ООО «Башкирэнерго»

Опыт создания систем безопасности значимых объектов КИИ

30 марта 2023 года

Павленко Тимур Марсович
Начальник департамента
информационной безопасности

Описание объекта защиты

Критический процесс – диспетчерское управление

Объект защиты –территориально распределенные автоматизированные системы диспетчерского управления.

11
ЗОКИИ

Наименование	Категория
АСДУ	II

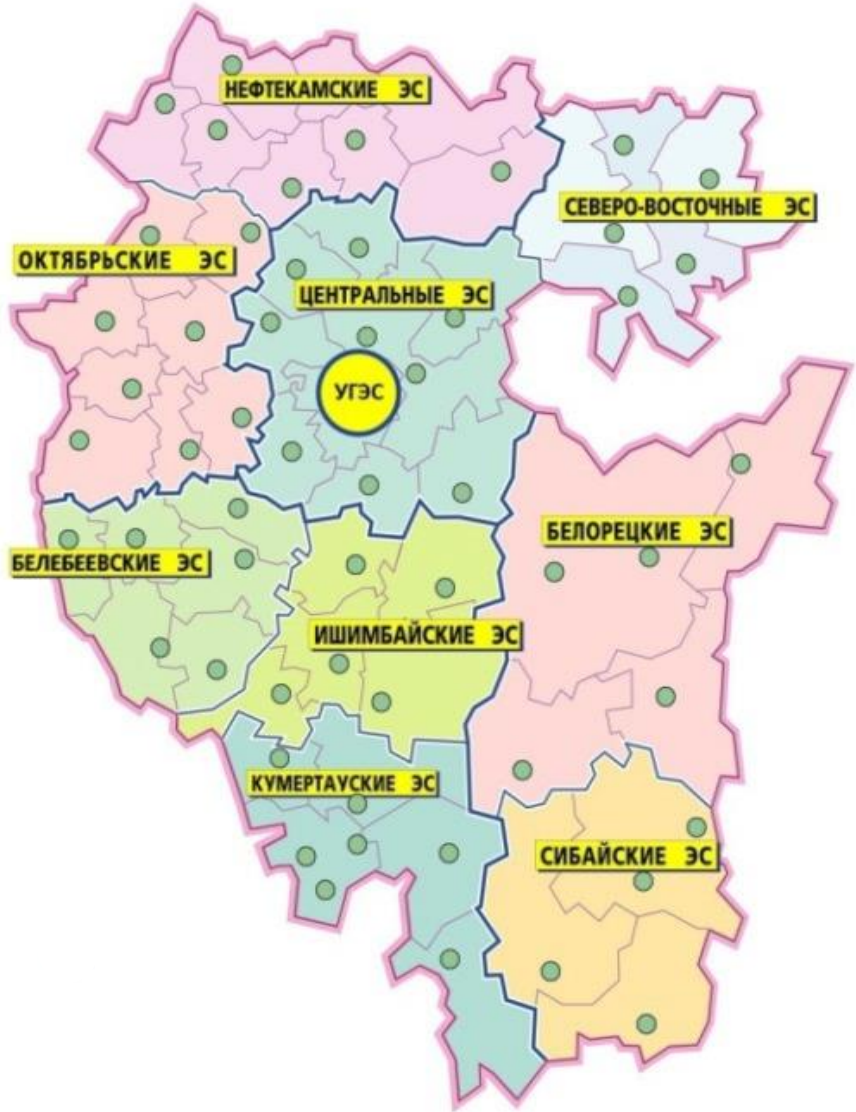
106
Сервера

1135
Компьютеры

6896
Сеть

558
АСУ ТП ПС

468
АСУ ТП РП/ТП



- ✓ **ЗОКИИ определены на основании процесса диспетчерского управления, с учётом зон ответственности диспетчерских пунктов.**
- ✓ **При этом учитывались степень автономности и самодостаточности системы.**

Этапы реализации 187-ФЗ

Этап	Особенности реализации
Определение объектов КИИ	Для удобства администрирования и контроля реализации требований законодательства было принято решение о привязке объектов КИИ к внедряемой 2-х уровневой модели ОТУ
Категорирование объектов КИИ	Категория АСДУ присваивалась по критерию социальная значимость, а именно – территория, на которой возможно нарушение обеспечения жизнедеятельности
Обследование ЗОКИИ	Работы выполнялись собственными силами. АСДУ рассматривалась как набор множества объектов.
Проектирование СОБИ ЗОКИИ	СОБИ ЗОКИИ рассматривалась как составная часть общей СЗИ. Разработан эскизный проект СОБИ ЗОКИИ
Внедрение СОБИ ЗОКИИ	Модернизация подсистем информационной безопасности велась параллельно с формированием эскизного проекта СОБИ ЗОКИИ. При выборе технических решений предпочтение отдается российским производителям.

