

ПАСПОРТ

**АСУ ТП Электролизного участка Кобальтового отделения Цеха электролиза никеля №2**

(АСУ ТП Электролизного участка кобальт 3000)

Обозначение документа: \_\_\_

Введен впервые.

Дата введения: \_\_.\_\_.20\_\_

**Содержание**

[1 Общие сведения об АСУ ТП 5](#_Toc24976468)

[1.1 Владелец АСУ ТП и эксплуатирующая организация 5](#_Toc24976469)

[1.2 Наименование АСУ ТП 5](#_Toc24976470)

[1.3 Назначение АСУ ТП 5](#_Toc24976471)

[1.4 Адреса размещения АСУ ТП 5](#_Toc24976472)

[1.5 Владелец АСУ ТП 5](#_Toc24976473)

[1.6 Состав информации, обрабатываемой в АСУ ТП 5](#_Toc24976474)

[1.7 Классификация опасности 5](#_Toc24976475)

[1.8 Категорирование АСУ ТП как объекта критической информационной инфраструктуры 6](#_Toc24976476)

[1.8.1 Критические технологические процессы 6](#_Toc24976477)

[1.8.2 Категорирование АСУ ТП 6](#_Toc24976478)

[1.9 Классификация АСУ ТП как КВО, ПОО, объекта, представляющего повышенную опасность для жизни и здоровья людей и для окружающей природной среды 7](#_Toc24976479)

[1.10 Организации, задействованные в обслуживании АСУ ТП 7](#_Toc24976480)

[1.11 Проектная и иная документация на АСУ ТП 7](#_Toc24976481)

[1.12 Режимы работы АСУ ТП 8](#_Toc24976482)

[2 Общие сведения о технологических процессах 9](#_Toc24976483)

[2.1 Наименование технологических процессов 9](#_Toc24976484)

[3 Описание архитектуры АСУ ТП 17](#_Toc24976485)

[3.1 Описание оборудования верхнего уровня 17](#_Toc24976486)

[3.2 Описание оборудования среднего уровня 18](#_Toc24976487)

[3.3 Описание оборудования нижнего уровня 19](#_Toc24976488)

[3.4 Описание сетевого оборудования 19](#_Toc24976489)

[3.5 Структурная схема АСУ ТП 19](#_Toc24976490)

[3.6 Описание взаимодействия с внешними АСУ и ИС 20](#_Toc24976491)

[3.7 Описание взаимодействия с сетями связи 20](#_Toc24976548)

[4 Перечень ключевого персонала и распределение функций по обеспечению безопасности 21](#_Toc24976549)

[4.1 Перечень ключевого персонала 21](#_Toc24976550)

[4.2 Распределение функций по обеспечению безопасности 21](#_Toc24976551)

[5 Описание мер по обеспечению безопасности 24](#_Toc24976552)

[5.1 Идентификация и аутентификация 24](#_Toc24976553)

[5.2 Управление доступом 24](#_Toc24976554)

[5.3 Ограничение программной среды 25](#_Toc24976555)

[5.4 Защита машинных носителей информации 25](#_Toc24976556)

[5.5 Аудит безопасности 25](#_Toc24976557)

[5.6 Антивирусная защита 25](#_Toc24976558)

[5.7 Предотвращение вторжений (компьютерных атак) 25](#_Toc24976559)

[5.8 Обеспечение целостности 25](#_Toc24976560)

[5.9 Обеспечение доступности 25](#_Toc24976561)

[5.9.1 Резервирование оборудования 25](#_Toc24976562)

[5.9.2 Резервное копирование и восстановление 26](#_Toc24976563)

[5.9.3 Наличие комплекта ЗИП 26](#_Toc24976564)

[5.9.4 Мониторинг технического состояния 26](#_Toc24976565)

[5.10 Защита технических средств и систем 26](#_Toc24976566)

[5.10.1 Меры физической защиты оборудования 26](#_Toc24976567)

[5.10.2 Бесперебойное электроснабжение 27](#_Toc24976568)

[5.11 Защита информационной (автоматизированной) системы и ее компонентов 27](#_Toc24976569)

