Энергосервисные контракты, как защита объектов критической информационной инфраструктуры

ВЛАДИМИР РАСПОПОВ - ДИРЕКТОР ГОСУДАРСТВЕННОГО АВТОНОМНОГО УЧРЕЖДЕНИЯ НИЖЕГОРОДСКОЙ ОБЛАСТИ «ЦЕНТР КООРДИНАЦИИ ПРОЕКТОВ ЦИФРОВОЙ ЭКОНОМИКИ»

2020г.

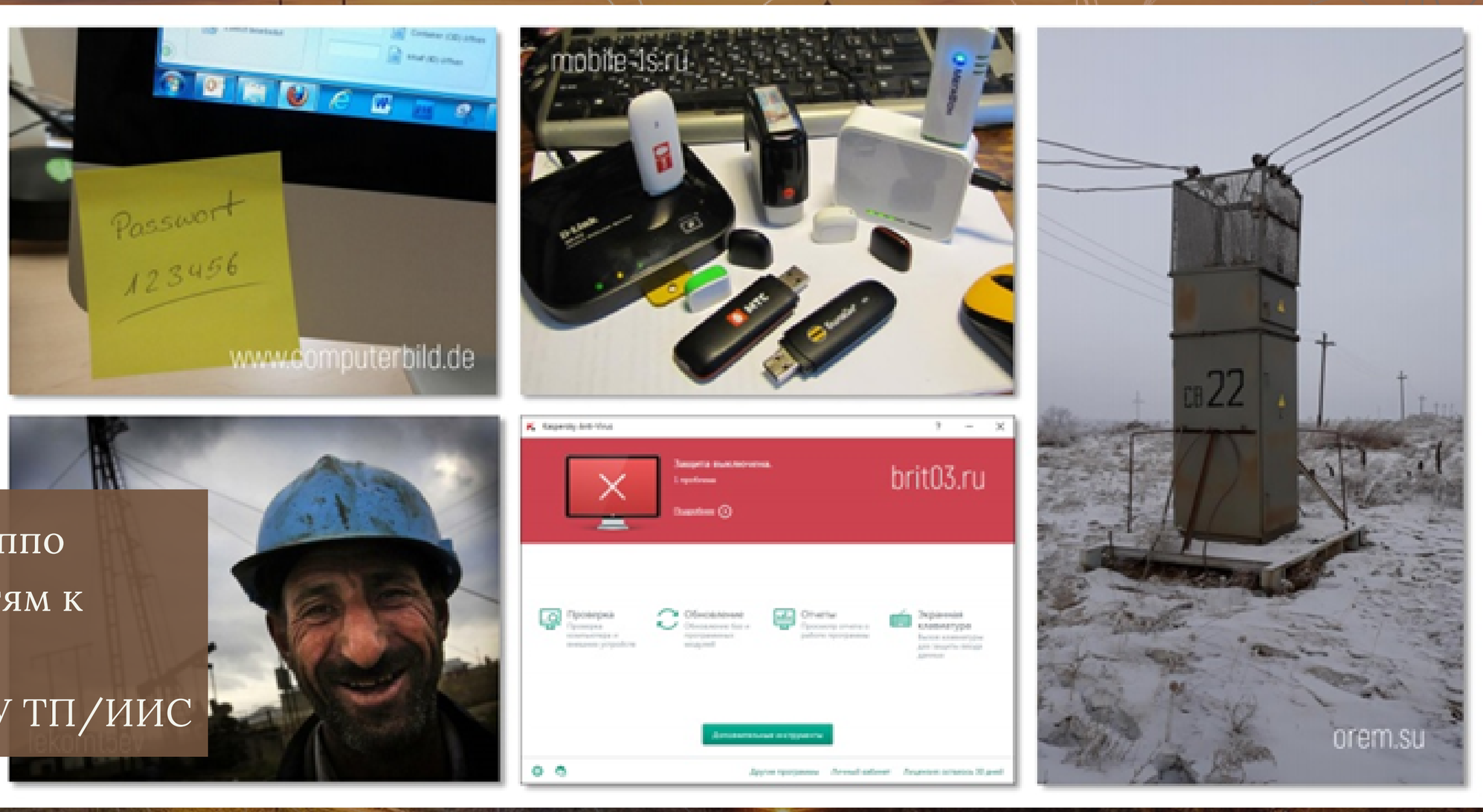
Базис проекта "Умный город"

