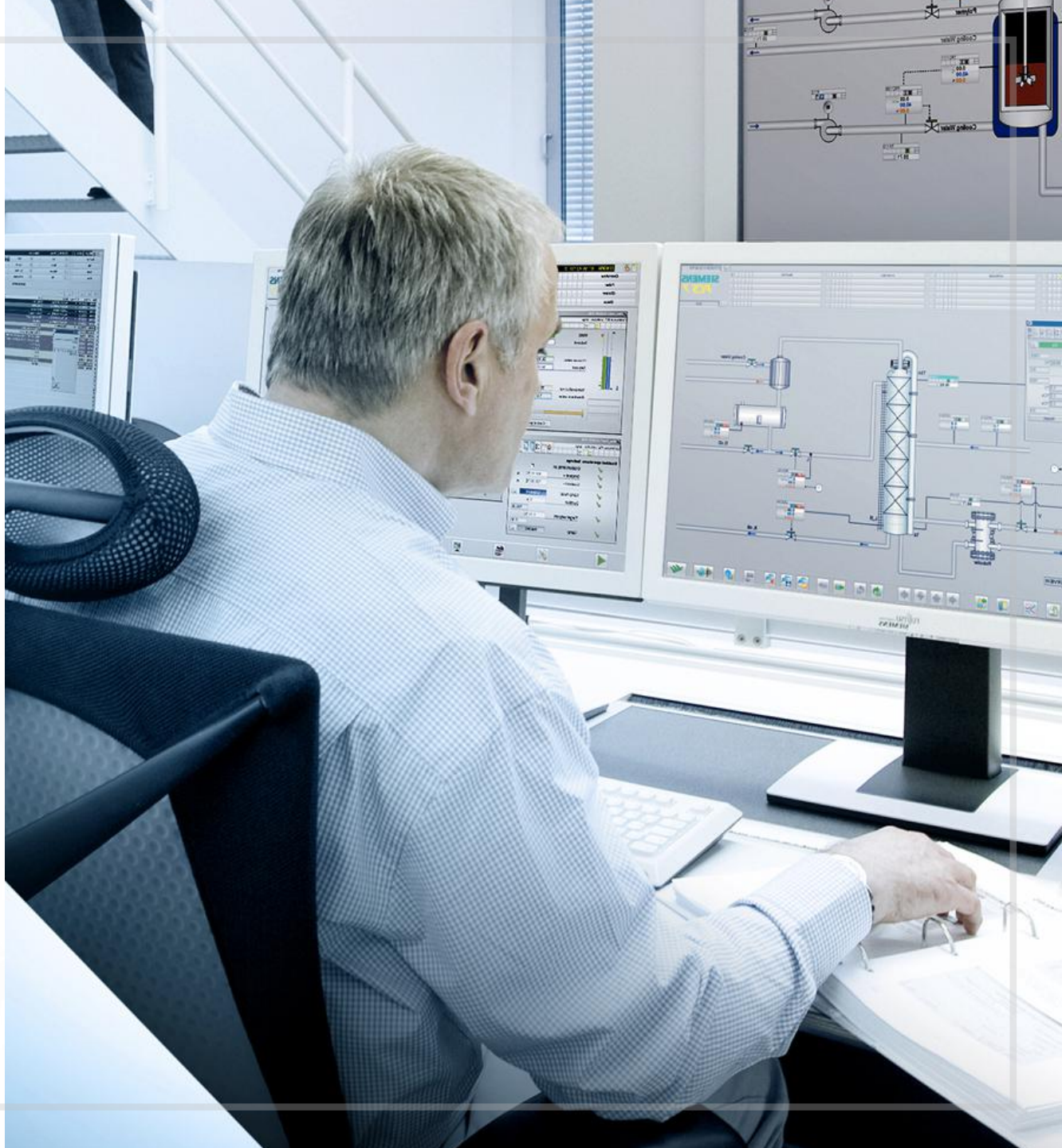
PICS: Защита автоматизированных систем управления

Информационная защита АСУ

Проблема

- Различные автоматизированные системы управления (АСУ) широко распространены и используются в транспорте, на производствах, в жилых помещениях, местах скопления людей (торговые центры, аэропорты и др.)

