

Петербургская ЭнергоСберегающая
Компания

Свидетельство № 0312.01-2017-7805583894-П-172

Заказчик - Филиал ООО "ЕвроСибЭнерго-Гидрогенерация"
Иркутская ГЭС

Комплексная система управления ГА для участия в
АВРЧМ. Инв. № КСУ000097931. Модернизация систем
виброконтроля.

Система выявления сейсмособытия

РАБОЧАЯ ДОКУМЕНТАЦИЯ

Информационная безопасность

П37.2021.01-ИБ



Петербургская ЭнергоСберегающая
Компания

Свидетельство № 0312.01-2017-7805583894-П-172

Заказчик - Филиал ООО "ЕвроСибЭнерго-Гидрогенерация"
Иркутская ГЭС

Комплексная система управления ГА для участия в
АВРЧМ. Инв. № КСУ000097931. Модернизация систем
виброконтроля.

Система выявления сейсмособытия

РАБОЧАЯ ДОКУМЕНТАЦИЯ

Информационная безопасность

П37.2021.01-ИБ

Главный инженер проекта

А.Ю. Губарев

| | | |
|--------------|--------------|--------------|
| Инв. № подл. | Подл. и дата | Взам. инв. № |
| | | |

Санкт-Петербург
2022

| Обозначение | Наименование | Примечание |
|-------------------|---|--------------------------------|
| ПЗ7.2021.01-ИБ.ТП | Ведомость технического проекта | |
| | Состав проектной документации | Выполнен отдельным томом |
| ПЗ7.2021.01-ИБ.П2 | Пояснительная записка к техническому проекту | |
| ПЗ7.2021.01-ИБ.С1 | Схема структурная комплекса технических средств защиты информации | |
| ПЗ7.2021.01-ИБ.С2 | Схема функциональной структуры | |
| ПЗ7.2021.01-ИБ.В4 | Спецификация оборудования изделий и материалов | |

[illegible]

СОДЕРЖАНИЕ

| | | |
|---------|---|----|
| 1. | Введение..... | 2 |
| 2. | Перечень принятых сокращений..... | 4 |
| 3. | Задачи по обеспечению информационной безопасности проектируемого объекта | 5 |
| 4. | Общая характеристика объекта..... | 7 |
| 5. | Структурно-функциональные характеристики объекта обеспечения информационной безопасности..... | 8 |
| 6. | Минимальные требования по обеспечению безопасности информации | 11 |
| 7. | Итоговый состав мер по обеспечению безопасности информации | 14 |
| 8. | Архитектура подсистемы обеспечения информационной безопасности | 30 |
| 9. | Технические решения..... | 39 |
| 9.1. | Подсистема сетевой безопасности | 46 |
| 9.2. | Подсистема управления учётными записями | 53 |
| 9.3. | Подсистема регистрации событий безопасности | 56 |
| 9.4. | Подсистема антивирусной защиты | 58 |
| 9.5. | Подсистема централизованного управления средствами защиты и контроля защищенности | 67 |
| 10. | Организационные решения..... | 69 |
| 10.1. | Подсистема управления информационной безопасностью..... | 69 |
| 10.1.1. | Штатное расписания и назначение ответственных..... | 70 |
| 10.1.2. | Разработка организационно-распорядительной документации | 72 |
| 10.2. | Подсистема защиты технических средств | 78 |
| | Приложение 1 | 80 |

Согласовано

Взам. инв. №

Подп. и дата

Инв. № подл.

П37.2021.01-ИБ.П2

Комплексная система управления ГА для участия в АВРЧМ. Инв. № КСУ000097931. Модернизация систем виброконтроля

| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | № КСУ0000097931. Модернизация систем виброконтроля | | | |
|-----------|--------|------------|------|-------|-------|--|-------------|------|--------|
| Разраб. | | Денисевич | | | 07.22 | Система выявления сейсмособытия | Стадия | Лист | Листов |
| Пров. | | Егоров | | | 07.22 | | Р | 1 | 118 |
| | | | | | | | | | |
| | | | | | | Пояснительная записка к техническому проекту | <div></div> | | |
| Н. контр. | | | | | | | | | |
| Утв. | | Афендииков | | | 07.22 | | | | |

1. Введение

В настоящем документе разработана подсистема обеспечения информационной безопасности (Далее – ПОИБ) при модернизации системы виброконтроля оборудования Иркутской гидроэлектростанции (Далее – ИГЭС).

По решению субъекта критической информационной инфраструктуры (Далее – КИИ) – руководства ИГЭС в документации детализируются для последующей реализации минимально достаточные меры защиты модернизируемой Системы для обеспечения информационной безопасности 3 категории значимости объекта КИИ.

Документ предназначен для персонала, реализующего организационные и технические мероприятия, выполнение которых необходимо для обеспечения безопасности информационных ресурсов и компонентов модернизируемой системы виброконтроля оборудования ИГЭС.

