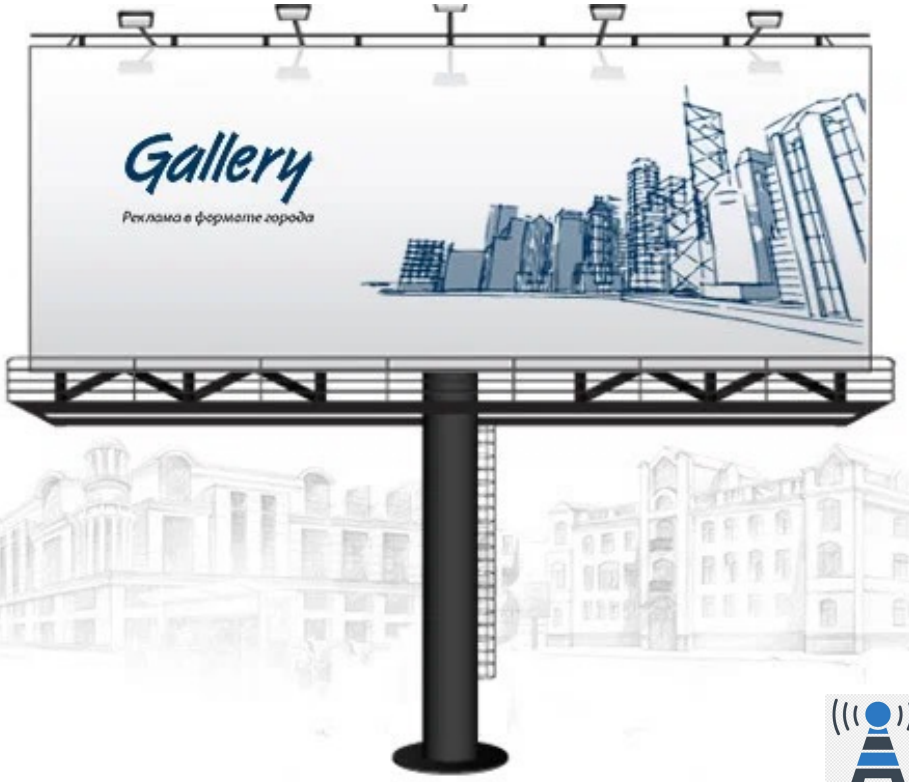
Информационная безопасность в наружной рекламе