Цель:

- **Минимизировать угрозы, направленные на нарушение функционирование АСДУ.**
- **Обеспечить устойчивое функционирование АСДУ при проведении компьютерных атак.**

Этапы СОБИ ЗОКИИ

Техническое задание

- Учтены требования к программным\программно-аппаратным средствам;
- Постановка целей и задач в соответствии с приказом ФСТЭК России от 25.12.2017 г. № 239;

Проектирование

- Разработаны типовые решения для создаваемых\модернизируемых систем;
- Учтена унификация и приоритет на встроенные механизмы ОБИ;
- При выборе проектных решений рассматривались только российские системы ОБИ;

Внедрение

- Требования ОБИ контролируются на этапе рабочей 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 из эксплуатации

- 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».**

Проектирование комплексной системы ОБИ ЗОКИИ

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

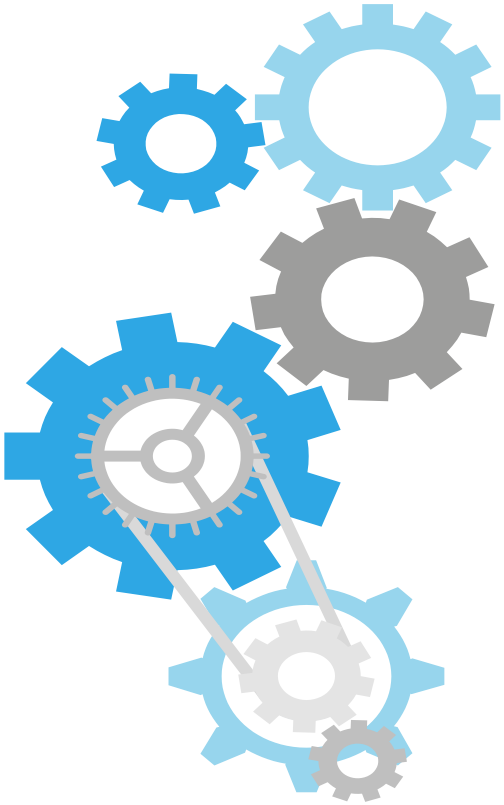
1. Определение состава организационных и технических мер защиты
2. Декомпозиция мер на подсистемы