- *ориентация на человека;*
- *технологичность городской инфраструктуры;*
- *повышение качества управления городскими ресурсами;*
- *комфортная и безопасная среда;*
- *цифровой двойник города*

Риски цифровизации

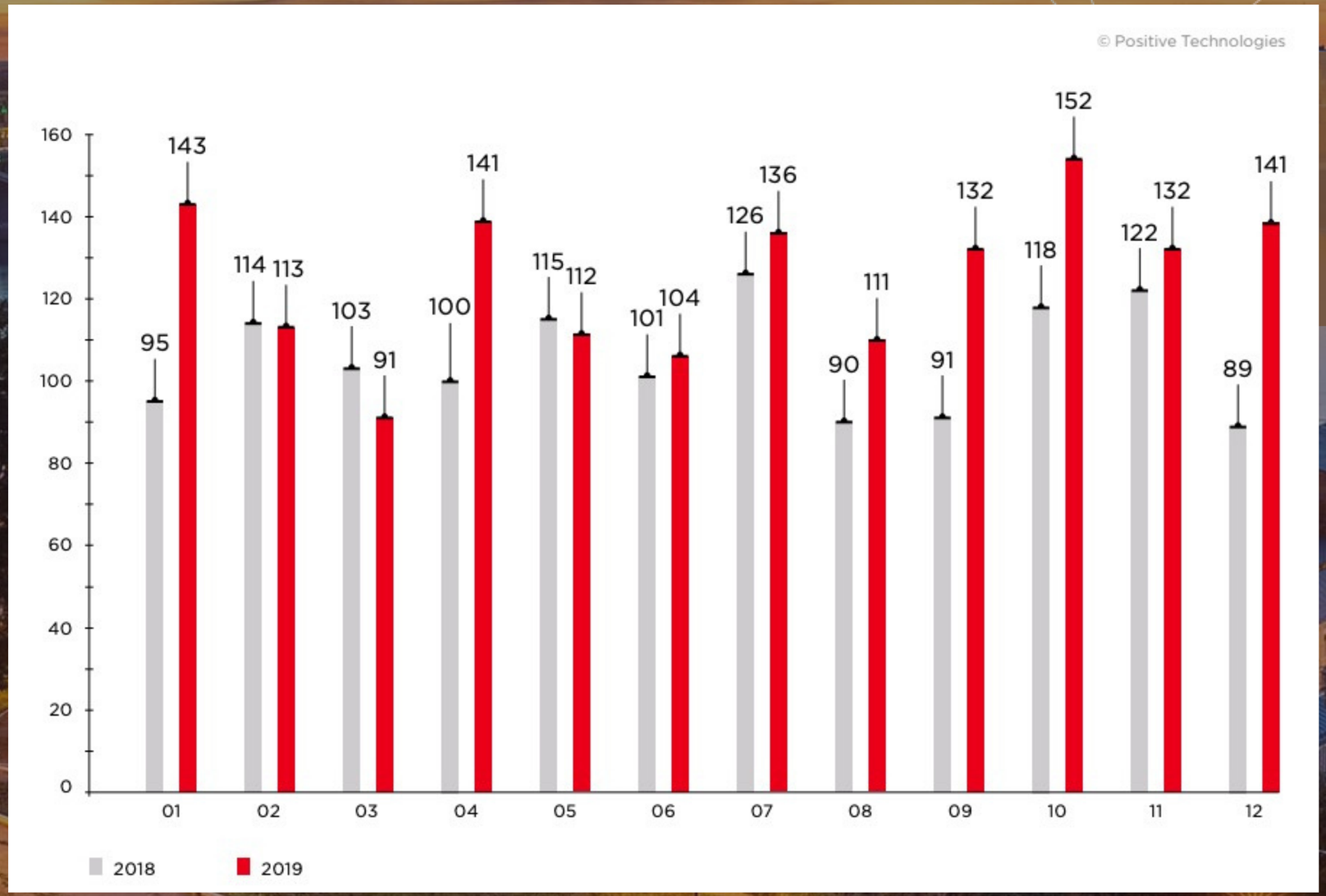
По данным МИД РФ: в 2020 году объекты КИИ России испытали более 1 миллиарда кибератак на объекты критической информационной инфраструктуры России за первые 6 месяцев