Александр Малахов
Директор департамента
Информационных технологий
Gallery

СОЮЗ УЧАСТНИКОВ РЫНКА НАРУЖНОЙ РЕКЛАМЫ

Состав современной цифровой рекламной конструкции



Компьютер

Камера

Wi-Fi ловушка

Провайдер, канал передачи данных

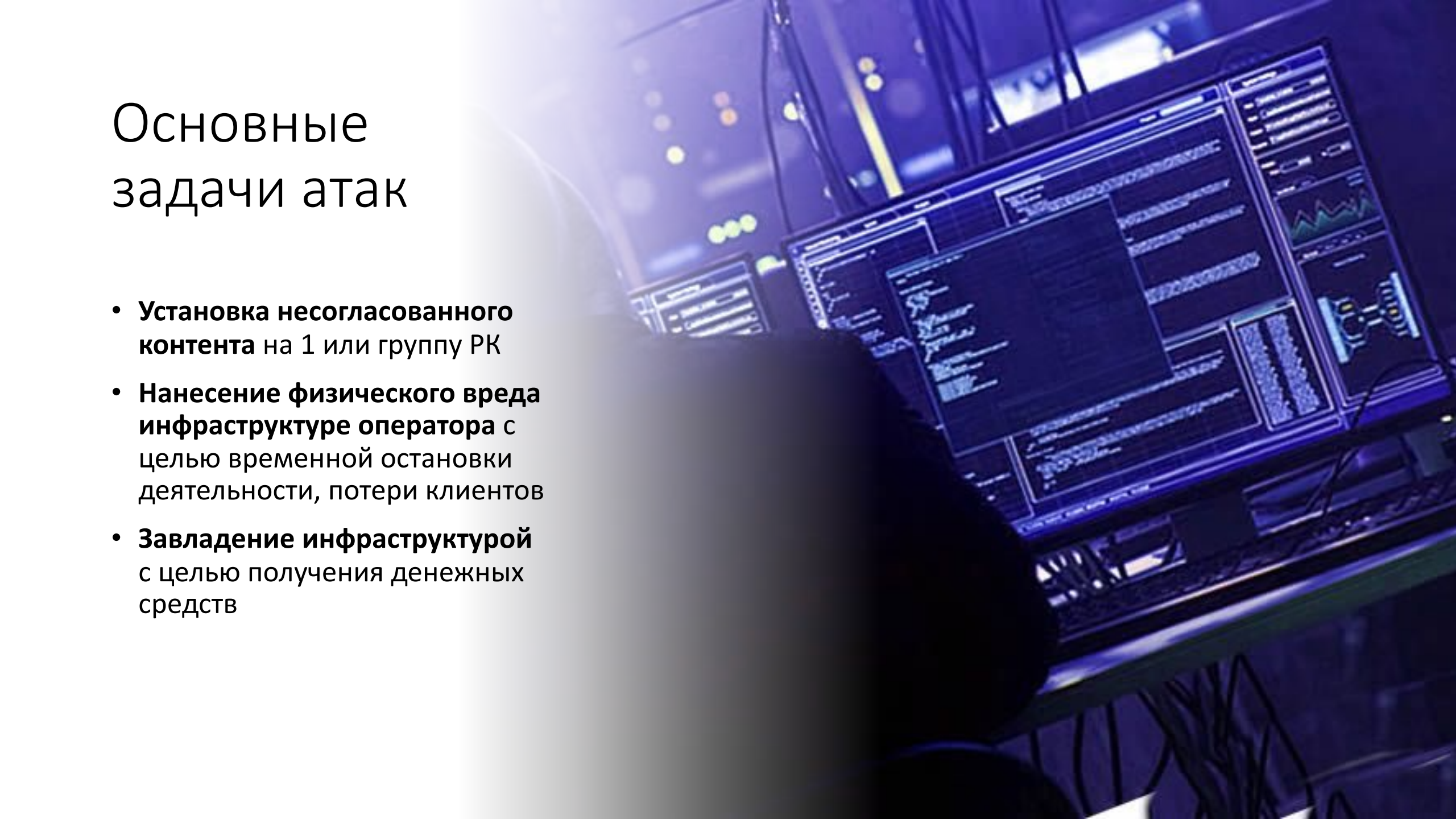
Сервера, необходимые для обеспечения
Работоспособности системы, передачи файлов

Основные типы атак

- **Физический** – получение физического доступа к РК
- **Программный** – взлом уязвимой части инфраструктуры с целю получения доступа над группой РК
- **Человеческий** – мотивация или принуждение сотрудника компании, имеющего расширенные права, на совершение противоправных действий или передачи своих учетных данных третьим лицам

Основные задачи атак

- **Установка несогласованного контента** на 1 или группу РК
- **Нанесение физического вреда инфраструктуре оператора** с целью временной остановки деятельности, потери клиентов
- **Завладение инфраструктурой** с целью получения денежных средств