Решения в данной документации приняты в соответствии с действующими на территории Российской Федерации законодательством, международными и национальными стандартами, нормативными и методическими документами ФСТЭК России, в области информационной безопасности, в частности:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 02.07.2021 г.);
2. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи» (с изм. и доп., вступ. в силу с 01.05.2022 г.);
3. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (ред. от 05.10.2015 г.);
4. Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
5. Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений» (ред. от 02.07.2013г.);
6. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646;
7. Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры»;
8. Указ Президента РФ от 01 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
9. ISO/IEC 11801 «Информационные технологии. Структурированная кабельная система для помещений заказчиков;

| | |
|--------------|--|
| Взам. инв. № | |
| Подп. и дата | |
| Инв. № подл. | |

| | | | | | |
|------|--------|------|------|-------|------|
| | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |

П37.2021.01-ИБ.П2

| |
|------|
| Лист |
| 2 |

10. EN 50173 «Информационные технологии. Структурированная кабельная система»;
11. EIA/TIA-568A «Стандарт телекоммуникационной инфраструктуры коммерческих зданий»;
12. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
13. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
14. ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении»;
15. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;
16. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
17. Приказ ФСТЭК России от 25.12.2017 г. № 239 (ред. от 20.02.2020г.) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
18. Информационное сообщение ФСТЭК России от 24.03.2022 № 240/22/1549 «О мерах по повышению защищённости информационной инфраструктуры».

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 3 |

2. Перечень принятых сокращений

| | |
|---------------|--|
| АВПО | Антивирусной программное обеспечение |
| АПКШ | Аппаратно-программный комплекс шифрования |
| АРМ | Автоматизированное рабочее место |
| АСО | Активное сетевое оборудование |
| АСУ ТП | Автоматизированная система управления технологическим процессом |
| ЛВС | Локальная вычислительная сеть |
| КТС | Комплекс технических средств |
| СВТ | Средство вычислительной техники |
| ЗИП | Запасные части, инструменты и приспособления |
| ИБ | Информационная безопасность |
| ИБП | Источник бесперебойного питания |
| ИМ | Исполнительный механизм |
| ИГЭС | Иркутская гидроэлектростанция |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| КЗ | Контролируемая зона |
| КИП | Контрольно-измерительные приборы |
| КШ | Криптографический шлюз |
| НСД | Несанкционированный доступ |
| МЭ | Межсетевой экран |
| СВТ | Средство вычислительной техники |
| СрЗИ | Средство защиты информации |
| СЗИ | Система защиты информации |
| ПЛК | Программируемый логический контроллер |
| ПОИБ | Подсистема обеспечения информационной безопасности |
| ПТС | Программно-технические средства |
| ПТК | Программно-технический комплекс |
| ПУ | Программа управления |
| ПУ ЦУС | Программа управления центром управления сетью криптографических шлюзов |
| САУ | Система автоматического управления |
| СПД | Сеть передачи данных |
| УБИА | Угроза безопасности информации является актуальной |
| ЦУС | Центр управления сетью криптографических шлюзов |
| ЧМИ | Человеко-машинный интерфейс |
| ЭО | Экстренный останов |
| VPN | Virtual Private Network |

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 4 |

3. Задачи по обеспечению информационной безопасности проектируемого объекта

Защита информации является составной частью работ по созданию, модернизации и обеспечению функционирования любой АСУ и обеспечивается на всех стадиях их жизненного цикла. В соответствии с действующими нормативными положениями требования по обеспечению информационной безопасности АСУ, то есть к подсистеме защиты информации АСУ определяются в зависимости от класса их защищённости и актуальных угроз безопасности информации.

Реализуемые организационные и технические меры в подсистеме обеспечения информационной безопасности модернизируемой системы виброконтроля оборудования ИГЭС должны решать следующие задачи:

1) обеспечивать доступность обрабатываемой в автоматизированных системах управления информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);

2) соотносится с мерами по промышленной, функциональной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности модернизируемой Системы;

3) не оказывать отрицательного влияния на режим функционирования объекта в проектных режимах его работы, а проектируемые СрЗИ не должны оказывать негативного влияния на технологические процессы.

Решение по обеспечению информационной безопасности в модернизируемой Системе проводится:

1) в полном соответствии с нормативно-правовыми актами и методическими документами в области защиты информации, устанавливающими порядок разработки, внедрения и эксплуатации систем защиты, а также предъявляющим требования к обеспечению безопасности технологических процессов в АСУ;

2) с учетом используемых технологий и структурно-функциональных характеристик автоматизированных систем управления и особенностей их функционирования;

3) с перспективой дальнейшего развития/модернизации автоматизированных систем управления и взаимодействия со смежными системами.