[5.12 Планирование мероприятий по обеспечению безопасности 27](#_Toc24976570)

[5.13 Управление конфигурацией 27](#_Toc24976571)

[5.14 Управление обновлениями программного обеспечения 27](#_Toc24976572)

[5.15 Реагирование на инциденты информационной безопасности 27](#_Toc24976573)

[5.16 Обеспечение действий в нештатных ситуациях 28](#_Toc24976574)

[5.17 Информирование и обучение персонала 28](#_Toc24976575)

[Приложение 1. Структурная схема АСУ ТП 29](#_Toc24976576)

**Сокращения и обозначения**

|  |  |
| --- | --- |
| АО | Акционерное общество |
| АРМ | Автоматизированнное рабочее место |
| АСУ | Автоматизированная система управления |
| АСУ ТП | Автоматизированная система управления технологическими процессами |
| ГОК | Быстринский горно-обогатительный комбинат |
| ГРКБ | ООО «ГРК «Быстринское» |
| ЗИП | Запасные части, инструменты и принадлежности |
| ИС | Информационная система |
| КВО | Критически важный объект |
| КИИ | Критическая информационная инфраструктура |
| КИПиА | Контрольно-измерительные приборы и автоматика |
| ОС | Операционная система |
| ОФ | Обогатительная фабрика |
| ПВТ | Площадка вспомогательных цехов |
| ПЛК | Программируемый логический контроллер |
| ПО | Программное обеспечение |
| ПОО | Потенциально опасный объект |
| РФ | Российская Федерация |
| СУБД | Система управления базами данных |
| ТСПД | Технологическая сеть передачи данных |
| ФЗ | Федеральный закон |
| ФСТЭК | Федеральная служба по техническому и экспортному контролю |
| ЦОД | Центр обработки данных |
| SCADA | Supervisory Control And Data Acquisition, программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления |
| SQL | Structured Query Language, «язык структурированных запросов» |
| USB | Universal Serial Bus, универсальная последовательная шина |

# Общие сведения об АСУ ТП

## Владелец АСУ ТП и эксплуатирующая организация

Собственник АСУ ТП:ООО «ГРК «Быстринское»

Эксплуатирующая организация: ООО «ГРК «Быстринское»

## Наименование АСУ ТП

Полное наименование: АСУ ТП Электролизного участка Кобальтового отделения Цеха электролиза никеля №2

Краткое наименование: (АСУ ТП Электролизного участка кобальт 3000)

## Назначение АСУ ТП

АСУ ТП обеспечивает управление технологическими процессами

## Адреса размещения АСУ ТП

Забайкальский край, Газимуро-Заводской район, село Газимурский завод, площадка Быстринского ГОК.

## Владелец АСУ ТП

Владельцем АСУ ТП является Начальник цеха электролиза никеля.

## Состав информации, обрабатываемой в АСУ ТП

Состав обрабатываемой информации:  
- показания контрольно-измерительных приборов, аналоговых и дискретных;  
- сигналы дискретного управления;  
- сигналы аналогового регулирования;  
- управляющие команды от операторов;  
- тренды показаний контрольно-измерительных приборов;  
- архивы событий и действий операторов.

## Классификация опасности[[1]](#footnote-1)

Класс опасности опасных производственных объектов: III .

## Категорирование АСУ ТП как объекта критической информационной инфраструктуры[[2]](#footnote-2)

### Критические технологические процессы

АСУ ТП обеспечивает автоматизацию следующих технологических процессов:

- электролиз кобальта.

Состав показателей критериев значимости, по которым технологические процессы являются критическими, указан в таблице Таблица 1.

Таблица 1 – Отнесение технологических процессов к критическим[[3]](#footnote-3)

|  |  |  |
| --- | --- | --- |
| **№** | **Показатели** | |
|  | ***Процесс*: Электролиз кобальта** | |
|  | Социальная значимость | 1 |
|  | Экономическая значимость | 2 |
|  | Экологическая значимость | 3 |

### Категорирование АСУ ТП

АСУ ТП функционирует в сфере металлургической промышленности.