- С растущим количеством подобных систем увеличивается и количество вредоносного программного обеспечения. Основной целью вредоносного программного обеспечения является получение несанкционированного доступа к информации и получение контроля над объектом



Актуальность защиты АСУ

Последствия атак на АСУ

- Нарушение работоспособности ключевых систем на предприятии
- Технологические катастрофы
- Утечка информации

Всемирно известные атаки на АСУ

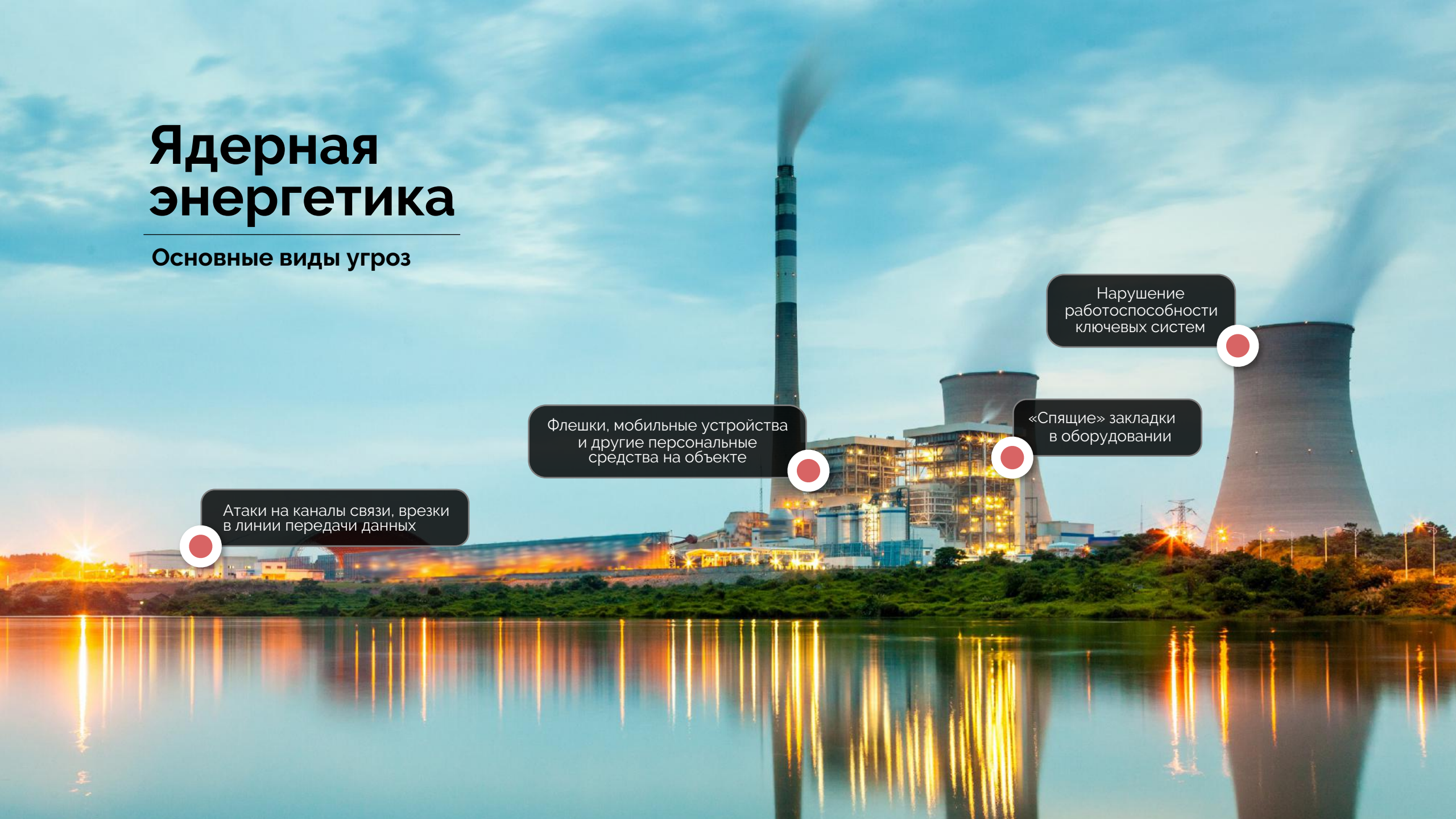
Атака Stuxnet на ядерные объекты Ирана в 2010