Детальный состав технических и организационных мер защиты, используемых при разработке подсистемы информационной безопасности модернизируемой

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|-----------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 5 |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | |

Системы, согласно требованиям Приказа ФСТЭК России от 25.12.2017 № 239, определяются на основании:

- 1) требуемой категории защищенности объектов КИИ;
- 2) актуальных угроз информационной безопасности;
- 3) требований к мерам и средствам защиты информации, применяемых в АСУ;
- 4) требований к защите информации при информационном взаимодействии АСУ с иными информационными системами.
- 5) требований Задания на разработку проектной и рабочей документации по объекту «Комплексная система управления ГА для участия в АВРЧМ. Инв. № КСУ 000097931. Модернизация систем виброконтроля»

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|-----------|--|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 6 | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | |

4. Общая характеристика объекта

В административном отношении Объект модернизации (разработки) – Иркутская ГЭС находится непосредственно в черте областного центра, в г. Иркутск в Российской Федерации с хорошо развитой городской инфраструктурой на территории принадлежащей заказчику – филиалу ООО «ЕвроСИБЭнерго-Гидрогенерация» Иркутская ГЭС.

В географическом отношении объект модернизации расположен у водного объекта на площади преимущественно с равнинным рельефом в азиатской части России на территории Восточной Сибири с резко-континентальным климатом и 1 классом гидротехнических сооружений (ГТС) (чрезвычайно высокой опасности). Сейсмичность в районе расположения по шкале MSK-64 составляет 8 баллов.

Модернизируемый объект полностью находится внутри помещений технического (производственного) здания, расположенного на территории заказчика по периметру которой располагаются инженерно – технических средств охраны, функционирует СКУД, сигнализация (периметральное и объектовая), круглосуточное и непрерывное видеонаблюдение, а также осуществляется непосредственная охрана всей территории сотрудниками территориального подразделения Федеральной службы войск национальной гвардии Российской Федерации – Росгвардии в соответствии с установленным регламентом.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 7 |

5. Структурно-функциональные характеристики объекта обеспечения информационной безопасности

В целом объектом обеспечения информационной безопасности является модернизируемая система виброконтроля оборудования Иркутской ГЭС, функционирование которой заключается в следующем.

На генерирующих агрегатах ИГЭС смонтировано 9 датчиков вибрации, каждый из которых по физической линии соединен с модулями обработки сигналов специализированного ПЛК. При поступлении служебной (сигнальной) информации от датчиков вибрации ПЛК по заранее установленному алгоритму обрабатывает её и по организованному с помощью средств маршрутизации и коммутации каналам связи направляет их на сервер РС1 и сервер РС2, работающих в «горячем резерве». На этих серверах информация аккумулируется (обрабатывается) в специализированном приложении и затем доводится на АРМ руководителей и иных лиц оперативно-производственных служб. По истечению установленного времени эта информация поступает для архивирования на сервера арх. 1 и арх. 2. По своей структуре, модернизируемая система виброконтроля оборудования Иркутской ГЭС является локальной системой и не предполагает присоединение к внешним сетям связи, в том числе и общего пользования.

Непосредственными объектами защиты от угроз информационной безопасности являются информационные ресурсы (технологическая информация) модернизируемой Системы и их носители, а также вспомогательные Системы, обеспечивающие её надежную и безопасную эксплуатацию.

Объекты защиты, для которых определены актуальные угрозы ИБ и меры по их нейтрализации можно отнести к следующим группам:

1. Технологическая информация.
2. СБТ (сервера, АРМ).
3. ПЛК.
4. Сетевое оборудование и кабели (линии) связи.
5. Программное обеспечение.
6. Исполнительное (контролирующее) полевое (периферийное)

оборудование.

7. Системы, обеспечивающие эксплуатацию Системы виброконтроля (бесперебойного электропитания, поддержания климата и т.п.).

По существу, к объектам защиты относят непосредственно информацию, ее носители и обеспечивающих их функционирование вспомогательные Системы.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|-----------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 8 |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | |

Система виброконтроля оборудования Иркутской ГЭС по существу является АСУ и построена по иерархической трёхуровневой распределенной системе с централизованным пунктом управления. Её организационно-технологическая структура включает следующие уровни управления:

- 1) верхний – оперативно-производственных служб (Далее – ОПС);
- 2) средний – систем автоматического управления (Далее – САУ);
- 3) нижний – контрольно-измерительных приборов (Далее – полевой уровень).

В качестве активно защищаемых информационных ресурсов и их носителей модернизируемой Системы рассматривается преимущественно оборудование верхнего уровня, данные, обрабатываемые на нем, а также телекоммуникационное оборудование и линии связи, обеспечивающие взаимодействие между уровнями управления. Защита среднего и нижнего уровней Системы обеспечивается преимущественно организационными мерами, с учётом рельефа местности, географических и иных особенностей Объекта.

Верхний уровень модернизируемой Системы предназначен для ведения мониторинга о состоянии защищаемого объекта (сейсмоактивности) в режиме реального времени и представление его результатов оперативно-производственному персоналу, функционированию технологической базы данных, создания архива информации, диагностики, программной диагностики оборудования.

