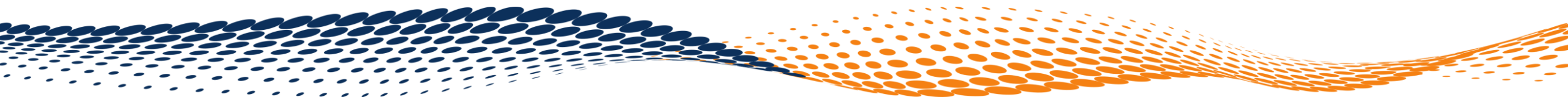




СИСТЕМА БЕЗОПАСНОСТИ В ИСУ

2024 год



Интеллектуальная система учёта электрической энергии (ИСУЭ) создается с целью реализации требований Постановления Правительства РФ от 19 июня 2020 г. № 890 «О порядке предоставления доступа к минимальному набору функций ИСУЭ»

ОСНОВНЫЕ ЦЕЛИ И ФУНКЦИИ ИСУЭ

- **Передача заявок** на управляющие воздействия приборами учёта, в том числе *удалённое* ограничение (возобновление) режима потребления
- **Повышение финансовой дисциплины потребителей**, упрощение процедуры введения ограничения мощности ИПУ потребителей
- **Сбор, обработка, передача и хранение** показаний приборов учёта
- **Мониторинг режимов потребления** электрической энергии за счет внедрения подсистем контроля и регулирования
- **Фиксация неучтённого потребления электроэнергии**, а также фактов несанкционированного вмешательства потребителей в работу ИПУ
- **Упрощение процесса передачи показаний** приборов учёта ЭЭ для потребителей
- **Повышение прозрачности** начислений по показаниям ИПУ
- **Организация доступа** к показаниям ИПУ со стороны заинтересованных юридических и физических лиц (потребителей)

Основная цель построения системы ИБ – минимизация рисков нарушения функционирования ИСУЭ и обеспечение соответствие требованиям регуляторов

Основные риски, которым подвержена ИСУЭ:

- Удалённое вмешательство в работу
- Ограничение подачи ЭЭ потребителям

В случае нарушения функционирования Системы возможны последствия с высокой социальной значимостью, связанные с вероятным ущербом для жизни или здоровья людей например:

- Ограничение подачи энергии на предприятия, медицинские учреждения и т.д.
- Нарушение работы транспортной инфраструктуры
- Нарушение или прекращение подачи ЭЭ в квартиры населения РФ
- И т.п.

Риски нарушения требований законодательства о области защиты **критической инфраструктуры** (№187-ФЗ от 26.07.2017) и в области защиты Персональных данных (№152-ФЗ от 26.01.2007)

Иные риски нарушения функционирования ИСУ:

- Потеря управления приборами учёта
- Потеря контроля потребляемой мощности потребителями
- Невозможность корректного сбора информации о потреблённой ЭЭ
- И т.д.

За несанкционированное вмешательство в работу ИСУЭ предусмотрена уголовная ответственность

- УК РФ ст. 274.1 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации
 - Срок до 5 лет, штраф до 1 млн. ₽ — получение **несанкционированного доступа** к информации ОКИИ или осуществление **неправомерного воздействия** на критическую информационную инфраструктуру, использование, создание или распространение компьютерных программ заведомо предназначенных для неправомерного воздействия на неё
 - Срок до 6 лет — нарушение **правил эксплуатации** средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, либо **правил доступа** к указанной информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда
 - Срок до 8 лет за деяния **группой лиц или с использованием служебного положения**
 - Срок до 10 лет за **тяжкие последствия**
- Дополнительно может быть квалифицировано по статьям 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ) и 272 УК РФ (Неправомерный доступ к компьютерной информации)