Энергосервисные контракты как способ минимизации рисков



Безопасный доступпо беспроводным сетям к измерительному оборудованию АСУ ТП/ИИС

Рост числа кибератак



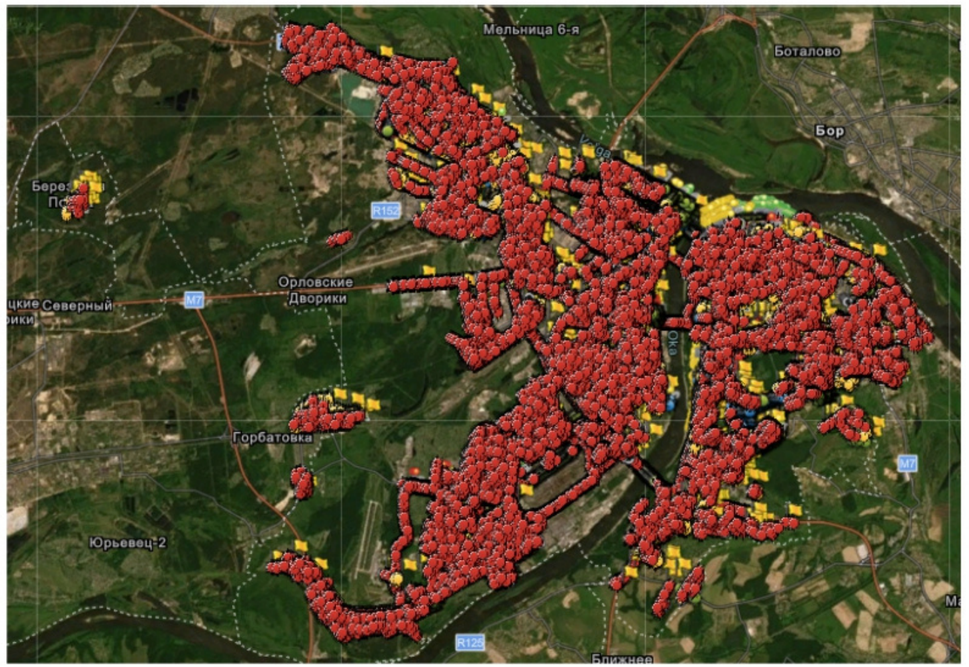
В 2019 году было зафиксировано больше 1,5 тысяч атак. Это на 19% выше по сравнению с 2018 годом.

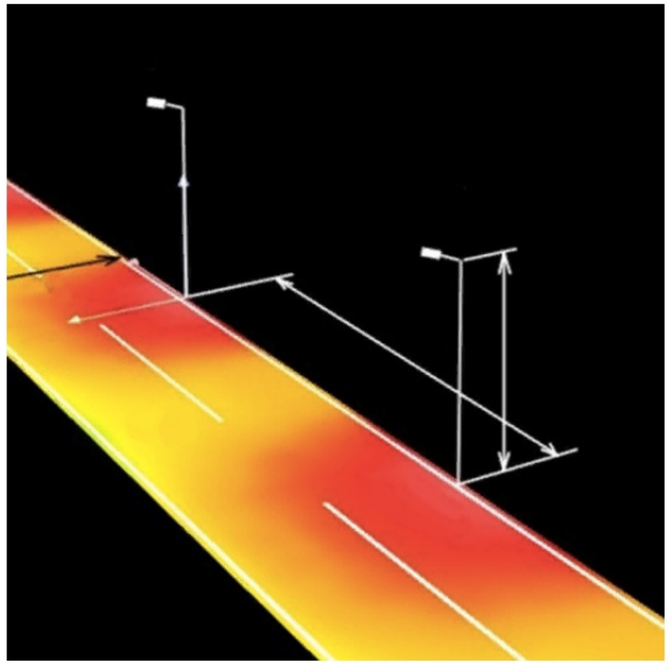
Энергосервис в Нижегородском регионе

Результаты подготовки энергосервисного контракта в освещении города Нижний Новгород

- Полностью цифровая карта системы освещения с привязкой к ГИС
- Увеличение освещенности до 4-х раз на основных магистралях
- Натуральный белый цвет основных магистралей города (4000К)
- Система АСУНО, а также контроль и управление светильниками на базебеспроводной сети LoRaWAN
- Повышение безопасности на дорогах и улицах города
- Отсутствие расходов на обслуживание системы, гарантия на оборудование

– НА ВЕСЬ СРОК ДЕЙСТВИЯ КОНТРАКТА





Энергосервис в Нижегородском регионе

Пути решения

Обеспечить физическую и функциональную защиту измерительного и каналообразующего оборудования

Организовать беспроводные каналы связи, независимые от операторов мобильного интернета

Максимально исключить удаленный доступ к измерительному оборудованию из других сетей