Модернизируемая Система, по сути АСУ осуществляет в штатном режиме мониторинг состояния (контроль) защищаемого объекта в автоматическом и в автоматизированном (по сути, в дистанционном режиме с участием оперативного персонала) режимах в соответствии с алгоритмами. В случае возникновения какой-либо нештатной ситуации на объекте (сейсмоактивности и т.п.) формируется сигнал для перевода ГА в аварийные режимы или останова.

Аппаратная реализация верхнего уровня управления (ОПС) включает в себя следующие средства, объединенные в не изолированной ЛВС сейсмоконтроля и обеспечивающие реализацию человеко-машинного интерфейса для оперативного и управляющего персонала:

- 1) 8-м АРМ оперативно-диспетчерского и управляющего персонала: директора, главного инженера, начальника ОЭЦ, специалиста СРЗиА, специалиста МГА ГЩУ, специалиста ДЭМ ГЩУ, 2-а АРМ специалиста НСС ГЩУ;
- 2) серверы РС1 и РС2;
- 3) серверы архива 1 и 2.

На этом уровне осуществляется сбор, обработка, архивирование и отображение всех контролируемых параметров, поступающих со среднего уровня – от систем

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 9 |

автоматического управления. На этом уровне и будут сосредоточены максимальные меры защиты информации от угроз ИБ.

Серверы смонтированы в промышленном, запирающемся шкафу с сигнализацией от несанкционированного открытия дверей, а комплекты АРМ пользователей размещаются непосредственно на рабочих местах управляющего и оперативно-диспетчерского персонала.

Средний уровень – САУ защищаемой Системы, являющийся подчиненным к ОПС и обеспечивает получение информации от полевого оборудования, ее алгоритмическую обработку и передачу информации на ОПС. Реализуется этот уровень на базе самостоятельного локального (объектового) САУ на основе ПЛК с модулями ввода/вывода, вычислителей, выполняющих функции блока обработки информации. Этот уровень функционирует в автоматическом режиме работы по заданным алгоритмам без вмешательства оперативно-диспетчерского персонала в процесс управления оборудованием.

Оборудование среднего уровня располагается в запираемом шкафу в контролируемом (закрываемом) аппаратном помещении ИГЭС и включает в себя: ПЛК с модулями ввода-вывода, вычислители, сетевое оборудование, Системы (источники) гарантированного электропитания и микроклимата.

Нижний или полевой уровень по существу представляет собой размещаемые непосредственно на технологическом оборудовании (основных агрегатов) ИГЭС контрольно-измерительные приборы – датчики вибрации, соединённые по физическим линиям с уровнем САУ и функционирующие в основном в физически недоступном для нарушителя режиме.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 10 |

6. Минимальные требования по обеспечению безопасности информации

Руководствуясь информационным письмом Заказчика от 12.10.2022 № Вх-22-0592 (приложение 1) при формировании минимальных требований по обеспечению ИБ следует исходить, что модернизируемая в настоящем проекте Система виброконтроля не является значимым объектом КИИ, однако в соответствии с п. 3 приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» устанавливается, что по решению субъекта критической информационной инфраструктуры настоящие Требования могут применяться для обеспечения безопасности объектов критической информационной инфраструктуры, не отнесенных к значимым объектам, что и следует из п. 7.4. Задания на разработку проектной и рабочей документации по объекту: «Комплексная система управления ГА для участия в АВРЧМ. Инв. № КСУ000097931. Модернизация систем виброконтроля».

Таким образом, применяемый в модернизируемой Системе набор мер должен быть минимально достаточным для обеспечения безопасности значимого объекта КИИ 3 (третьей) категории, хотя указанная Система, а по существу АСУ объекта, не является значимым объектом КИИ.

Выбор мер обеспечения безопасности информации модернизируемого объекта КИИ для их реализации включает следующие этапы:

1) определение базового набора мер обеспечения безопасности информации для установленной (определённой) категории значимости в соответствии с Приложением к приказу ФСТЭК России от 25.12.2017 № 239;

2) адаптацию базового набора мер обеспечения безопасности информации применительно к каждому уровню автоматизированной системы управления;

3) уточнение адаптированного базового набора мер обеспечения безопасности информации с учетом не выбранных ранее мер;

4) дополнение уточненного адаптированного базового набора мер обеспечения безопасности информации мерами, обеспечивающими выполнение требований к обеспечению безопасности информации, установленными иными нормативными правовыми актами, локальными правовыми актами, национальными стандартами, стандартом и Политикой Компании в области информационной безопасности.

Требования Заказчика состоят в минимально достаточном наборе мер для обеспечения безопасности информации объекта КИИ 3 категории значимости.

Однако, с учётом требований Задания на разработку проектной и рабочей документации по объекту взаимодействие технологических сетей с внешними

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 11 |

выделенными сетями должно быть организовано через межсетевой экран с организацией DMZ-зон, а взаимодействие между сетями и сегментами внутри технологических сетей должно осуществляться исключительно через физические интерфейсы, организованные на межсетевом экране. К тому же сегментирование должно быть проведено таким образом, чтобы исключить возможность доступа между сегментами в обход межсетевого экрана.