АСУ ТП как объекту КИИ категория значимости не присваивается.

Для АСУ ТП как объекта критической информационной инфраструктуры определяются значения следующих показателей:

1. **Показатель социальной значимости**

Возможно причинение ущерба жизни и здоровью людей, оцениваемое:

а) в количестве людей, жизни и здоровью которых возможно причинение ущерба (КЛ), человек.

Таблица 2 - Определение значений показателей и категорий значимости КИИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Показатель** | | **Возможности** | | |
| 1. **Социальная значимость** | | | | | | |
|  | Количество людей (КЛ), жизни и здоровью которых возможно причинение ущерба | |  | | |
| **Значения показателей и оценка** | | | | | | |
| Категория не присваивается  (КЛ = 0) | | III категория  (1 <= КЛ <= 50) | | II категория  (50 < КЛ <=500) | I категория  (500 < КЛ) | |
| - | | **√** | | - | - | |

Категория АСУ ТП как объекта КИИ: III.

## Классификация АСУ ТП как КВО, ПОО, объекта, представляющего повышенную опасность для жизни и здоровья людей и для окружающей природной среды[[4]](#footnote-4)

В случае нарушения штатного режима функционирования АСУ ТП или незаконного вмешательства в процессы функционирования АСУ ТП возможно возникновение чрезвычайной ситуации, при этом:

* + количество людей, погибших или получивших ущерб здоровью, составляет не более 3 человек.

В соответствии с постановлением Правительства РФ от 21.05.2007 № 304  
«О классификации чрезвычайных ситуаций природного и техногенного характера» это относится к чрезвычайной ситуации **локального характера**.

Класс защищенности АСУ ТП: К3 (третий).

## Организации, задействованные в обслуживании АСУ ТП

В обслуживании АСУ ТП задействованы только ответственные подразделения и должностные лица ГРКБ, указанные в пункте 4 настоящего документа. Внешние организации в процессах обслуживания АСУ ТП не задействованы..

## Проектная и иная документация на АСУ ТП

Перечень документации на АСУ ТП приведен в Таблице 3.

Таблица 3 - Перечень документации (проектная, эксплуатационная, организационно-распорядительная)

| № п/п | Наименование | Шифр | Разработчик | Год |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Режимы работы АСУ ТП

АСУ ТП функционирует в непрерывном, круглосуточном режиме в соответствии с непрерывным характером и режимом ведения технологического процесса ..

# Общие сведения о технологических процессах

## Наименование технологических процессов

АСУ ТП обеспечивает автоматизацию следующих технологических процессов:

-электролиз кобальта..

Описание процессов каждого узла, а также состав технологического оборудования, управляемых и контролируемых параметров указаны в Таблица 4.

Таблица 4 – Описание процессов и состав технологического оборудования

| **№** | **Наименование технологического оборудования** | **Наименование оборудования (АСУ ТП)[[5]](#footnote-5)** | **Контролируемые параметры** | **Регулируемые параметры** | **Описание процессов** |
| --- | --- | --- | --- | --- | --- |
|  |  | | | | |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |



# Описание архитектуры АСУ ТП

АСУ ТП имеет трехуровневую структуру:

* + уровень операторского управления (верхний);
  + уровень автоматического управления (средний);
  + уровень ввода (вывода) данных исполнительных устройств (нижний).

## Описание оборудования верхнего уровня

К оборудованию верхнего уровня относятся:

* + 2 сервера АСУ ТП;
  + 2 АРМ операторов;
  + 1 инженерная станция;
  + 1 сервер системы управления базами данных (далее – СУБД).

Перечень оборудования верхнего уровня приведен в Таблице Таблица 5.