Атака на объекты энергоснабжения в США в 2011

Атака на Сирийские государственные газовые и нефтяные компании в 2014

Ядерная энергетика

Основные виды угроз



Нефтепереработка

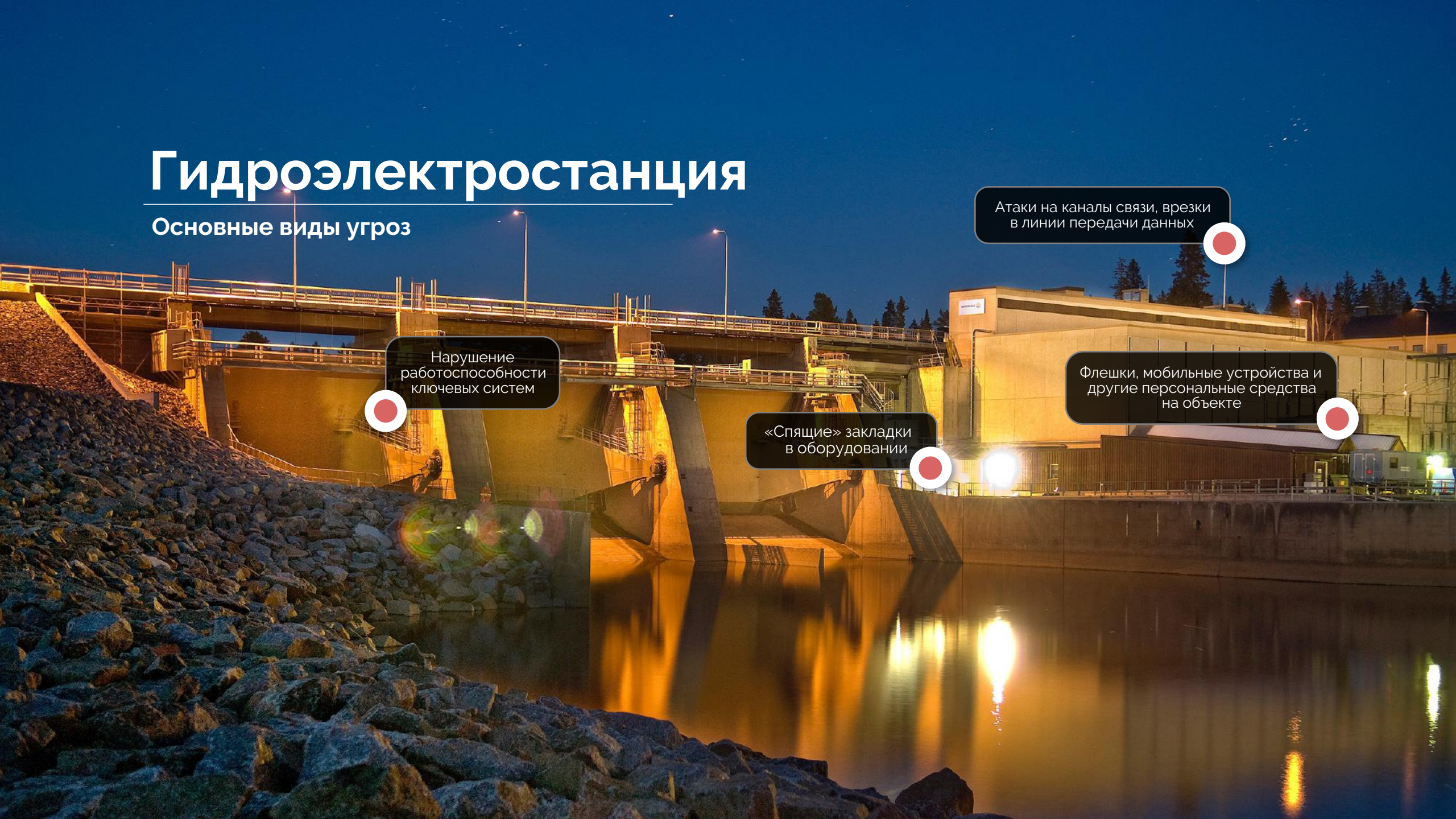
Основные виды угроз

