

ООО НПП «ЭСН»

**СТРОИТЕЛЬСТВО ВОДОГРЕЙНОЙ КОТЕЛЬНОЙ 400
ГКАЛ/ЧАС НА ТЕРРИТОРИИ ИВАНОВСКОЙ ТЭЦ-2**

(878.2023)

Перечень заданий на разработку разделов проекта, связанных с созданием
системы

878.2023-АСУ ТП.В3

Том 42

<i>Инв № подп.</i>	<i>Подп. и дата</i>	<i>Бланк инв. №</i>	<i>Инв № фубл.</i>	<i>Подп. и дата</i>

Содержание

Перечень заданий на разработку разделов проекта, связанных с созданием системы.....	3
Перечень сокращений	7
Перечень терминов	8

Перечень заданий на разработку разделов проекта, связанных с созданием системы

№	Наименование задания	Назначение задания	Дата выдачи	Срок выполнения работ
1	Разработка раздела «Информационная безопасность» в составе проекта автоматизации водогрейной котельной тепловой мощностью 400 Гкал/ч	Обеспечение комплексной защиты автоматизированной системы управления технологическим процессом (АСУ ТП) водогрейной котельной от актуальных угроз безопасности информации и несанкционированного доступа. Данный раздел предназначен для реализации мер и средств информационной безопасности (ИБ) на объекте, гарантирующих защиту критической информационной инфраструктуры котельной, устойчивость её работы и соответствие обязательным требованиям законодательства РФ. Разработка раздела ИБ позволит предотвратить киберинциденты, защитить технологические процессы от неправомерных действий, а также обеспечить безопасное функционирование котельной в целом.	19.08.2025	В течение 60 рабочих дней со дня представления Заказчиком исходных данных. Срок может быть сдвинут соразмерно сроку задержки представления необходимых данных от Конечного Заказчика.

Инв № подп.	Подп. и дата

Разработку раздела ИБ произвести в соответствии со следующими документами:

- Требования Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ;
- Приказ от 14 марта 2014 г. N 31 Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды;

Обеспечить в рамках выполнения комплекса работ выполнение работ по информационной безопасности в соответствии с:

- 99-ФЗ "О лицензировании отдельных видов деятельности" Статья 12. Перечень видов деятельности, на которые требуются лицензии - деятельность по технической защите конфиденциальной информации.
- Постановлением Правительства РФ N 79 "О лицензировании деятельности по технической защите конфиденциальной информации"

При осуществлении лицензируемого вида деятельности лицензированию подлежат

Изм.	Лист	№ докум.	Подп.	Дата	878.2023-АСУ ТП.В3	Лист
						3

- работы и услуги по проектированию в защищенном исполнении средств и систем информатизации;
- услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

Требования к информационной безопасности КИИ 3 категории при проектировании автоматизированного объекта водогрейной котельной 400 Гкал/час

1. Общие требования:

- Классификация объекта: КИИ 3 категории, согласно приказу Минэнерго РФ от 27.11.2020 № 838.
- Соблюдение законодательства: Требования ФЗ-187 "О безопасности критической информационной инфраструктуры" и других нормативно-правовых актов, регулирующих информационную безопасность КИИ.
- Анализ рисков: Проведение комплексного анализа рисков с учетом специфики объекта и потенциальных угроз.
- Документация: Разработка и ведение необходимой документации, включая политику информационной безопасности, инструкции, регламенты, планы реагирования на инциденты.
- Обучение персонала: Обучение персонала по вопросам информационной безопасности, включая проведение регулярных тренингов.

2. Требования к физической защите:

- Ограждение и доступ: Обеспечение физической защиты котельной и ее инфраструктуры от несанкционированного доступа.
- Контроль доступа: Реализация системы контроля доступа (СКУД) в помещениях котельной, где расположены элементы КИИ.
- Видеонаблюдение: Установка системы видеонаблюдения с архивированием данных и возможностью удаленного доступа.
- Сигнализация: Реализация системы охранной сигнализации с подключением к пульту централизованного наблюдения.

3. Требования к защите информации:

Инв № подп.	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата	878.2023-АСУ ТП.В3	Лист
						4

- Аутентификация и авторизация: Реализация надежных механизмов аутентификации и авторизации пользователей системы КИИ.
- Разграничение доступа: Применение принципа наименьших привилегий при настройке доступа пользователей к системе КИИ.
- Шифрование: Использование криптографических алгоритмов шифрования данных при передаче по сети и хранении на носителях.
- Журналирование: Включение функции журналирования событий с временными метками и регистрацией действий пользователей.
- Противодействие вредоносному ПО: Внедрение комплексных мер по защите от вредоносного ПО, включая антивирусное ПО, системы обнаружения вторжений, использование систем предотвращения вторжений.