Физическое проникновение на РК

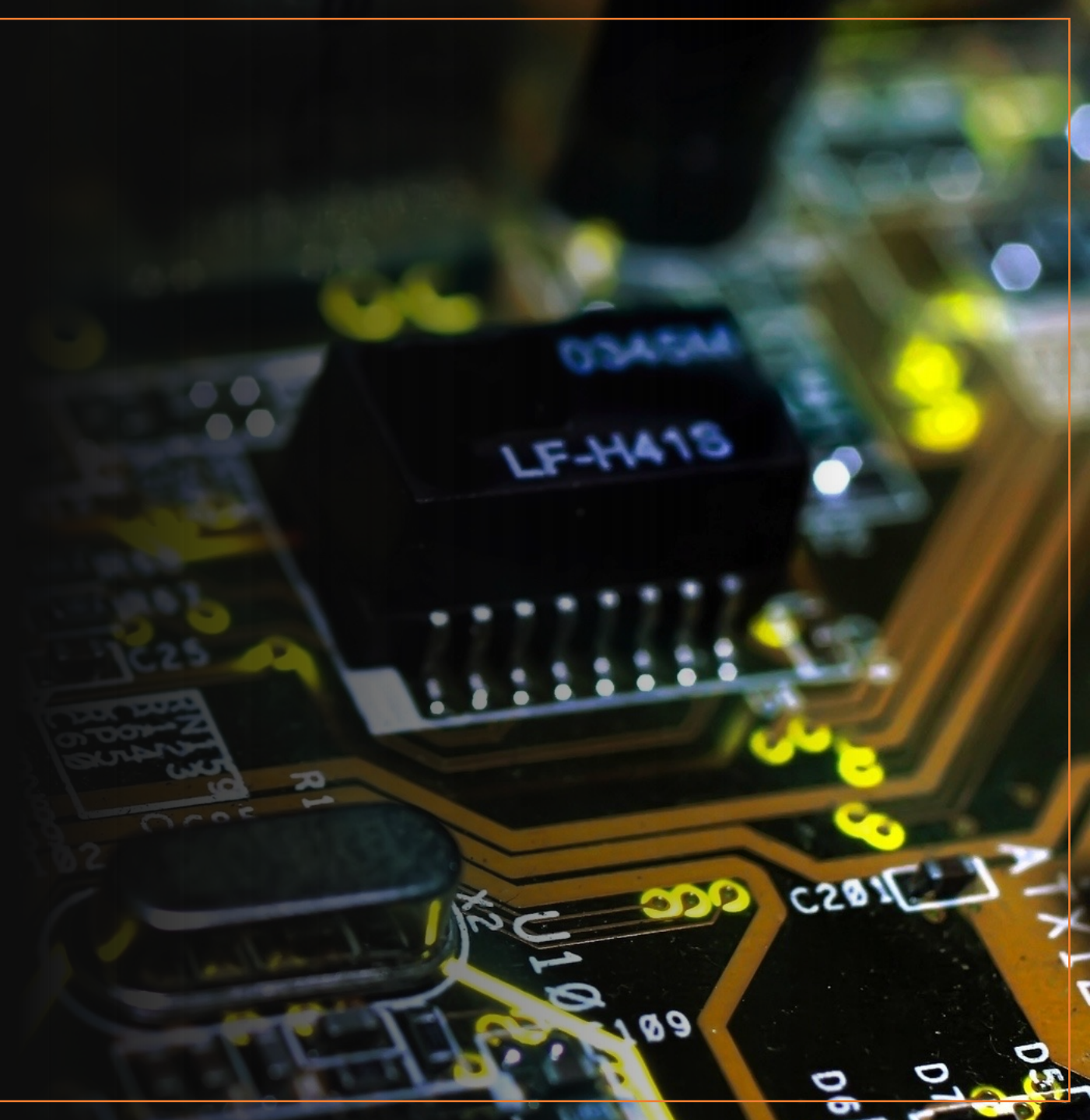
Методы предотвращения:

Установка аппаратно программного комплекса, определяющего факт проникновения на РК третьих лиц и выполняющего автоматические мероприятия по предотвращению урона.

- Сигнал диспетчеру для реагирования на инцидент
- Автоматическое отключение электричества на всей РК и последней мили

