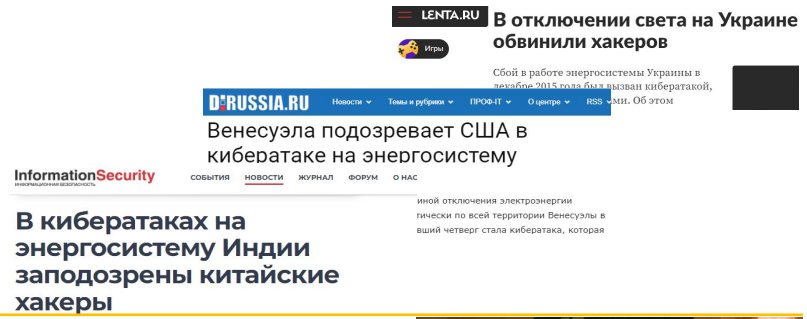
Предпосылки возникновения вопроса 2015-2016 г.

Актуальный нарушитель

Возникновение постепенный переход угроз из ряда «гипотетических» в практическую плоскость



Потенциальный ущерб

Киберфизический характер последствий

Критические уязвимости

Большое количество уязвимостей, обусловленное длительным периодом эксплуатации оборудования и сложностью вывода на обслуживание

ООО «Башкирэнерго»

Обеспечение безопасности в ходе жизненного цикла ЗОКИИ на примере электросетевой компании

14 февраля 2024 года

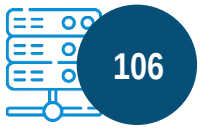
Янборисов Павел Сергеевич
Первый заместитель начальник департамента ИБ

Описание объекта защиты после 2017 года

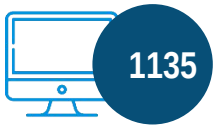
Объект защиты представлен территориально распределенными системами диспетчерского управления.

187-ФЗ
ЗОКИИ

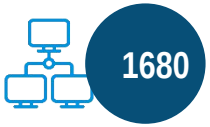
Масштаб объекта защиты



Сервера



Компьютеры



Сеть

АСУ ТП
Электроподстанции

АСУ ТП
РП/ТП

Перечень типовых ЗОКИИ.

Наименование объекта	Тип	Категория	Значимость	Количество
Автоматизированная система диспетчерского управления ООО «Башкирэнерго»	**АСУ**	II	**Социальная**	**1**
Автоматизированная система диспетчерского управления производственного отделения ООО «Башкирэнерго»	**АСУ**	II	**Социальная**	**10**

- ✓ **Выделение ЗОКИИ исходя из понимания процесса диспетчерского управления, с учётом зон ответственности диспетчерских пунктов.**
- ✓ **Учёт степени автономности и самодостаточности системы.**

Подход при реализации требований на этапах жизненного цикла

ТЗ

- Учтены требования к программным\программно-аппаратным средствам;
- Постановка целей и задач в соответствии с приказом ФСТЭК России от 25 декабря 2017 г. № 239;

Проектирование

- Разработаны типовые решения для создаваемых\модернизируемых систем;
- Учтена унификация и приоритет на встроенные механизмы ОБИ;

Внедрение

- Требования ОБИ контролируются на этапе проектной и исполнительной документации;
- Встраивание объектовых СЗИ в структуру коллективных СЗИ;

Ввод

- Оценка соответствия СЗИ, требованиям ОБИ;
- Анализ защищённости объекта в соответствии с Методикой по оценке защищённости (НКЦКИ);

Эксплуатация

- Ежегодные контроли (МОЗ\Аудит);
- Информирование персонала о новых УБИ, система обучения персонала;
- Корректирование мер ОБИ в соответствии с рекомендациями ФСТЭК России и НКЦКИ

Вывод

- Хранение режимных параметров и данных технологического процесса в течение установленного периода времени;
- Хранение документации в соответствии со сроками хранения номенклатуры дел;