4. Требования к сетевой безопасности:

- Использование изолированных сетей: Разделение сети КИИ от корпоративной сети.
- Использование межсетевых экранов: Установка и настройка межсетевых экранов для ограничения доступа к системе КИИ.
- Защита от DDoS-атак: Внедрение мер по противодействию DDoS-атакам.
- Протоколирование сетевых событий: Включение функции журналирования сетевых событий в системе КИИ.

5. Требования к защите программного обеспечения:

- Использование сертифицированного ПО: Применение сертифицированного ПО для КИИ.
- Регулярные обновления ПО: Регулярная проверка и установка обновлений ПО для устранения уязвимостей.
- Контроль целостности ПО: Применение механизмов контроля целостности ПО для предотвращения несанкционированных модификаций.

6. Требования к резервному копированию и восстановлению:

- Резервное копирование данных: Реализация механизмов резервного копирования данных КИИ.
- Тестирование восстановления: Регулярное тестирование процессов восстановления данных.
- Хранение резервных копий: Обеспечение безопасности хранения резервных копий данных.

7. Требования к реагированию на инциденты:

Инв № подп.	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата	878.2023-АСУ ТП.В3	Лист

- Планы реагирования на инциденты: Разработка и реализация планов реагирования на инциденты безопасности.
- Команда реагирования: Формирование команды реагирования на инциденты.
- Информирование заинтересованных сторон: Определение процедур информирования заинтересованных сторон в случае инцидента.

8. Требования к мониторингу и контролю:

- Системы мониторинга: Применение систем мониторинга информационной безопасности для отслеживания событий и анализ рисков.
- Аудит безопасности: Регулярный аудит системы безопасности КИИ.

9. Специальные требования:

- Защита от взлома: Внедрение специальных мер по защите от взлома, в том числе использование двухфакторной аутентификации, усиление паролей, использование физических защитных средств.
- Защита от несанкционированного доступа: Внедрение мер по предотвращению несанкционированного доступа к системе КИИ.
- Защита от взлома и диверсий: Внедрение мер по защите от взлома и диверсий, в том числе использование систем обнаружения вторжений, повышение уровня безопасности сети.

Инв № подп.	Подп. и дата	Инв № подп.	Взамен инв. №	Инв № документа	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата	878.2023-АСУ ТП.В3	Лист
						6

Перечень сокращений

Сокращение	Расшифровка
АСУ ТП	Автоматизированная система управления технологическим процессом
ИБ	Информационная безопасность
КИИ	Критическая информационная инфраструктура
СКУД	Система контроля и управления доступом
ПО	Программное обеспечение
DDoS	Distributed Denial of Service (распределённая атака типа «отказ в обслуживании»)
РФ	Российская Федерация
ФЗ	Федеральный закон

Инв № подп.	Подп. и дата	Подп. и дата	Инв № подп.

Изм.	Лист	№ докум.	Подп.	Дата	Лист
					878.2023-АСУ ТП.В3

Перечень терминов

Термин	Расшифровка
Автоматизированная система управления технологическим процессом (АСУ ТП)	Организационно-техническая система, обеспечивающая автоматическое и автоматизированное управление технологическим процессом, включающая технические средства, программное обеспечение и персонал.
Информационная безопасность (ИБ)	Состояние защищённости информации, при котором обеспечиваются её конфиденциальность, целостность и доступность.
Критическая информационная инфраструктура (КИИ)	Информационные системы, сети и ресурсы, имеющие важное значение для функционирования государства, экономики и безопасности.
Система контроля и управления доступом (СКУД)	Аппаратно-программный комплекс для идентификации, аутентификации и управления доступом персонала в защищённые зоны.
Программное обеспечение (ПО)	Совокупность программ и программных средств, используемых для функционирования автоматизированных систем.
DDoS-атака	Тип кибератаки, при которой злоумышленники перегружают систему множеством запросов, вызывая отказ в обслуживании.
Федеральный закон (ФЗ)	Нормативно-правовой акт Российской Федерации, обладающий высшей юридической силой после Конституции РФ.

<i>Инв № подп.</i>	<i>Подп. и дата</i>	
	<i>Инв № подп.</i>	<i>Подп. и дата</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>
<i>Подп.</i>	<i>Дата</i>	

Лист регистрации изменений

878.2023-АСУ ТП.В3

Лист

9