Таблица 5 – Перечень оборудования верхнего уровня

| № п/п | Назначение | Производитель | Сетевое имя | IP | Размещение | Установленное ПО |
| --- | --- | --- | --- | --- | --- | --- |
| **Серверы АСУ ТП** | | | | | | |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **АРМ операторов** | | | | | | |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Инженерные станции разработки** | | | | | | |
|  |  |  |  |  |  |  |
| **Серверы БД** | | | | | | |
|  |  |  |  |  |  |  |

Оборудование не входит в корпоративный домен Active Directory. Сервер СУБД обеспечивает хранение технологических данных АСУ ТП, дальнейшую передачу данных внешним системам КГМК.  
Все оборудование подключено к ТСПД по технологии Ethernet. Взаимодействие оборудования верхнего уровня между собой осуществляется по протоколам TCP/IP.  
Серверы АСУ ТП осуществляют прием поступающей со среднего уровня (ПЛК) информации для ее последующей обработки и визуализации для оператора. Взаимодействие между серверами и ПЛК осуществляется по протоколу Modbus/TCP.  
Интерфейс операторам предоставляется посредством АРМ, визуализирующих информацию, поступающую с активного сервера АСУ ТП, предоставляющих возможность управления технологическим оборудованием и параметрами технологических процессов.  
Инженерная станция служит для ведения разработки проектов АСУ ТП для всех систем Кобальтового отделения ЦЭН-2..

## Описание оборудования среднего уровня

К оборудованию среднего уровня относятся:

* + ПЛК
  + .

Перечень оборудования среднего уровня приведен в таблице Таблица 6.

Таблица 6 – Перечень оборудования среднего уровня

| № п/п | Производитель | Модель | Кол-во | IP | Размещение | Примечание |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

ПЛК SE Modicon Quantum осуществляют сбор и первичную обработку информации, управление технологическим процессом, расчет и выработку воздействий на регулируемые органы электролизного участка в целом.  
Контроллеры Festo осуществляют управление клапанами технологического оборудования участка, управляются контролерами SE Modicon Quantum.  
Взаимодействие на уровне ПЛК осуществляется по протоколу Modbus/TCP.  
3.3 Описание оборудования нижнего уровня

## Описание оборудования нижнего уровня

К оборудованию нижнего уровня относятся контрольно-измерительные приборы и исполнительные механизмы, осуществляющие мониторинг, контроль и управление основным технологическим оборудованием участка.  
Состав контрольно-измерительных приборов включает:  
-манометры, датчики давления;  
-термометры;  
-уровнемеры;  
-расходомеры;  
-pH-метры;  
-датчики ОВП;  
-газоанализаторы;  
Состав исполнительных механизмов включает:  
-регулирующие и запорные клапаны;  
-клапаны электромагнитные, пневматические, соленоидные;  
-частотные приводы насосов, частотные преобразователи на двигателях насосов.  
Сбор информации с контрольно-измерительных приборов осуществляется на уровне аналоговых и цифровых сигналов на базе ПЛК SE Modicon Quantum. Управление клапанами осуществляется по сигналам ПЛК Festo, взаимодействие ПЛК с исполнительными механизмами реализовано посредством сухих контактов. Обмен сигналами между ПЛК SE Modicon Quantum и шкафами управления клапанами, оборудованием частотных приводов насосов осуществляется по протоколу Modbus/TCP.

## Описание сетевого оборудования

Перечень сетевого оборудования приведен в таблице 7.

Таблица 7 - Перечень сетевого оборудования

| № п/п | Производитель | Модель | Наименование | Кол-во | Размещение |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Структурная схема АСУ ТП

Структурная схема АСУ ТП представлена в Приложении 1.

## Описание взаимодействия с внешними АСУ и ИС

Описание взаимодействия АСУ ТП с внешними АСУ и ИС представлено в таблице Таблица 8.

Таблица 8 - Взаимодействие с внешними АСУ и ИС

| **№ п/п** | **Источник/ инициатор** | **Приемник** | **Протокол** | **Порт** | **Назначение** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Описание взаимодействия с сетями связи

АСУ ТП взаимодействует с технологической сетью передачи данных для приема-передачи информации..