Вместе с тем, базовыми принципами обеспечения информационной безопасности в автоматизированных системах управления, в том числе и в модернизируемой Системе являются:

- 1) отделение технологических сетей АСУ от корпоративной ЛВС, внешних сетей, а также от сетей общего пользования на физическом или сетевом (логическом) уровнях;
- 2) применение межсетевых экранов в точках сопряжения промышленной сети со смежными и внешними сетями, а также на границах разнородных сетей (проводные и беспроводные);
- 3) идентификация (фильтрация) по MAC-адресам на портах (интерфейсах) активного сетевого оборудования;
- 4) отключение неиспользуемых интерфейсов (портов) ввода/вывода с применением механизмов, встроенных в операционные системы АРМ и серверов, а также опечатывание неиспользуемых в процессе эксплуатации интерфейсов;
- 5) максимальное ограничение физического доступа субъектов к сетям и иным компонентам АСУ, управление доступом к физическим ресурсам ЛВС, АРМ и серверам посредством системы контроля и управления доступом (СКУД), а также применением на объекте систем безопасности (охранная сигнализация, видеонаблюдение, охранные подразделения и т.п.);
- 6) организация управления учетными записями пользователей и использование строгой парольной политики;
- 7) контроль параметров сетевого оборудования и правила фильтрации трафика на межсетевых экранах;
- 8) защита привилегированных учётных записей (администратора безопасности, системного администратора);
- 9) минимизация привилегий пользователей и служб;
- 10) использование актуального антивирусного программного обеспечения;
- 11) регулярное обновление системного, прикладного, специального программного обеспечения, безопасности операционной системы;
- 12) прокладка линий связи способом, затрудняющим НСД;

| | | | | | | | | | |
|--------------|--------------|--------------|-------------------|-------|------|--|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | П37.2021.01-ИБ.П2 | | | | | | |
| | | | 12 | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | | | | |

13) формирование штатного расписания и должностных инструкций обслуживающего персонала в соответствии с требованиями ИБ (назначение ответственных, разделение полномочий, исключение возможности принятия единоличного решения, влияющего на безопасность);

14) доведение информации по обеспечению ИБ до персонала, допущенного к компонентам Системы, проведение инструктажей, обучений;

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|----|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | 13 |

7. Итоговый состав мер по обеспечению безопасности информации

В ходе анализа нормативно-технических документов, определяющих функционирование АСУ, было определено, что выполнение требований в области защиты технологических процессов является приоритетным и полностью перекрывает требования, установленные иными нормативными правовыми актами в области защиты информации. Соответственно, дополнение уточненного адаптированного базового набора мер по обеспечению безопасности информации не требуется.

Однако, с учётом изменений нормативного регулирования, внесённых приказами ФСТЭК России от 09.08.2018 № 138, от 26.19.2019 № 60 и от 20.02.2020 № 35 в приказ ФСТЭК России от 25.12.2017 № 239, для АСУ проектируемого объекта итоговый состав мер по обеспечению безопасности информации, включая организационные мероприятия, реализуемый в программных, аппаратных и организационных средствах представлен в Таблице 2.

Таблица 2 - Итоговый состав мер по обеспечению безопасности информации

| Обозначение | Меры по обеспечению безопасности информации в АСУ | Реализуемые техническими средствами защиты информации | Реализуемые организационным и мероприятиями | Нейтрализация УБИ (https://bd.u.fstec.ru/threat) | |
|-------------------|--|---|---|--|------|
| ИАФ | I. Идентификация и аутентификация | | | | |
| ИАФ.0 | Регламентация правил и процедур идентификации и аутентификации | | Политики информационной безопасности Компании. Регламент предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | 6,8,13,30,74,86,100,123,131,152,168,211 | |
| ИАФ.1 | Идентификация и аутентификация пользователей и иницируемых ими процессов | Выполнение требований достигается выполнением следующих мероприятий: – применение встроенных в компоненты защищаемой системы инструментов аутентификации (средства операционной системы и прикладные средства аутентификации ПО); – конфигурирование ЛВС с учетом сегментирования | Контроль выполнения управления учетными записями и всех требований ИБ отделом безопасности Компании | 6,8,13,30,98,100,131,152,168,211 | |
| ИАФ.2 | Идентификация и аутентификация устройств | | | 8,30,98,131,212 | |
| ИАФ.3 | Управление идентификаторам и | | | 30,131,212 | |
| ИАФ.4 | Управление средствами | | | 8,30,74,86,100,123, | |
| П37.2021.01-ИБ.П2 | | | | | |
| Лист | | | | | |
| 14 | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |

| | | | | | |
|-------------------|--------|--|--|--|---|
| | | аутентификации | сетей; – применение дополнительных (накладных) специализированных инструментов, входящих в состав СрЗИ. | | 131,152,204 |
| | ИАФ.5 | Идентификация и аутентификация внешних пользователей | | | 8,30,98,131,152 |
| | ИАФ.7 | Защита аутентификационной информации при передаче | – использование безопасных протоколов обмена (https, ssh и пр.). | | 8,30,74,86,100,12,3,131,152,204 |
| УПД | | II. Управление доступом | | | |
| | УПД.0 | Регламентация правил и процедур управления доступом | | Выполнение Политики информационной безопасности Компании. Регламент предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | 6,7,12,15,18,23,24,28,31,63,67,68,69,86,88,89,90,91,107,111,112,116,122,129,170,187,198,204,211,213 |
| | УПД.1 | Управление учетными записями пользователей | | | 6,7,28,31,63 |
| | УПД.2 | Реализация модели управления доступом | Выполнение требований достигается выполнением следующих мероприятий: – применение встроенных в компоненты защищаемой системы инструментов аутентификации (средства операционной системы и прикладные средства аутентификации ПО); – организация подсистемы управления учетными записями с применением дополнительных специализированных инструментов, входящих в состав СрЗИ (наложенных); – конфигурирование ЛВС с учетом сегментирования. | Контроль управления учетными записями отделом безопасности Компании | 6,7,15,18,23,28,31,63,67,88,89,107,116,122,129,16,7,170,187,198,204,213 |
| | УПД.4 | Разделение полномочий (ролей) пользователей | | | 6,7,14,18,23,24,28,31,63,68,90,107,112,170,211 |
| | УПД.5 | Назначение минимально необходимых прав и привилегий | | | 6,7,12,14,15,16,18,23,24,28,31,63,67,68,69,86,88,89,90,107,111,112,113,116,121,122,124,127,143,152,167,178, |
| Инв. № подл. | | | | | |
| | | | | | |
| | | | | | |
| Подп. и дата | | | | | |
| | | | | | |
| Взам. инв. № | | | | | |
| | | | | | |
| П37.2021.01-ИБ.П2 | | | | | Лист |
| | | | | | 15 |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |

| | | | | | | | | | |
|--------|--|--|---|-------|------|---|--|--|--|
| | | | | | | | | | 183,185,1 87,188,19 8,211,212, 213 |
| УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизирован ную) систему | | | | | | | | 7,8,14,15, 63,88,187, 198,212 |
| УПД.10 | Блокирование сеанса доступа пользователя при неактивности | | | | | | | | 8,16,24,28 ,63,88,113 ,187,198,2 12 |
| УПД.11 | Управление действиями пользователей до идентификации и аутентификации | | | | | | | | 18,28,63,1 70,185,18 7,198 |
| УПД.13 | Реализация защищенного удаленного доступа | Мера исключена. При эксплуатации защищаемой системы удалённый к ней доступ не предполагается, так как система локальная. | | | | | | | |
| УПД.14 | Контроль доступа из внешних информационных (автоматизирован ных) систем | – применение встроенных в компоненты защищаемой системы инструментов аутентификации (средства операционной системы и прикладные средства аутентификации ПО); – применением дополнительных специализированных инструментов, входящих в состав СрЗИ (через межсетевой экран с организацией DMZ-зон); – конфигурирование ЛВС с учетом сегментирования. | Регламент предоставления доступа. Контроль управления учетными за- писями отделом безопасности Компании | | | | | | 6,8,15,16, 18,28,34,6 9,98,104,1 07,113,14 3,167,170, 187,198 |
| ОПС | III. Ограничение программной среды Для 3 категории значимости объекта КИИ все меры по ОПС исключены и не требуется их разработка и реализация | | | | | | | | |
| ЗНИ | IV. Защита машинных носителей информации | | | | | | | | |
| ЗНИ.0 | Регламентация правил и процедур защиты машинных носителей информации | | | | | Выполнение Политики информационной безопасности Компании. Регламент предоставления доступа. Контроль выполнения всех | | | 71,74,91,1 43,156,15 8,179, |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | |
| | | | | | | Лист | | | |
| | | | | | | 16 | | | |

| | | | | | | | |
|--------------|---|--|---|-------|------|---|-----------------|
| | | | | | | требований ИБ отделом безопасности Компании | |
| ЗНИ.1 | Учет машинных носителей информации | | | | | Руководство пользователя (администратора) | 74,91,156 |
| ЗНИ.2 | Управление физическим доступом к машинным носителям информации | Выполнение требований достигается выполнением следующих мероприятий: – отключение неиспользуемых интерфейсов (портов) ввода/вывода с применением встроенных в компоненты защищаемой системы инструментов; – опечатывание неиспользуемых интерфейсов (портов) ввода/вывода; – контроль подключения носителей информации с применением специализированных (наложенных) инструментов, входящих в состав СрЗИ; – соблюдение правил по уничтожению конфиденциальной информации с компонентов АСУ перед передачей их сторонним организациям для проведения ремонтных работ. | Соблюдение правил, установленных Политикой информационной безопасности Компании. Руководство пользователя (администратора) | | | 71,74,91,1 43,158,17 9 | |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации | | | | | 74,88,91,1 43,158,17 9 | |
| ЗНИ.7 | Контроль подключения машинных носителей информации | | | | | 74,88,91,1 43,158,17 9 | |
| ЗНИ.8 | Уничтожение (стирание) на информации на машинных носителях информации | | | | | 71,91 | |
| АУД | V. Аудит безопасности | | | | | | |
| АУД.0 | Регламентация правил и процедур аудита безопасности | | | | | Выполнение Политики информационной безопасности Компании. Регламент предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | 154,176,2 14 |
| АУД.1 | Инвентаризация информационных ресурсов | средства защиты информации (наложенные), СВТ используемые в АСУ объекта | | | | Регламент предоставления доступа. Контроль | 23 |
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | Лист |
| | | | | | | | 17 |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | |

| | | | | | | | | |
|---------------|--|--|---|--|------|-------------------|---|--|
| | | | | | | | выполнения всех требований ИБ отделом безопасности Компании | |
| АУД.2 | Анализ уязвимостей и их устранение | Реализация мер достигается применением специализированных инструментов, входящих в состав СрЗИ, имеющих следующую функциональность: – контроль состава и целостности ПО; – регистрация событий безопасности; – централизованный сбор, хранение и архивирование журналов; – контроль устройств, подключаемых к АРМ и Серверам; – контроль состояния устройств с возможностями блокирования АРМ (Сервера) при изменении состояния заданных устройств. | Регламент предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | 17,122,132,154,213,214 | | | | |
| АУД.3 | Генерирование временных меток и (или) синхронизация системного времени | | | 176,214 | | | | |
| АУД.4 | Регистрация событий безопасности | | | 177,214 | | | | |
| АУД.6 | Защита информации о событиях безопасности | | | 124,214 | | | | |
| АУД.7 | Мониторинг безопасности | | | 177,214 | | | | |
| АУД.8 | Реагирование на сбои при регистрации событий безопасности | Специализированные инструменты, входящие в состав СрЗИ, имеющие функционал программного сканера уязвимостей. | Руководство пользователя (администратора) . Корректирующие действия выполняются по результатам анализа инцидентов по согласованию с отделом безопасности Компании | 124,176,214 | | | | |
| АУД.10 | Проведение внутренних аудитов | Средства защиты информации, СВТ, используемые в АСУ объекта | Руководство пользователя (администратора) . Регламент предоставления доступа. | 214 | | | | |
| АВЗ | VI. Антивирусная защита | | | | | | | |
| АВЗ.0 | Регламентация правил и процедур антивирусной защиты | | Выполнение Политики информационной безопасности Компании. | 6,8,27,145,167,170,186,188,190,198,204,208,213 | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | |
| Интв. № подл. | Подп. и дата | Взам. инв. № | | | | | Лист | |
| | | | | | | | 18 | |

| | | | | | | | | | |
|--------------|--------------|------|------|-------|------|-------------------|------|--|--|
| Инв. № подл. | Взам. инв. № | | | | | Подп. и дата | Лист | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | |
| | | | | | | 19 | | | |

| | | | | | | | |
|-------|--|--|--|--|--|-------------------------------------|---|
| | | | | | | отделом безопасности Компании | |
| ОЦЛ.1 | Контроль целостности программного обеспечения | Реализация мер достигается применением специализированных инструментов, входящих в состав СрЗИ, имеющих следующую функциональность: – контроль состава и целостности ПО; – регистрация событий безопасности; | | | | | 6,12,13,17 ,73,121,12 9,145,169, 183 |

| | | | | |
|-------|--|--|--|--|
| | | | Регламент предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | |
| АВЗ.1 | Реализация антивирусной защиты | Реализация мер достигается применением компонентов антивирусной защиты, входящих в состав СрЗИ. | Регламент предоставления доступа. Руководство администратора | 6,8,27,145,167,170,186,188,190,198,204,208,213 |
| АВЗ.2 | Антивирусная защита электронной почты и иных сервисов | | | 6,27,145,167,168,186,188,208 |
| АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | | | 27,145,167,168,170,176,186,188,190,198,204,208,213 |
| СОВ | VII. Предотвращение вторжений (компьютерных атак) Для 3 категории значимости объекта КИИ все меры СОВ исключены и не требуется их разработка и реализация | | | |
| ОЦЛ | VIII. Обеспечение целостности | | | |
| ОЦЛ.0 | Регламентация правил и процедур обеспечения целостности | | Выполнение Политики информационной безопасности Компании. Регламент предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | 6,12,13,17,121,145,169,183 |
| ОЦЛ.1 | Контроль целостности программного обеспечения | Реализация мер достигается применением специализированных инструментов, входящих в состав СрЗИ, имеющих следующую функциональность: – контроль состава и целостности ПО; – регистрация событий безопасности; | | 6,12,13,17,73,121,129,145,169,183 |

