночные клубы