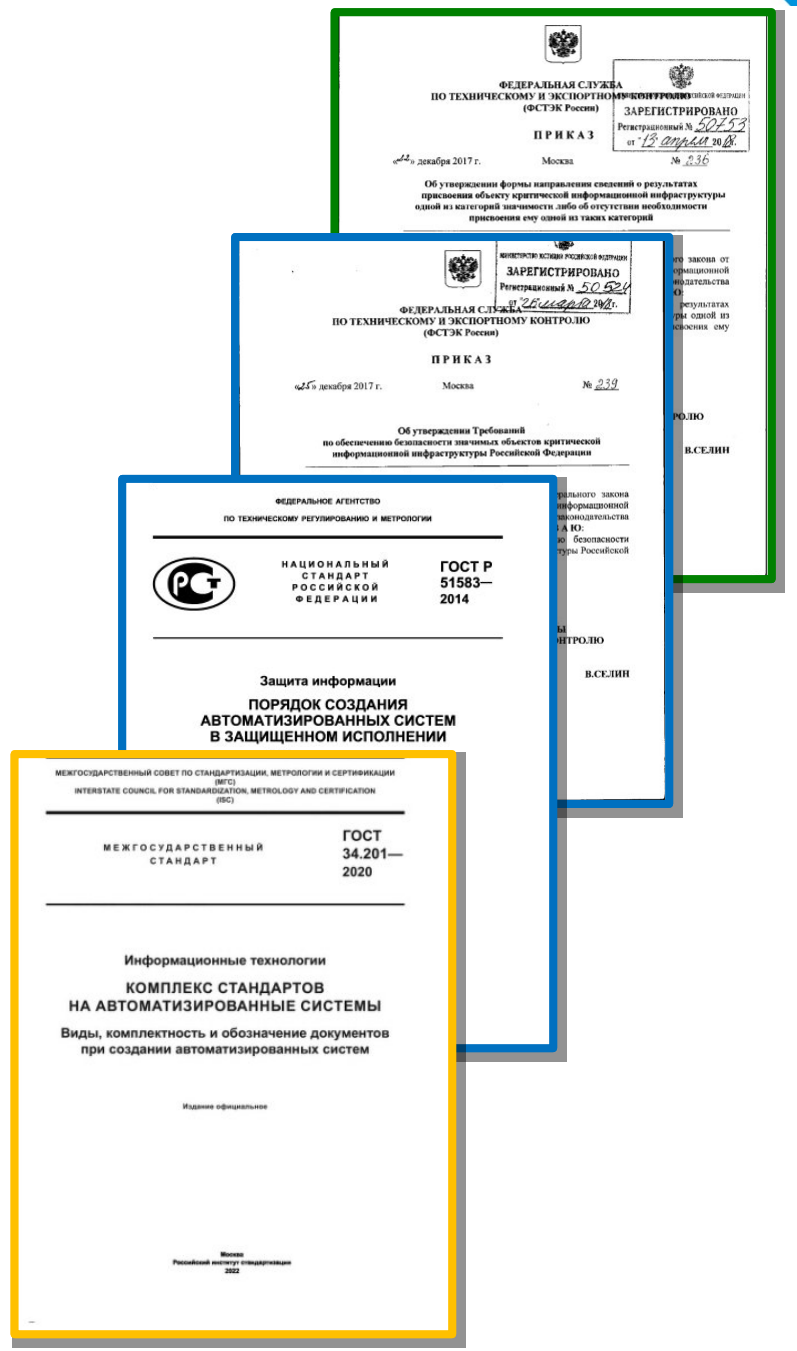
✓ **В соответствии с ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении».**

Техническое задание

- Общие сведения;
- Цели и назначение создания автоматизированной системы;
- Характеристика объектов автоматизации;

- Требования к автоматизированной системе;
- Состав и содержание работ по созданию автоматизированной системы;
- Порядок разработки автоматизированной системы;
- Порядок контроля и приемки автоматизированной системы;
- Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу автоматизированной системы в действие;

- Требования к документированию.



Проектирование

Моделирование угроз

1. Банк угроз ФСТЭК России
2. Разработка модели нарушителей
3. Определение состава актуальных угроз

Выбор мер защиты

1. Выбор базового набора мер в соответствии с категорией значимости
2. Адаптация базового набора и дополнение