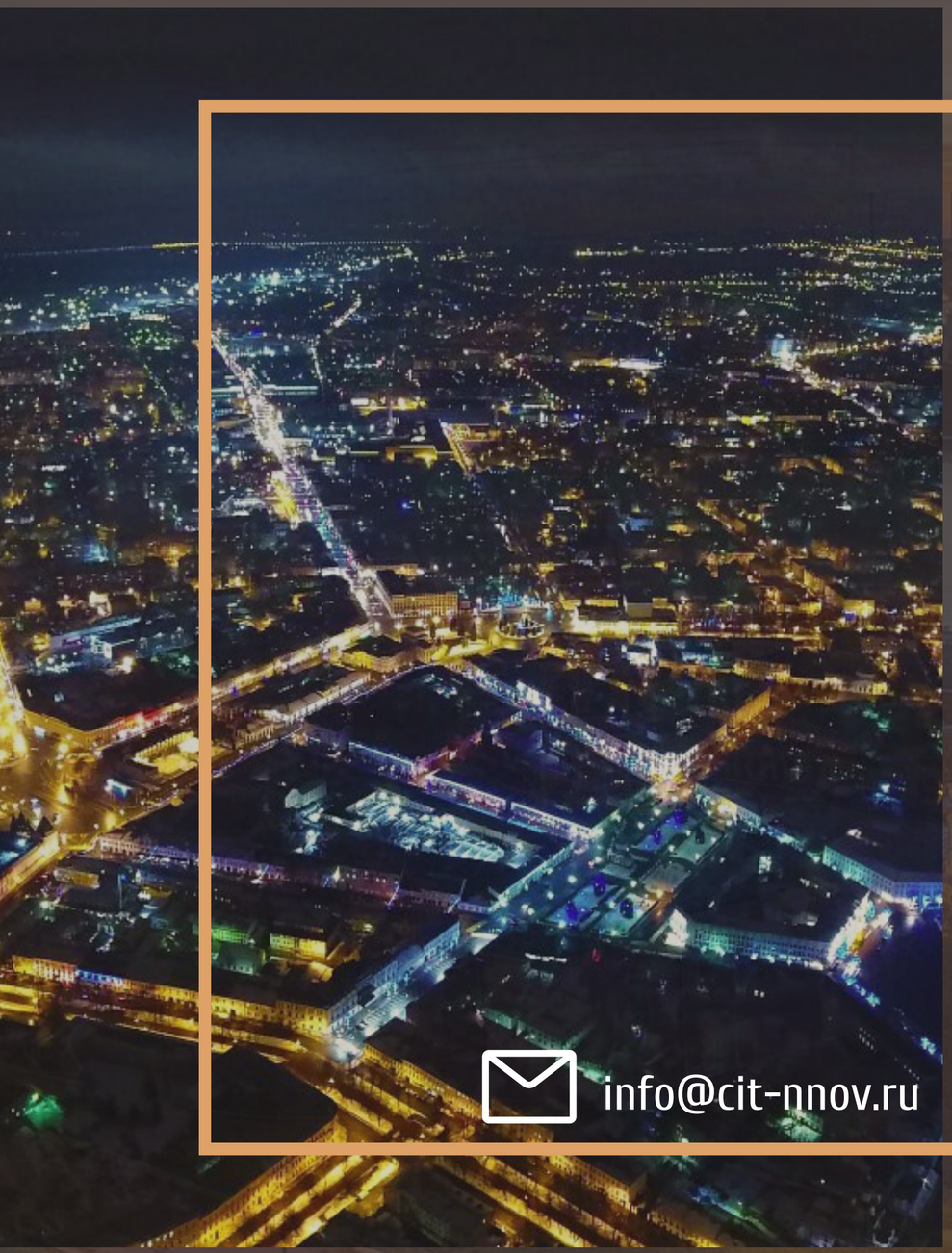
Ввести правила аутентификации, протоколирования действий пользователей, мониторинга событий

Регулярно менять пароли (хотя бы высокого уровня) и ограничить распространение всех паролей

Сегментировать технологическую сеть, исходя из специфики ее построения и использования беспроводных каналов связи

Реальная защита объектов КИИ

1. Проверка систем на уязвимости
2. Адекватный мониторинг сетей, используемых для контроля таких объектов критической инфраструктуры
3. Контроль над съемными устройствами
4. Мониторинг ПК, к которым подключены
5. программируемые логические контроллеры (или PLC)



Спасибо за внимание!

info@cit-nnov.ru

2020г.