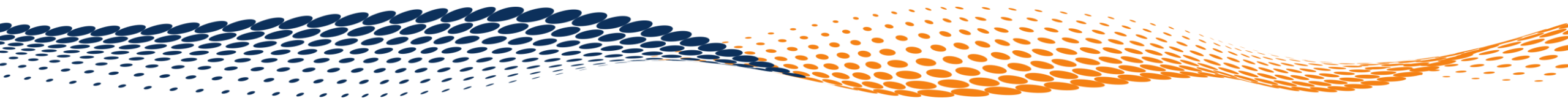
За прочие нарушения при работе с ИСУЭ предусмотрена административная ответственность

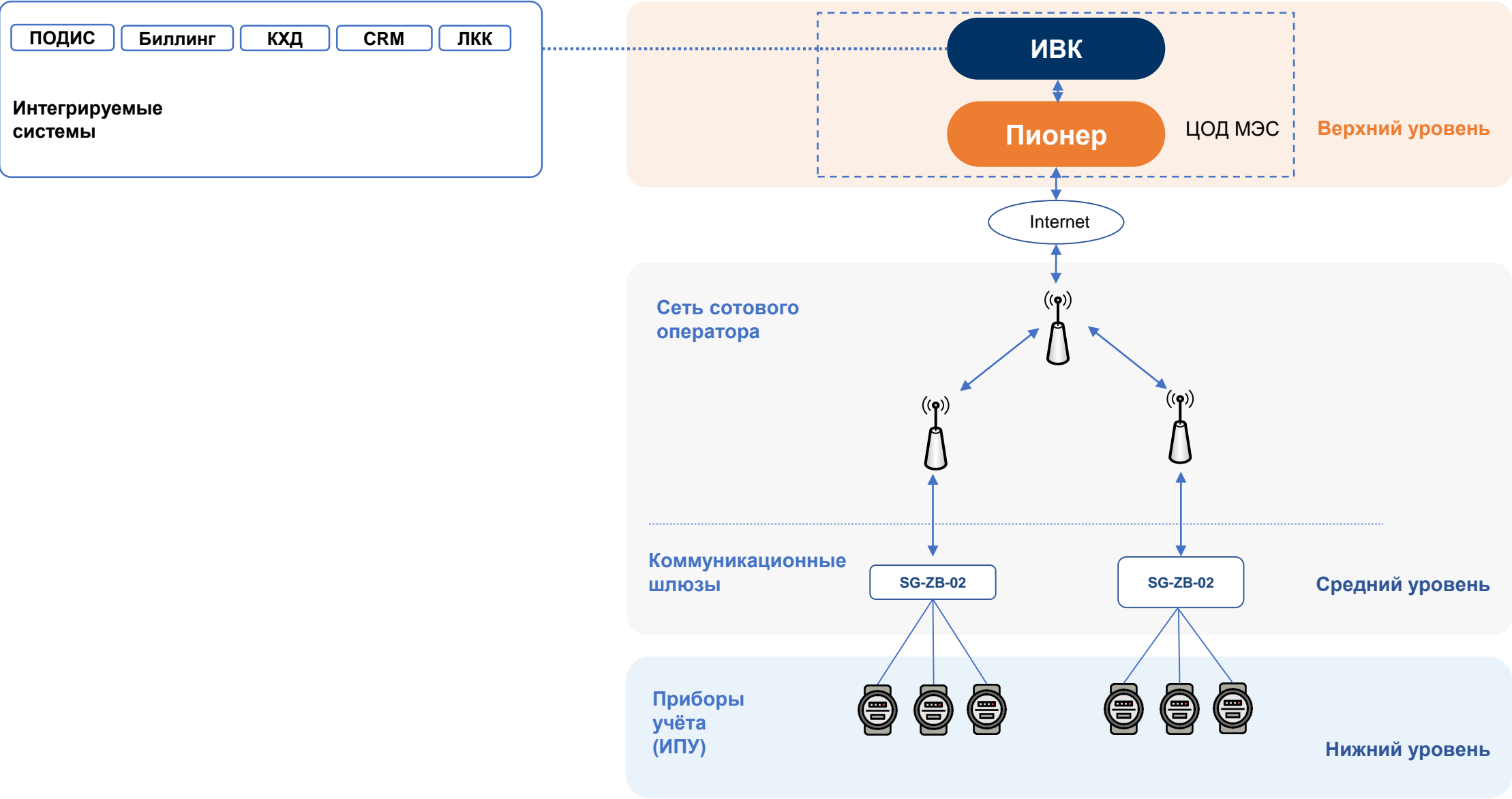
- КоАП РФ Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
 - Штраф до 50 000 ₽ на должностное лицо или 100 000 ₽ на юрлицо за нарушение требований к созданию или функционированию значимых объектов критической информационной инфраструктуры (без признаков уголовного преступления)
 - Штраф до 50 000 ₽ на должностное лицо или 500 000 ₽ на юрлицо за нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, нарушение порядка обмена информацией о компьютерных инцидентах
- Привлечение осуществляют ФСТЭК России и ФСБ России
- Если не выполнено ранее вынесенное предписание (постановление, решение, представление), то штраф за невыполнение до 20 000 ₽ + дисквалификация
- Прочие штрафы, связанные с нарушениями в области персональных данных и информации ограниченного доступа