Выбор модели защиты

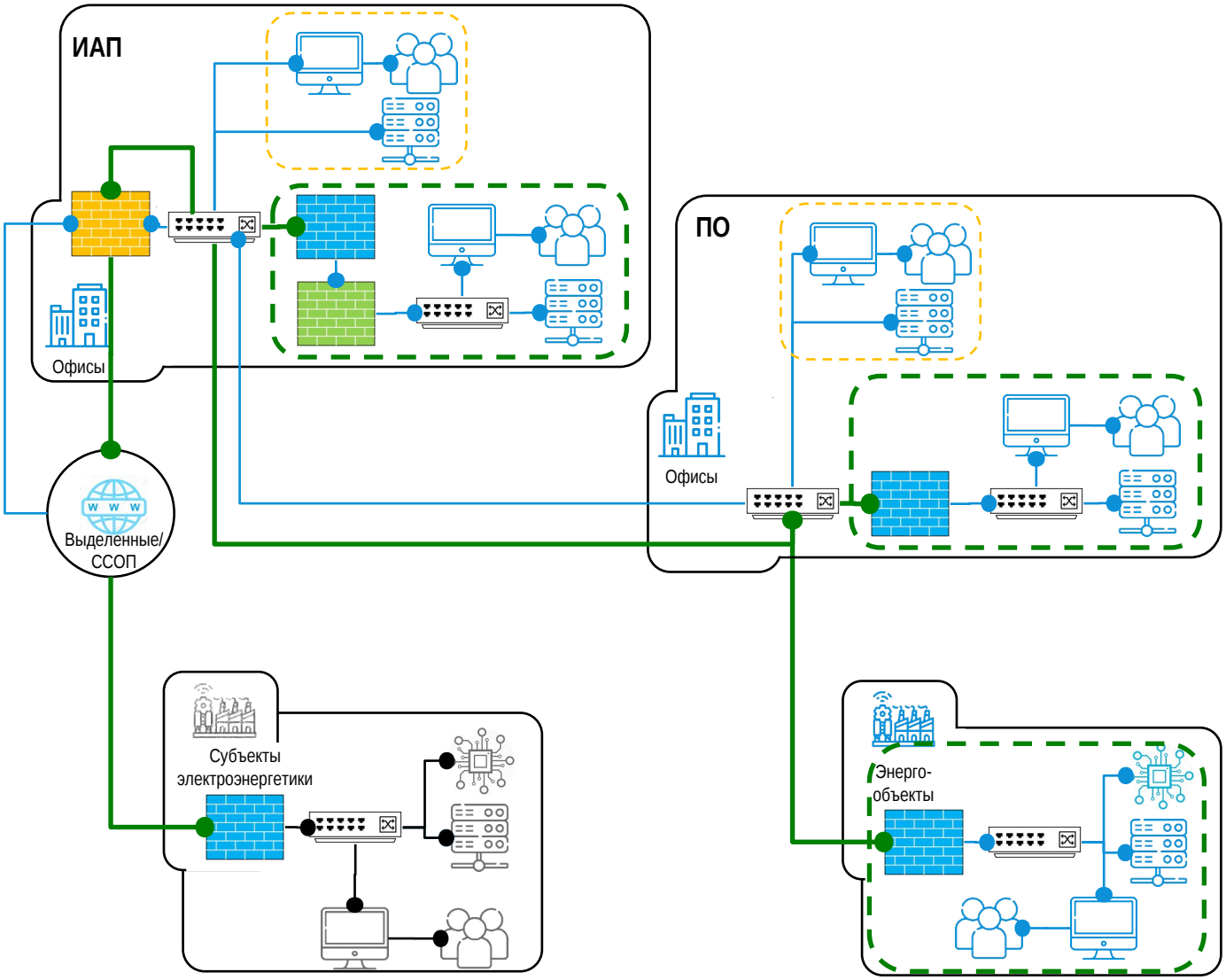
1. Определение состава организационных и технических мер защиты
2. Декомпозиция мер на подсистемы

Определение средств защиты

1. Декомпозиция подсистем на классы решений
2. Выбор средств защиты информации

✓ **Выбор модели защиты и средств защиты основан на анализе множества вариантов моделей защиты методом взвешенной суммы критериев.**

Типовые решения



ЛЕГЕНДА

- МСЭ Периметра Компании
- МСЭ Периметра ЗОКИИ
- МСЭ Периметра площадки
- Сетевое оборудование
- Сервера
- АРМы
- Контроллеры
- Пользователи
- Корпоративный сегмент
- Технологический сегмент
- Защищённая сеть
- Технологические\выделенные сети

✓ **Организация защищённой сети передачи данных, с применением существующей инфраструктуры**

Внедрение

Подсистемы	2019	2020	2021	2022	2023	2024	2025
Подсистема анализа защищенности							
Подсистема управления событиями ИБ							
Подсистема антивирусной защиты							
Подсистема межсетевого экранирования и обнаружения вторжений							
Подсистема защиты каналов связи							
Подсистема двухфакторной аутентификации работников							
Подсистема управления PKI							
Подсистема обучения персонала							
Подсистема управления ИБ (GRC)							

Ввод

- Предварительные испытания;
- Опытная эксплуатация;
- Анализ уязвимостей и принятие мер по их устранению;
- Приемочные испытания.

ГОСТ Р 59792- 2021
Виды испытаний автоматизированных систем

Эксплуатация

- *Планирование мероприятий по обеспечению безопасности значимого объекта;*
  - **Ежегодное планирование мероприятий по ОБИ и отчётность.**
- *Анализ угроз безопасности информации;*
  - **Отслеживание состава, архитектуры ЗОКИИ, мониторинг БДУ, сроков действия сертификатов.**
- Управление подсистемой безопасности значимого объекта;
  - **Распределение и закрепление функций и обязанностей по ОБИ на уровне приказов и ДИ.**
- Управление конфигурацией значимого объекта и его подсистемой безопасности;
  - **Контроль и согласование изменений, оценка их влияния на объект.**
- *Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта;*
  - **Утверждение и отработка плана реагирования на КИ, в соответствии с требованиями НКЦКИ.**
- *Обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта;*
  - **Резервирование чувствительных компонентов, отработка DRP.**
- *Информирование и обучение персонала значимого объекта;*
  - **Внедрение системы первичных, периодических и вводных инструктажей.**
- *Контроль за обеспечением безопасности значимого объекта.*
  - **Контроль, мониторинг, анализ защищённости.**

СПАСИБО ЗА ВНИМАНИЕ

Янборисов Павел Сергеевич
Первый заместитель начальник департамента ИБ ООО «Башкирэнерго»
E-mail:yanborisovps@bashkirenergo.ru
Тел.:8-919-603-45-60