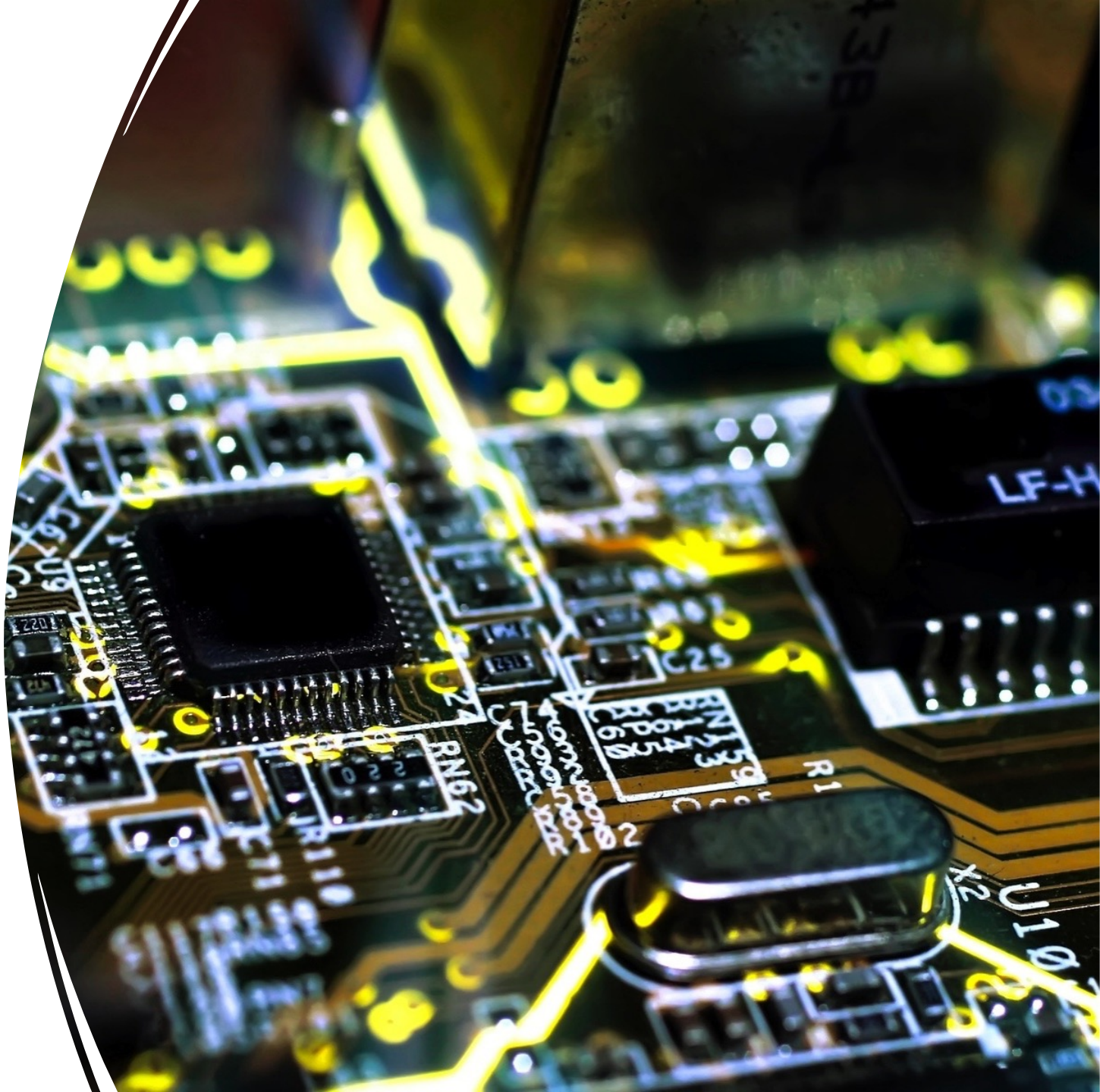
Система контроля работоспособности РК Gallery

- **Полностью спроектированная плата**
- **Собственное программное обеспечение**
- **Контроль всех показателей на РК**
- **Автономная работа**
- **Возможность доработки под изменяющиеся требования**