# Перечень ключевого персонала и распределение функций по обеспечению безопасности

## Перечень ключевого персонала

Таблица 9 - Перечень ключевого персонала

|  |  |  |
| --- | --- | --- |
| № п/п | Функции | Структурные подразделения |
|  | Ответственность за функционирование технологического оборудования АО «Кольская горно-металлургическая компания» | Главный инженер - технический директор |
|  | Ответственность за функционирование технологического оборудования ЦЭН-2 | Главный инженер цеха электролиза никеля |
|  | Ответственность за функционирование технологического оборудования КО | Начальник кобальтового отделения |
|  | Ответственность за физическое функционирование контрольно-измерительного оборудования, управляющих устройств и автоматики | Отдел эксплуатации технических средств АСУ ТП |
|  | Ответственность за логическое функционирование автоматики | Отдел эксплуатации технических средств АСУ ТП |
|  | Ответственность за логическое функционирование серверов АСУ ТП и рабочих станций операторов | Отдел эксплуатации ПО АСУ ТП |
|  | Ответственность за логическое функционирование сетевого оборудования | Отдел эксплуатации технических средств АСУ ТП |
|  | Ответственность за обеспечение информационной безопасности | Отдел информационной безопасности;  Отдел эксплуатации ПО АСУ ТП |

## Распределение функций по обеспечению безопасности

Распределение функций по обеспечению безопасности АСУ ТП в текущей организационной структуре ГРКБ сформировано на основании следующих документов:

* Должностная инструкция главного инженера цеха электролиза никеля АО «Кольская ГМК»;
* Положение об управлении автоматизации АО «Кольская ГМК»;
* Положение об отделе организации ремонтов управления автоматизации АО «Кольская ГМК»;
* Должностная инструкция главного специалиста отдела автоматизации технологических процессов и производственных комплексов Управления автоматизации АО «Кольская ГМК»;
* Должностная инструкция главного специалиста группы развития систем промышленной автоматизации Управления автоматизации АО «Кольская ГМК»;
* Регламент взаимодействия отдела информационной безопасности департамента безопасности АО «Кольская ГМК» и отдела информационной безопасности Кольского филиала ООО «Норникель – общий центр обслуживания».

Таблица 10 - Распределений функций по обеспечению безопасности

| № п/п | Подразделение/ работник | Функции и обязанности |
| --- | --- | --- |
|  | Главный инженер цеха электролиза никеля | * Руководство организационно-профилактической работой по охране труда и промышленной безопасностью; * организация и проведение проверки автоматизированного рабочего места в цехе по уровню соответствия требованиям по охране труда и промышленной безопасности; * контроль за обеспечением оборудования повышенной опасности необходимой технической документацией, предусмотренной правилами безопасности и системами стандартов безопасности; * участие в разработке технической и технологической документации, направленной на обеспечение сохранности продукции; * разработка и осуществление мер защиты персонала и объектов цеха от чрезвычайных ситуаций и мероприятий, способствующих повышению устойчивости функционирования цеха в условиях чрезвычайных ситуаций; * разработка планов по ликвидации аварий в цехе |
|  | Управление автоматизации | * Технологическое сопровождение активов автоматизации технологических процессов и производственных комплексов; - техническое сопровождение функциональности средств КИПиА, а также производственных информационных систем; * техническое сопровождение программного обеспечения средств КИПиА и АСУ ТП; * организация и внедрение новых активов средств КИПиА и АСУ ТП; * контроль за исполнением и приемкой работ у внутренних и внешних исполнителей; * организация процессов создания, модернизации, списания и утилизации компонентов технических средств КИПиА и АСУ ТП; * контроль исполнения и закрытия инцидентов от пользователей, эксплуатирующих технические средства АСУ ТП; * контроль исполнения установленных сроков разрешения инцидентов |
|  | Главный специалист отдела автоматизации технологических процессов и производственных комплексов | * Осуществление контроля соблюдения принципа единой технической политики в области создания, разработки, проектирования, закупа, внедрения, монтажа, наладки, пуска и эксплуатации АСУ ТП и КИПиА; * контроль предварительных испытаний и проверки работоспособности АСУ ТП и КИПиА; * систематический анализ состояния средств измерения, промышленной автоматизации и программного обеспечения АСУ ТП и КИПиА; * проведение анализов неисправностей и отказов средств АСУ ТП и КИПиА, разработка корректирующих мероприятий; * выполнение функциональных обязанностей по охране труда и промышленной безопасности |
|  | Главного специалиста группы развития систем промышленной автоматизации | * Координация деятельности подрядных организаций в рамках исполнения договорных обязательств; * передача в эксплуатацию вновь создаваемых и модернизируемых средств АСУ ТП и КИПиА |
|  | Отдел организации ремонтов | * Планирование и выполнение технического обслуживания и ремонта систем промышленной автоматизации и систем противопожарной автоматики; * координация деятельности подрядных организаций в рамках исполнения договорных обязательств |
|  | Департамент безопасности | * Управление требованиями информационной безопасности на стадиях жизненного цикла ИТ-активов, информационных систем и компонентов ИТ-инфраструктуры, АСУ ТП (управление требованиями ИБ, управление проектами ИБ, анализ и контроль ИТ-проектов в части ИБ, управление документацией ИБ); * классификация информационных активов и оценка рисков информационной безопасности; * управление инцидентами ИБ (обнаружение, реагирование, расследование); * идентификация и классификация компонентов АСУ ТП; * оценка рисков ИБ АСУ ТП; * управление доступом к АСУ ТП; * управление инцидентами ИБ АСУ ТП; * внутренний аудит ИБ АСУ ТП; * обеспечение ИБ на стадиях жизненного цикла АСУ ТП; * защита АСУ ТП техническими средствами |