Электроподстанция

Основные виды угроз

Гидроэлектростанция

Основные виды угроз



Аэропорт

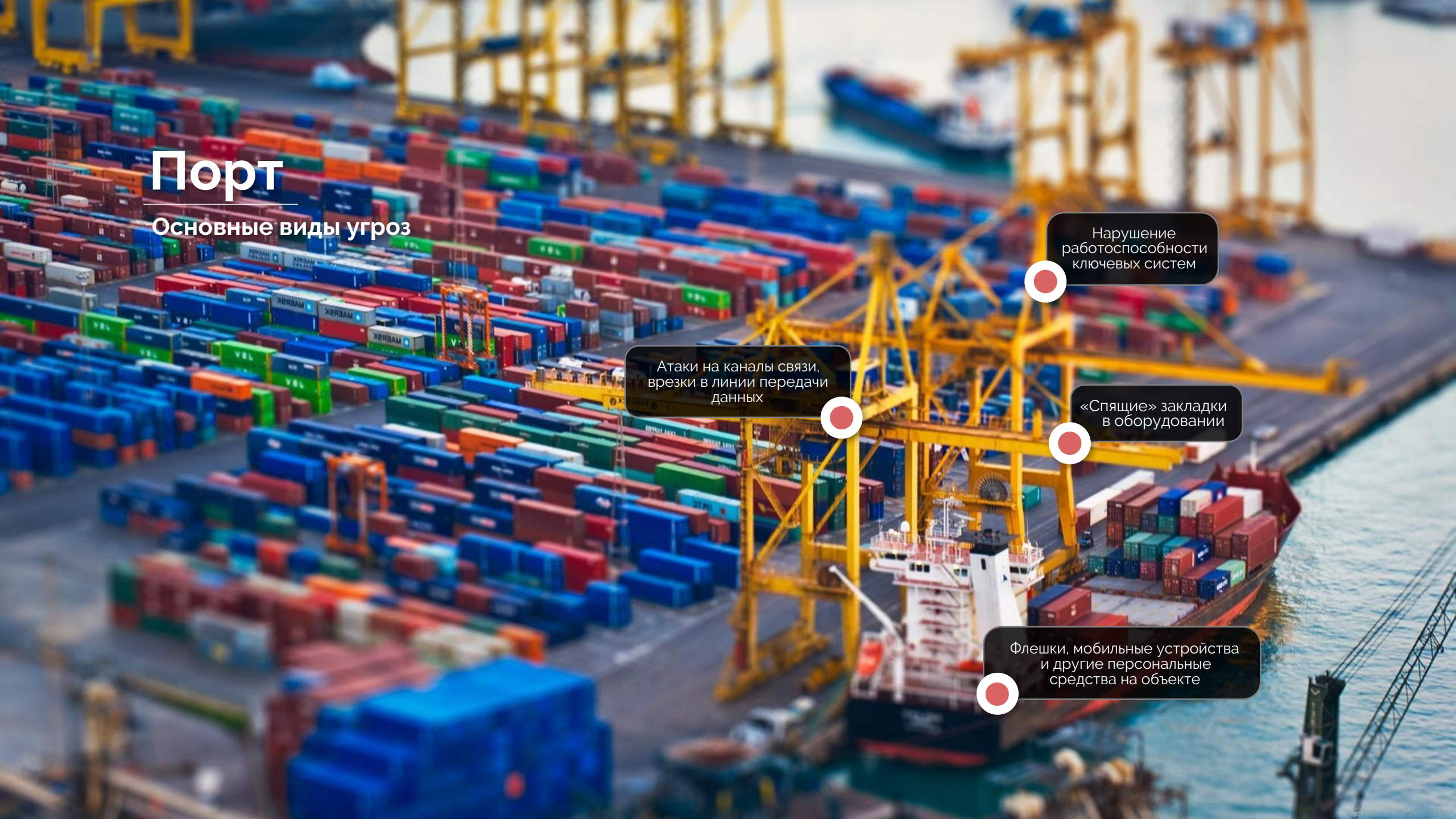
Основные виды угроз

ЖД

Основные виды угроз

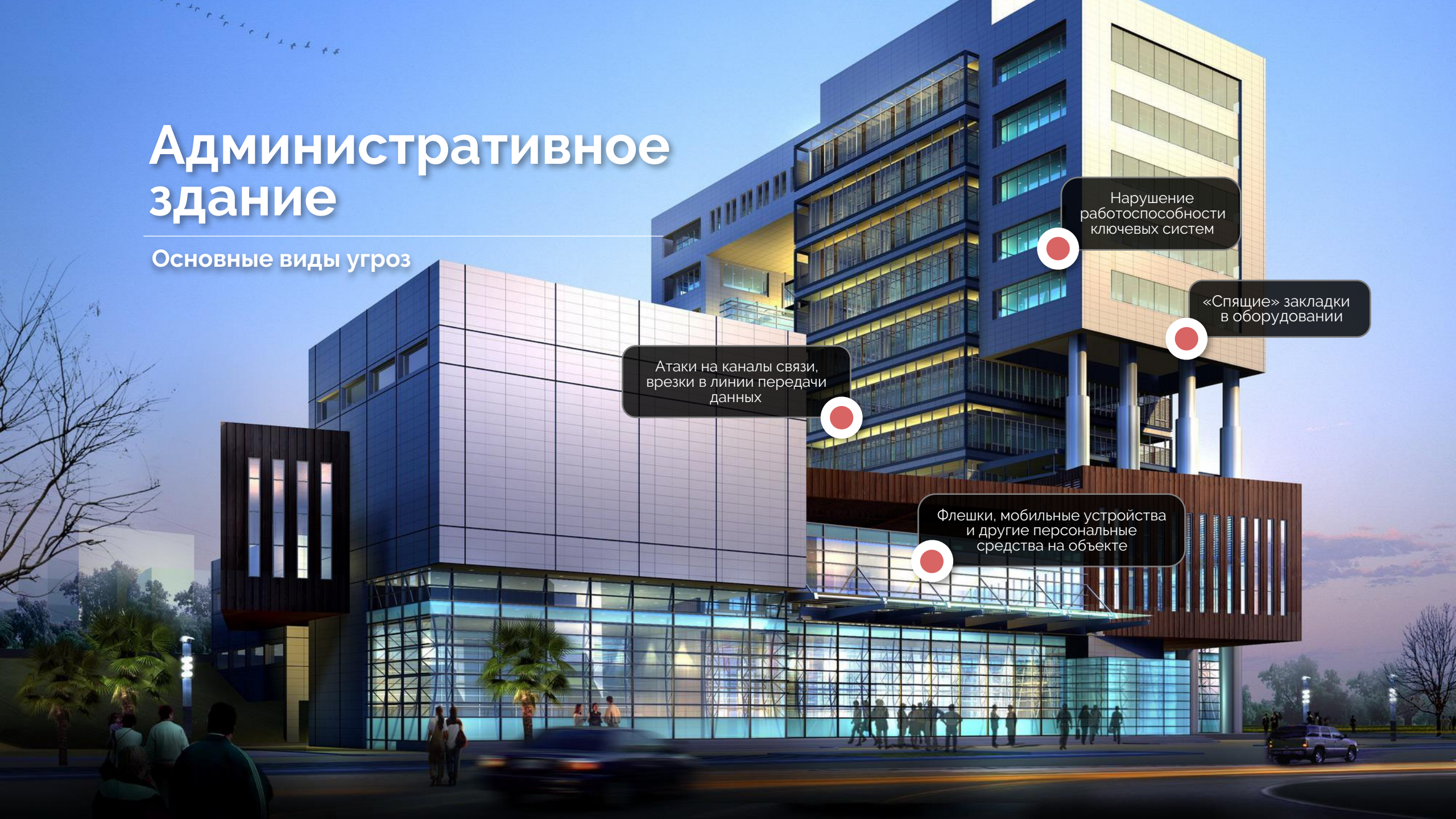
Завод

Основные виды угроз


Порт
Основные виды угроз
Нарушение работоспособности ключевых систем
Атаки на каналы связи, врезки в линии передачи данных
«Спящие» закладки в оборудовании
Флешки, мобильные устройства и другие персональные средства на объекте