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.**

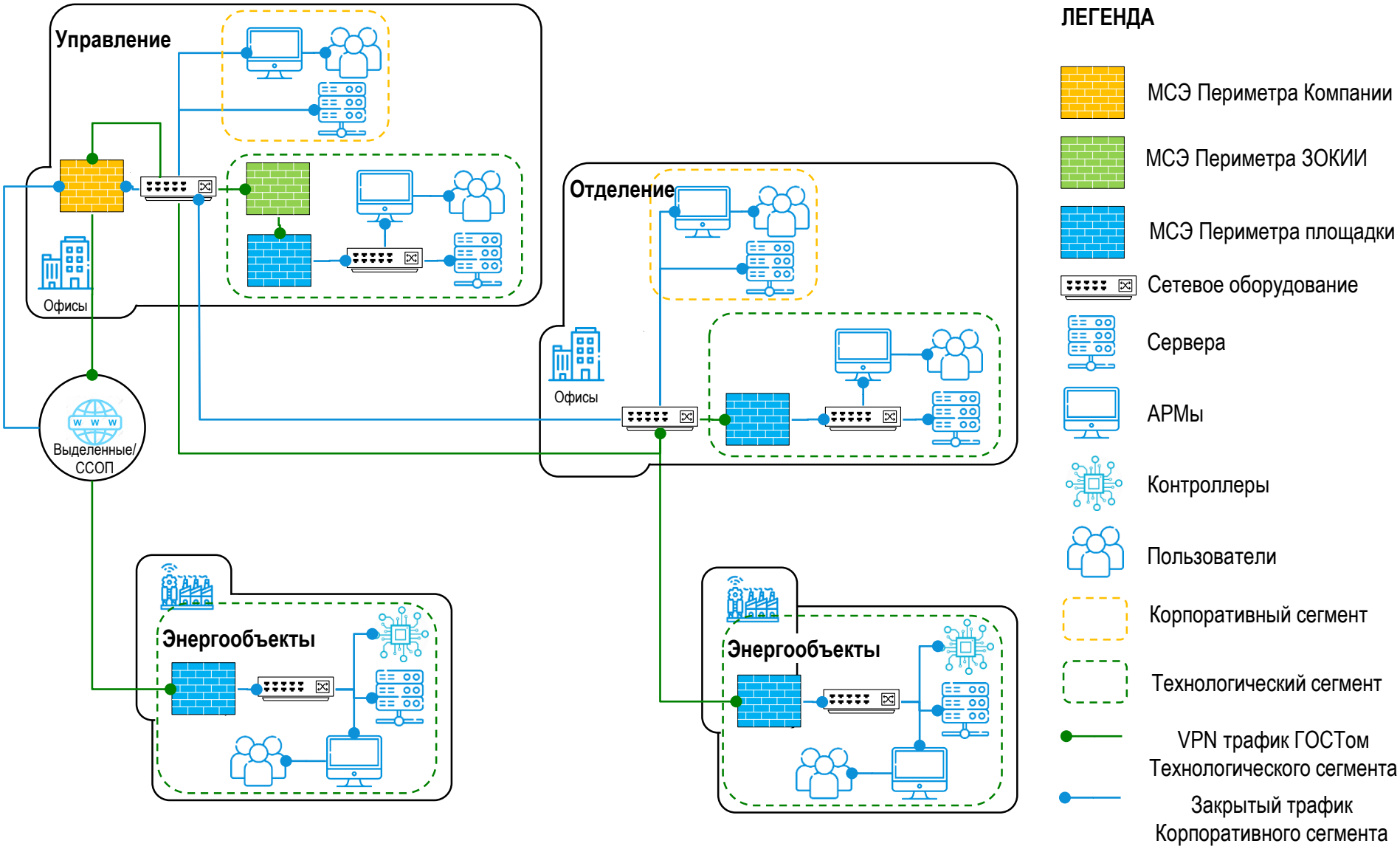
Состав комплексной системы ОБИ ЗОКИИ



Наименование подсистемы	Реализуемые меры
Подсистема управления доступом	ИАФ, УПД, ОПС, АУД, ЗИС, УКФ
Подсистема антивирусной защиты	АВЗ, ЗНИ, ЗНИ, ОЦЛ, АУД, ЗИС
Подсистема анализа защищенности	АУД
Подсистема межсетевого экранирования и обнаружения вторжений	ЗИС, УПД, СОВ, АУД
Подсистема управления событиями ИБ	АУД, ИНЦ
Подсистема защиты каналов связи	ЗИС, ИАФ, АУД
Подсистема резервирования и обеспечения отказоустойчивости	ОДТ, ДНС

✓ **Дополнительно к указанному перечню, запланировано обучение работников и внедрение GRC**

Защита технологического сегмента на примере подсистем МСЭ\VPN



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

Развитие подсистем информационной безопасности

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

О госконтроле.

Постановление Правительства РФ от 17 февраля 2018 г. № 162 “Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации”.

Ключевые вехи

1. Информирование субъекта КИИ о включении план – информационное письмо;
2. Уведомление субъекта КИИ о начале проверки – письмо с копией приказа, при желании и возможности очная встреча;
3. Подготовка к проверке – организация рабочих мест, подготовка документов и объектов;
4. Проверка – Акт проверки, предписание;
5. Результат проверки – План устранения нарушений;

Оценка

- общих сведений о субъекте КИИ
- состояния системы безопасности ЗОКИИ и организации работ по обеспечению безопасности ЗОКИИ
- сил обеспечения безопасности ЗОКИИ
- реализации задач мониторинга и контроля безопасности ЗОКИИ
- организационно-распорядительных документов по обеспечению безопасности ЗОКИИ
- организации работ по обеспечению функционирования системы безопасности ЗОКИИ
- достаточности и эффективности применяемых мер по обеспечению безопасности ЗОКИИ
- сведений о ЗОКИИ
- правильности внедрения средств защиты информации
- достаточности применяемых средств защиты информации
- организационных мер по обеспечению безопасности ЗОКИИ
- управления доступом, а также идентификации и аутентификации пользователей
- системы защиты от угроз, связанных с использованием ресурсов сети «Интернет» и электронной почты
- защиты периметра ЗОКИИ
- антивирусной защиты и безопасной работы со съемными машинными носителями информации на ЗОКИИ

План устранения нарушений формируется по всем выявленным нарушениям и рекомендациям.

По итогам реализации плана устранения нарушений необходимо направить во ФСТЭК России отчет с подтверждающими документами.

Спасибо за внимание

Тимур Павленко
pavlenkotm@bashkirenergo.ru