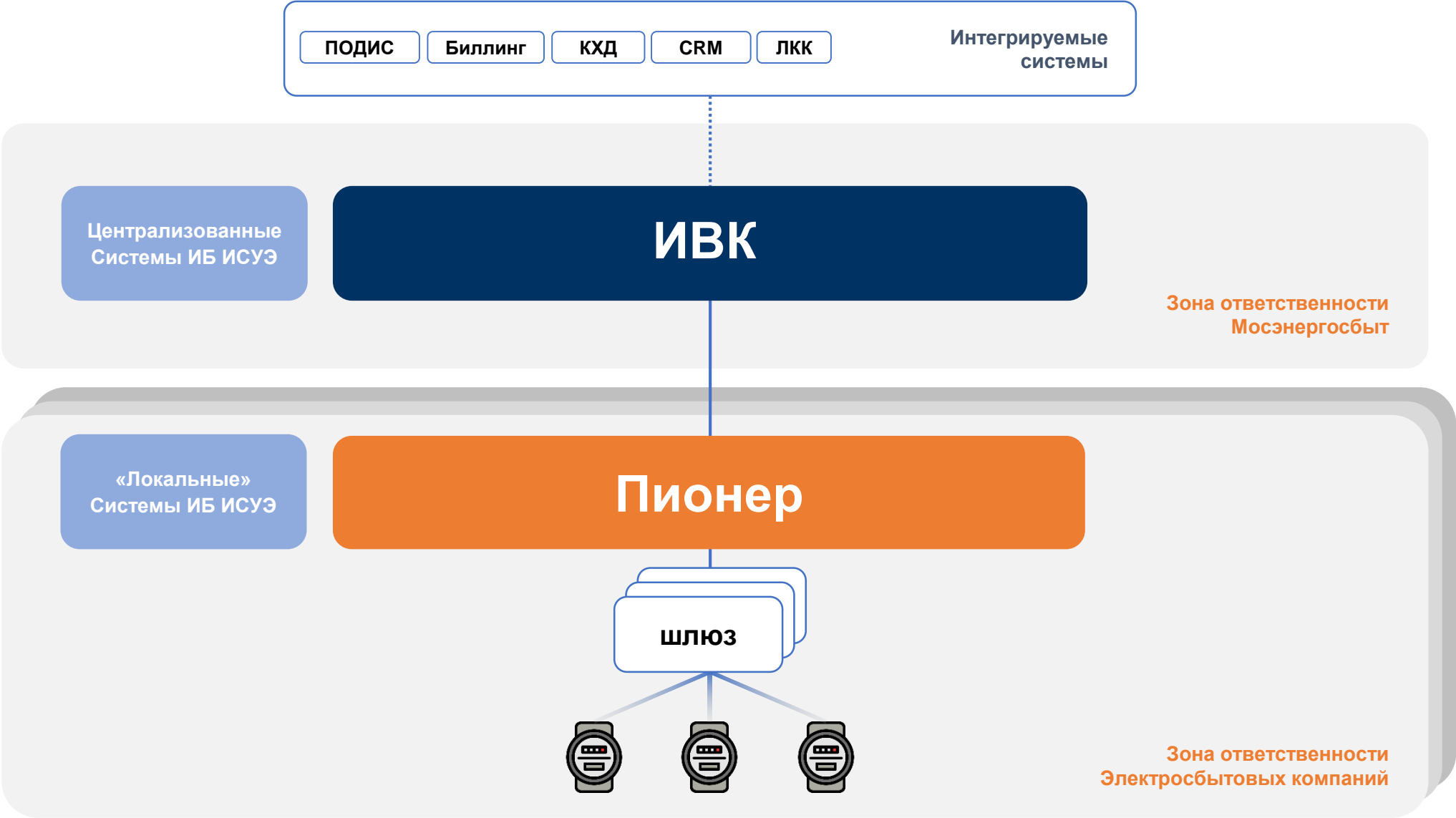
В системе ведется мониторинг!