Административное здание

Основные виды угроз

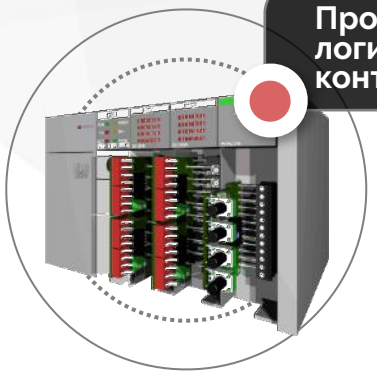


Системы контроля информационных атак

Специальный вирус

Командный центр

Программируемый логический контроллер



Завод

Системы контроля информационных атак

Системы контроля информационных атак

Командный центр

Программируемый логический контроллер

Завод 1

время X

В оборудование интегрирован GSM модуль

Остановить завод

Командный центр в другой стране

Завод 2

Завод 3

Кооперанты

Командный центр

Защищено

Защищено

Незащищено

Самолет

Программируемый логический контроллер

Завод 1

Двигатель

Программируемый логический контроллер

Завод 2

Электроника

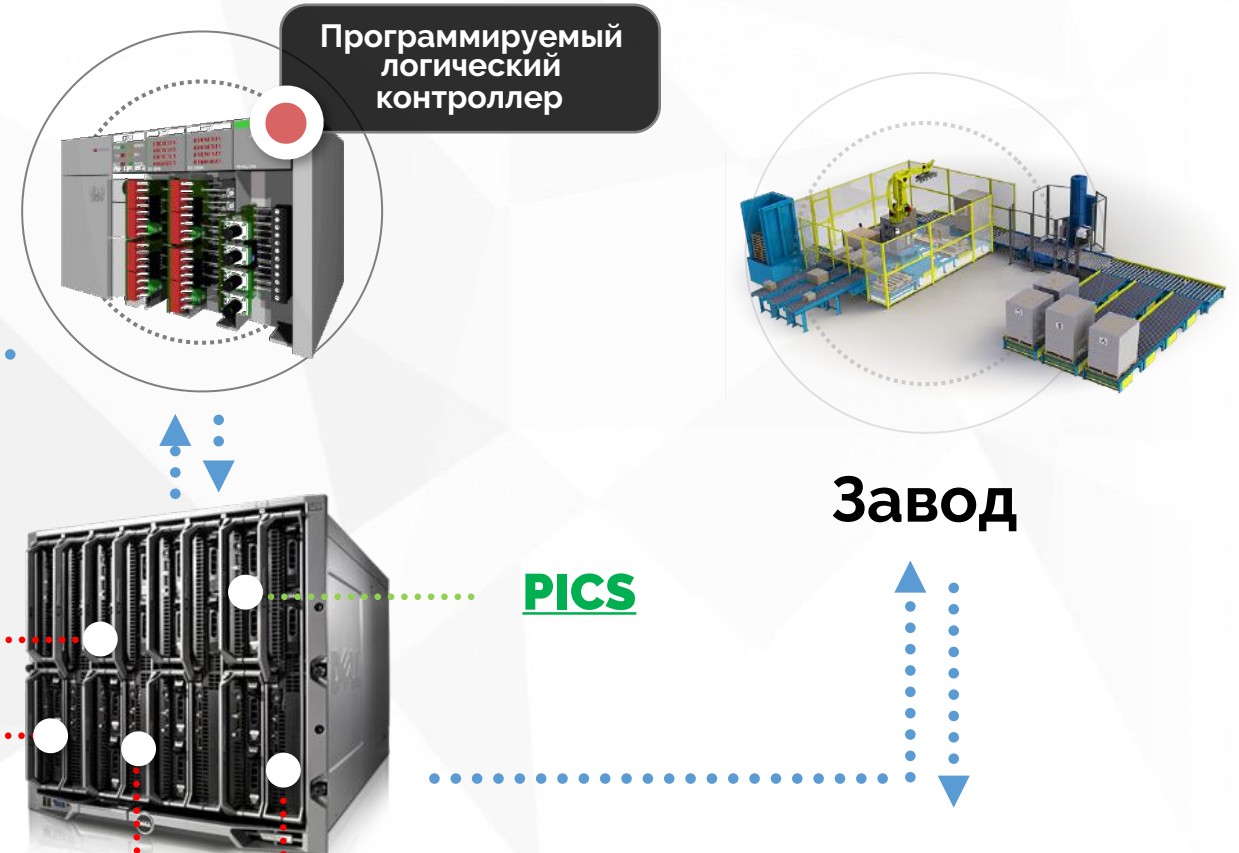
Программируемый логический контроллер

Завод 3

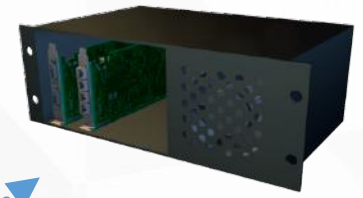
Вирусная атака

Вирус

Защита и состав компонента



Сценарий защиты



PICS

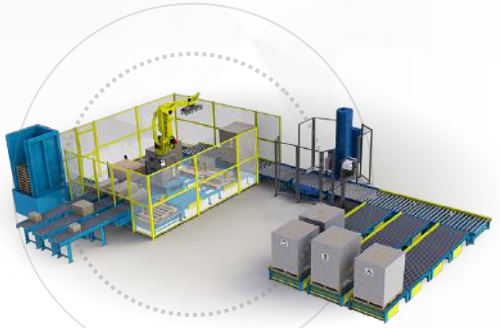
Вирусная атака

Вирус

Блокировка

Предупреждение

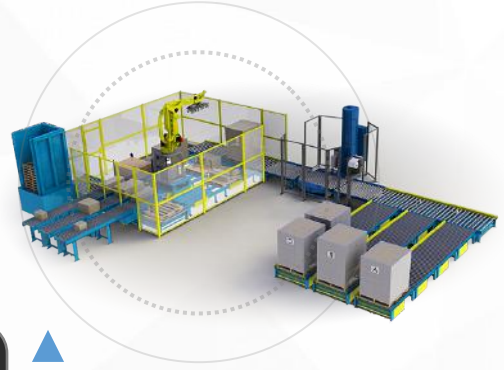
Программируемый логический контроллер



Завод

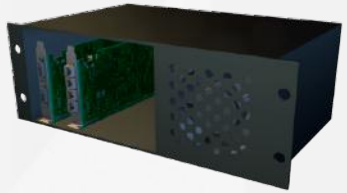
Командный центр

Сценарий защиты



Завод

Программируемый логический контроллер



PICS

Командный центр

Блокировка

Ложный ПЛК

Состав защиты

Подключаемая
система расширения

(может быть куплена позже)