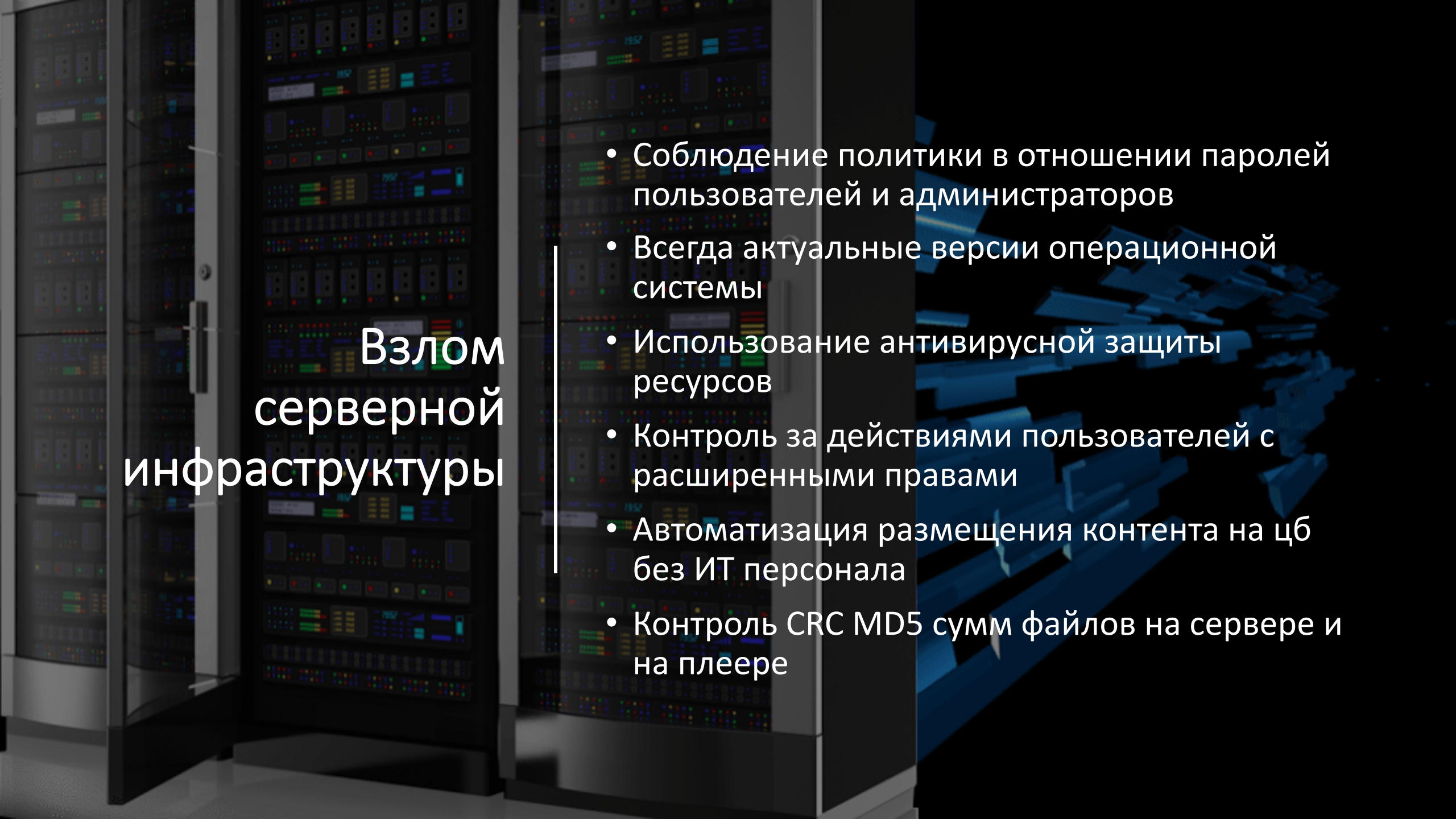
Система контроля работоспособности РК Gallery функционал

- Удаленный автоматический перезапуск компонентов РК без необходимости выездов
- Мониторинг через камеру качества выводимого изображения
- Отслеживание зависания компьютера
- Отслеживание неработающих панелей
- Мониторинг электрической составляющей (потребление, мощность)
- Противодействие проникновению
- Контроль температурных показаний



Взлом инфраструктуры оператора связи

- Нельзя полагаться только на технологические решения используемые операторами связи
- Необходимо организовывать свой периметр безопасности внутри каналов провайдера
- Всегда актуальные версии прошивок сетевых коммутаторов и других элементов системы



Взлом серверной инфраструктуры

- Соблюдение политики в отношении паролей пользователей и администраторов
- Всегда актуальные версии операционной системы
- Использование антивирусной защиты ресурсов
- Контроль за действиями пользователей с расширенными правами
- Автоматизация размещения контента на цб без ИТ персонала
- Контроль CRC MD5 сумм файлов на сервере и на плеере

Взлом через сотрудников

- Повышение лояльности компании
- Комфортные условия труда
- Конкурентная зарплата
- Поведенческий анализ сотрудников

Спасибо за внимание!

Александр Малахов
Директор департамента
Информационных технологий

СОЮЗ УЧАСТНИКОВ РЫНКА НАРУЖНОЙ РЕКЛАМЫ