# Описание мер по обеспечению безопасности

## Идентификация и аутентификация

Идентификация и аутентификация на верхнем уровне осуществляются средствами SCADA Wonderware InTouch, а также ОС Windows. На уровне SCADA и на уровне ОС применяется ролевая система разграничения доступа, предусматривающая в общем случае роли, представленные в таблице 11..

Таблица 11 – Роли, использующиеся для эксплуатации АСУ ТП

|  |  |  |
| --- | --- | --- |
| № п/п | Роль | Назначение |
|  | Оператор | Единая учетная запись, которую используют все операторы, работающие с АСУ ТП. Аутентификация в данном случае осуществляется по паролю. Для УЗ, использующейся для входа в ОС, блокирование сеанса доступа в случае неактивности не осуществляется. Данное решение вызвано необходимостью постоянного отображения управляющей мнемосхемы на мониторах рабочих станций, а также потребностью в быстром реагировании операторов на отклонения параметров технологического процесса |
|  | Администратор | Единая учетная запись, которую используют работники Отдела эксплуатации ПО АСУ ТП и Отдела эксплуатации технических средств АСУ ТП, ответственные за администрирование АСУ ТП. Для данной учетной записи применяется аутентификация по паролю |

Идентификация и аутентификация на среднем уровне (при подключении к ПЛК со стороны SCADA-системы, при удаленном и локальном подключении администраторами АСУ ТП) не реализованы. Локальное подключение осуществляется со специализированных ноутбуков, используемых администраторами АСУ ТП.  
Идентификация и аутентификация при подключении к телекоммуникационному оборудованию реализованы при помощи единой общей учетной записи, которая устанавливается производителем оборудования, смена пароля не производится..

## Управление доступом

Предоставление доступа к АСУ ТП для операторов АСУ ТП осуществляется при назначении работника на соответствующую должность. Отдельные учетные записи не заводятся.  
Предоставление доступа к АСУ ТП для администраторов АСУ ТП осуществляется при назначении работника на соответствующую должность Отдела эксплуатации технических средств АСУ ТП или Отдела эксплуатации ПО АСУ ТП. После прохождения работником обучения, стажировки, дублирования, участия в противопожарных и противоаварийных тренировках и допуска к самостоятельной работе руководителем подразделения предоставляется доступ пользователю в отдельный документ в Lotus Notes, где хранятся пароли от учетных записей, используемых подразделением для доступа к компонентам АСУ ТП. Для отдельных компонентов всеми администраторами используется единый пароль. Регламент смены паролей отсутствует. Пароль меняется ОЭПО АСУ ТП в случае подозрения на его компрометацию.  
Доступ к АСУ ТП для работников внешних организаций не предоставляется..