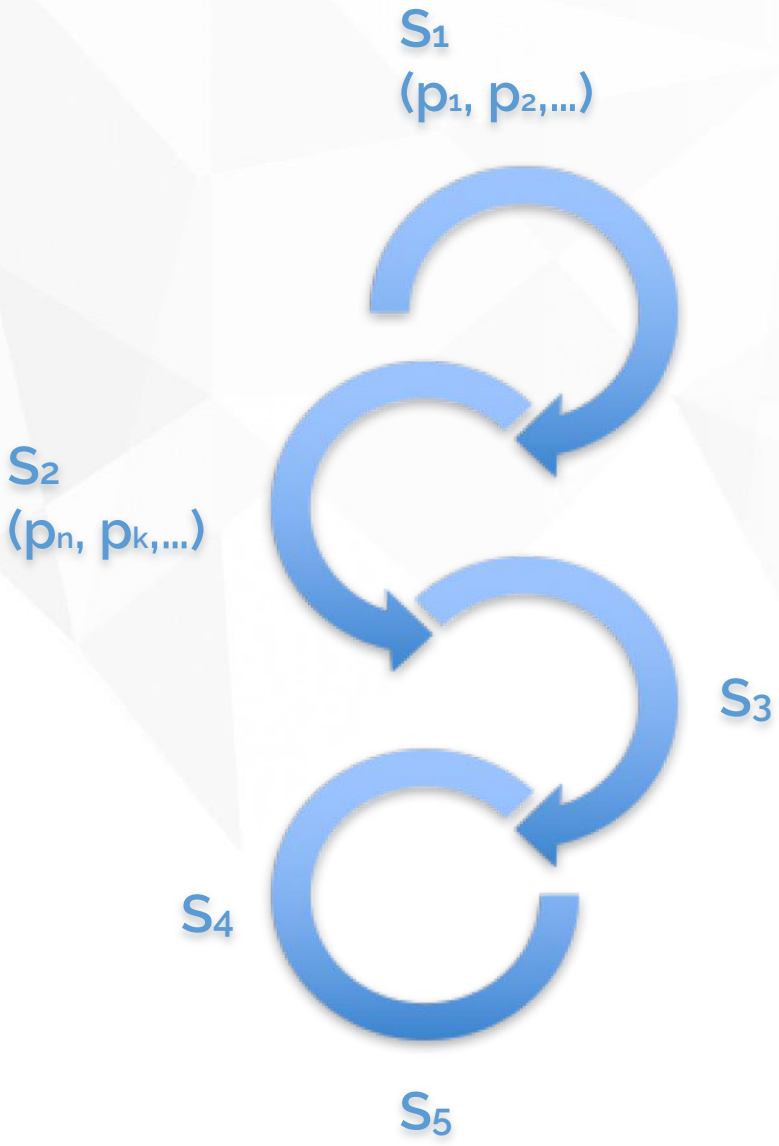
Модули:

- Модуль 1
- Модуль 2
- Модуль 3
- Модуль 4

PICS-
основа алгоритма

В составе PICS более 20 запатентованных алгоритмов, в том числе:

- Глубокая проверка пакетов
- Сигнатурный анализ
- Проверка целостности
- Статистический анализ
- Контроль соответствия технологического процесса



Преимущества PICS

	PICS	Анти-вирусы	Сканер уязвимостей	Межсетевое экранирование	Диод данных
Вирусные атаки на SCADA	✓	✓	✗	✗	✗
Нелегальная перестановка устройств на нижнем уровне	✓	✗	✗	✗	✗
ARP-spoofing	✓	✗	✗	✓	✓
Перепрограммирование ПЛК	✓	✗	✗	✗	✗
Уязвимости SCADA	✓	✗	✓	✗	✗
Нарушение технологических процессов	✓	✗	✗	✗	✗
Несанкционированный удаленный доступ	✓	✗	✗	✗	✗

Конкурентный анализ

	PICS	Cisco SAFE	CheckPoint NGNFW	Tenable Network Security	Tofino Security Appliance
Аппаратный / программный комплекс	Аппаратно-программный комплекс	Аппаратно-программный комплекс	Аппаратно-программный комплекс	Программное обеспечение	Аппаратно-программный комплекс
Количество поддерживаемых протоколов	11	7	10	4	7
Межсетевой экран	✓	✓	✓	✗	✓
Автоматический аудит безопасности	✓	✗	✓	✓	✗
Адаптировация под нужды заказчика	✓	✗	✗	✗	✗
Обнаружения несанкционированного доступа/недокументированных функций	✓	✗	✗	✗	✓
Проверка протоколов обмена данных	✓	✓	✓	✗	✓
Проверка моделей оборудования и программного обеспечения для обнаружения уязвимостей в базе данных	✓	✗	✗	✓	✗

Процесс интеграции

01 **Аудит**

(1-2 месяца)

Результат
200 страниц

02 **Проект**

(2 месяца)

Командный центр ▶ **ПЛК** ▶ **Предприятие**

План

Проектная документация
+ Цена проекта

03 **Установка и настройка**

(2 месяца)

04 **Сервисная поддержка**

Обновление антивируса
+ Поддержка системы