КЛЮЧЕВЫЕ РЕШЕНИЯ ПО ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ ИСУЭ







МОСЭНЕРГОСБЫТ

- **ИБК**, включая АРМ
- **СУП СПД Пионер** МЭС
- **АРМ операторов ИБК**
и СУП СПД Пионер сегмента

ЭНЕРГОСБЫТОВЫЕ КОМПАНИИ

- **СУП СПД Пионер** ЭСК
- АРМ операторов
СУП СПД Пионер

* Несмотря на наличие договоров сопровождения подсистем ИБ между МЭС и ЭСК ответственность за обеспечение ИБ лежит на **ЭСК, как владельцах СУП СПД Пионер.**

Сегментирование системы, изоляция сегментов ИСУЭ от общей инфраструктуры ЦОД МЭС

- Устройства однонаправленной передачи данных (Дата-диод), для изоляции ИС ИВК и СУП СПД «Пионер», друг от друга и возможной их компрометации извне.



Механизмы подтверждения заявок поступающих со стороны пользователей

- Подтверждение заявок пользователей электронной цифровой подписью
- Невозможность подачи управляющих команд от физлиц
- Модуль автоматической проверки корректности заявок
- Ручная валидация заявок пользователей при передаче управляющих команд



Применение средств защиты информации
в соответствии с законодательством РФ
и внутренней нормативной документацией ПАО
«Интер РАО»

Проверка безопасности исходных кодов
программного обеспечения ИВК и СУП СПД
Пионер (безопасная разработка)

Мониторинг событий, влияющих на
функционирование ИСУЭ, с передачей
инцидентов в Центр противодействия
кибератакам ПАО «Интер РАО»

- Событий приборов учёта
- Отключений
- Ограничений подачи
- Инфраструктурных событий
- Бизнес-рисков

Корректность реализации проектных решений подтверждена на практике

Проведены тестирования на проникновение (имитация взлома системы)

- Тестирования на всех уровнях системы
- Тестирования разными методами
- Тестирования из всех точек

Проведены учебные рассылки писем с вредоносным содержанием

- Подтверждена гипотеза о необходимости изоляции контуров системы

Разработать и предложить возможные сценарии реализации риска ограничение потребителя а также предложения по возможным мерам, направленным на сокращение вероятности и последствий реализации такого риска.

Предложить меры, направленные на невозможность реализации следующего сценария:

- Злоумышленник понял как работает ИСУ, понял какую команду нужно дать на ПУ для ограничения потребителя. Написал скрипт, который в радиоэфире находит ПУ и направляет на него команду на отключение реле
- Злоумышленник ездит на авто рядом с МКД и отключает нагрузку путем подачи команд на ограничение потребителя



СПАСИБО ЗА ВНИМАНИЕ!