## Ограничение программной среды

Ограничение программной среды обеспечивается штатными средствами ОС. Операторы АСУ ТП имеют ограниченные права, в том числе ограничена возможность установки компонентов программного обеспечения. Операторы АСУ ТП могут запускать стороннее ПО и его компоненты в том случае, если для этого не требуются права администратора..

## Защита машинных носителей информации

Ограничение использования машинных носителей информации обеспечивается штатными средствами ОС. Операторы АСУ ТП имеют ограниченные права, в том числе ограничена возможность подключения носителей информации к АРМ. USB-порты отключаются путем изменения значений ключей в реестре (regedit) Windows..

## Аудит безопасности

События безопасности, подлежащие регистрации, не определены. Параметры регистрации настроены «по умолчанию». Сроки хранения события безопасности не ограничены. Регистрация событий безопасности на АРМ операторов и сервере производится штатными средствами ОС, события безопасности записываются в журнал событий ОС. Помимо этого, регистрация событий безопасности производится программным обеспечением Wonderware InTouch..

## Антивирусная защита

На АРМ операторов в качестве средства антивирусной защиты применяется Kaspersky Endpoint Security 10.3.0.6294.  
На серверах в качестве средства антивирусной защиты применяется McAfee VirusScan Enterprise 8.8.  
На АРМ и серверах осуществляется регулярное обновление антивирусных баз..

## Предотвращение вторжений (компьютерных атак)

Средства обнаружения и предотвращения вторжений не применяются..

## Обеспечение целостности

Средства обеспечения целостности не применяются..

## Обеспечение доступности

### Резервирование оборудования

Горячее резервирование оборудования верхнего уровня реализуется следующим образом:  
-путем запуска идентичных проектов на двух АРМ операторов: при отказе какой-либо рабочей станции вся оперативная информация отображается на оставшейся;  
-за счет использования двух мониторов на каждом АРМ оператора;  
-за счет резервирования серверов АСУ ТП.  
Горячее резервирование оборудования среднего уровня реализуется путем установки двух идентичных процессорных модулей ПЛК с модулем синхронизации. Сбор, обработку оперативной информации, выдачу управляющих воздействий осуществляет контроллер, являющийся основным. Контроллер, являющийся резервным, синхронизирует свое состояние с основным через модули синхронизации. В случае отказа основного ПЛК его функции принимает на себя резервный. После восстановления, отказавший ПЛК принимает на себя функции резервного..

### Резервное копирование и восстановление

Создание резервных копий образов АРМ операторов и серверов осуществляется c помощью ПО AOMEI Backupper версии 1.4.  
Резервное копирование проектов, разработанных в ПО InTouch осуществляется вручную сотрудниками Отдела эксплуатации ПО АСУ ТП. Резервное копирование осуществляется каждый раз при изменении проекта на инженерной станции. Файлы резервных копий хранятся на сетевом диске. Доступ к папке сетевого диска и резервной копии проекта имеют только уполномоченные на это сотрудники Отдела эксплуатации ПО АСУ ТП..

### Наличие комплекта ЗИП

Для АРМ обеспечивается наличие запасных частей, инструментов и принадлежностей.  
Для сетевого оборудования и ПЛК АСУ ТП обеспечивается наличие аналогичных типов устройств для возможности замены в случае выхода из строя используемых. В случае отказа оборудования, находящегося в промышленной эксплуатации, осуществляется его замена и восстановление рабочей конфигурации из резервной копии. Производится закупка отказавших компонентов по мере расходования ЗИП..

### Мониторинг технического состояния

.

## Защита технических средств и систем

Мониторинг технического состояния оборудования обслуживающим персоналом производится на регулярной основе средствами самодиагностики оборудования среднего и верхнего уровней. Операторы выполняют мониторинг состояния системы, отображающегося на диагностическом экране InTouch. Состояние оборудования нижнего уровня диагностируется алгоритмами, заложенными в ПЛК, а также оценкой трендов текущих показателей (наличие существенных отклонений от средних значений показаний приборов, несоответствие состояния оборудования управляющим воздействиям).

### Меры физической защиты оборудования

кек.

физ1.

физ2.

физ3.

физ4.

### Бесперебойное электроснабжение

физ5.

## Защита информационной (автоматизированной) системы и ее компонентов

Бесперебойное питание оборудования осуществляется посредством подключения его через источники бесперебойного питания с аккумуляторными батареями. К источникам бесперебойного питания подключено все оборудование верхнего и среднего уровня, а также сетевое оборудование..

## Планирование мероприятий по обеспечению безопасности

Средства межсетевого экранирования не применяются.  
Средства криптографической защиты каналов связи не применяются..

## Управление конфигурацией

Процедуры планирования мероприятий по обеспечению безопасности АСУ ТП не определены..

## Управление обновлениями программного обеспечения

Процедуры управления конфигурацией АСУ ТП не определены..

## Реагирование на инциденты информационной безопасности

Обновление системного и прикладного ПО АСУ ТП осуществляется работниками Отдела эксплуатации ПО АСУ ТП в технологические «окна», в периоды плановых остановок технологического оборудования. После установки обновлений осуществляется тестирование корректности функционирования компонентов АСУ ТП, в случае выявления нарушений функционирования осуществляется восстановление работоспособной конфигурации из резервных копий. Документированный регламент управления обновлениями отсутствует..

## Обеспечение действий в нештатных ситуациях

Мониторинг работоспособности АСУ ТП организован за счет контроля штатного функционирования АСУ ТП и технологических процессов со стороны оператора АСУ ТП. Операторы работают посменно в режиме (24/7), в случае возникновения сбоев, потенциально связанных с нарушением нормального функционирования оборудования среднего или верхнего уровня АСУ ТП, операторы формирует заявку в системе регистрации неисправностей, которая поступает на обработку в центр автоматизации производства. Работники центра осуществляют диагностику неполадок и принимают меры по восстановлению нормального функционирования АСУ ТП, привлекая необходимые подразделения в соответствии с характером возникшей проблемы.  
В случае необходимости принятия срочных мер оператор связывается с дежурной службой центра автоматизации производства по телефону. Дежурная служба организует диагностику неполадок и принятие мер по восстановлению нормального функционирования АСУ ТП, привлекая необходимые подразделения в соответствии с характером возникшей проблемы.  
Дежурная служба центра автоматизации производства работает в режиме 24/7.  
Все заявки операторов регистрируются в системе регистрации неисправностей. Документированный процесс управления инцидентами в АСУ ТП отсутствует.

## Информирование и обучение персонала

Мониторинг работоспособности АСУ ТП организован за счет контроля штатного функционирования АСУ ТП и технологических процессов со стороны оператора АСУ ТП. Операторы работают посменно в режиме (24/7), в случае возникновения сбоев, потенциально связанных с нарушением нормального функционирования оборудования среднего или верхнего уровня АСУ ТП, операторы формирует заявку в системе регистрации неисправностей, которая поступает на обработку в центр автоматизации производства. Работники центра осуществляют диагностику неполадок и принимают меры по восстановлению нормального функционирования АСУ ТП, привлекая необходимые подразделения в соответствии с характером возникшей проблемы.  
В случае необходимости принятия срочных мер оператор связывается с дежурной службой центра автоматизации производства по телефону. Дежурная служба организует диагностику неполадок и принятие мер по восстановлению нормального функционирования АСУ ТП, привлекая необходимые подразделения в соответствии с характером возникшей проблемы.  
Дежурная служба центра автоматизации производства работает в режиме 24/7.  
Все заявки операторов регистрируются в системе регистрации неисправностей. Документированный процесс управления инцидентами в АСУ ТП отсутствует..

1. Структурная схема АСУ ТП

1. Федеральный закон от 21.07.1997 №116-ФЗ «О промышленной безопасности опасных производственных объектов». [↑](#footnote-ref-1)
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». [↑](#footnote-ref-2)
3. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [↑](#footnote-ref-3)
4. Приказ ФСТЭК России от 14.03.2014 № 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». [↑](#footnote-ref-4)
5. Указывается компонент АСУ ТП, который осуществляет сбор параметров технологического оборудования и/или формирование регулирующего воздействия на исполнительные механизмы. [↑](#footnote-ref-5)