| | | | | | | | |
|------------|---|--|------|---|------|--------------------------------|--|
| | | | | | | | |
| | | – централизованный сбор, хранение и архивирование журналов; – контроль устройств, подключаемых к АРМ и Серверам; – контроль состояния устройств с возможностями блокирования АРМ (Сервера) при изменении состояния заданных устройств. | | | | | |
| ОДТ | | IX. Обеспечение доступности | | | | | |
| ОДТ.0 | Регламентация правил и процедур обеспечения доступности | | | Выполнение Политики информационной безопасности Компании. Инструкция с требованиями по резервному копированию. Регламент предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | | 51,129,156,158 | |
| ОДТ.4 | Резервное копирование информации | Встроенные и прикладные средства, используемые в АСУ | | Руководство администратора. Инструкция с требованиями по резервному копированию. Контроль | | 156,158 | |
| ОДТ.5 | Обеспечение возможности восстановления информации | резервные копии данных, резервируемые СВТ | | требованиями по резервному копированию. | | 51,156,158 | |
| ОДТ.6 | Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях | Наличие экземпляра ПО на отторгаемом носителе и резервных копий данных Системы. Дублирующие СВТ. | | выполнения всех требований ИБ отделом безопасности Компании | | 51,129,158 | |
| ОДТ.8 | Контроль предоставляемых вычислительных ресурсов и каналов связи | Мера исключена. При эксплуатации защищаемой системы предоставление вычислительных ресурсов и каналов связи сторонним организациям не предполагается. | | | | | |
| ЗТС | | X. Защита технических средств и систем | | | | | |
| ЗТС.0 | Регламентация правил и процедур защиты | | | Внутренний регламент объекта. | | 4,5,18,24,53,63,74,88,107,122, | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | |
| | | | | | | Лист | |
| | | | | | | 20 | |

| | | | | | | | | | |
|-------------------|--------------|--------------|-------|--|--|---|--|--|--|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | технических средств и систем | | Выполнение Политики информационной безопасности Компании. Контроль выполнения всех требований ИБ отделом безопасности Компании. | 139,143,157,160,187,207 | | |
| | | | ЗТС.2 | Организация контролируемой зоны | Применение компонентов СрЗИ имеющих функциональность по межсетевому экранированию сетевого трафика как локальному (программный МЭ на АРМ и серверах), так и аппаратному (на границах периметра сегментов сети); | Внутренний регламент объекта. | 4,5,18,53,63,74,88,107,113,122,139,157,160,187 | | |
| | | | ЗТС.3 | Управление физическим доступом | | Внутренний регламент объекта, СКУД, видеонаблюдение, охранная сигнализация. | 4,5,8,18,23,24,30,53,63,74,88,98,107,113,122,123,139,143,160,187,207 | | |
| | | | ЗТС.4 | Размещение устройств вывода (отображения) информации, исключая ее несанкционированный просмотр | Размещение компонентов с учётом выполнения условий: – в запираемых помещениях, оборудованных системами поддержания микроклимата, охранными системами и СКУД; – размещение в шкафах, оборудованных запираемыми дверями; – размещение мониторов АРМ в местах, исключая несанкционированное чтение данных; – обеспечение источниками бесперебойного электропитания. | Внутренний регламент объекта. Рабочая документация, видеонаблюдение | 57,187,207 | | |
| | | | ЗТС.5 | Защита от внешних воздействий | | | 24,51,139,180,182 | | |
| | | | ЗИС | XI. Защита автоматизированной системы и ее компонентов | | | | | |
| | | | ЗИС.0 | Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее | | Выполнение Политики информационной безопасности Компании. Регламент | 5,30,98,140,156,177,183,187 | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| П37.2021.01-ИБ.П2 | | | | | | | Лист | | |
| | | | | | | | 21 | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | | | | |

| | | | | | | |
|--------------|---|---|-------------------|--|--|--|
| | | | | | | |
| | | компонентов | | предоставления доступа. Контроль выполнения всех требований ИБ отделом безопасности Компании | | |
| ЗИС.1 | Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями | | | Формирование штатного расписания и должностных инструкций сотрудников, эксплуатирующих защищаемую систему, а также сотрудников отдела безопасности Компании. | 5,177,183,187 | |
| ЗИС.2 | Защита периметра информационной (автоматизированной) системы | СрЗИ используемые в АСУ объекта с функцией межсетевого экранирования. | | Внутренний регламент объекта, видеонаблюдение | 23,34,98,104,114,122,132,140,145,176,183,187 | |
| ЗИС.3 | Эшелонированная защита информационной (автоматизированной) системы | При реализации мер защиты применен комплексный подход: – применение физических средств защиты от НСД; – применение программных средств антивирусной защиты и защиты от вторжений; – организация парольной защиты и разграничения прав доступа и т.п. | | Регламент предоставления доступа. Внутренний регламент объекта. Видеонаблюдение. СКУД. | 6,34,73,98,122,132,140,145,177,183 | |
| ЗИС.5 | Организация демилитаризованной зоны | СрЗИ используемые в АСУ объекта с функцией межсетевого экранирования. | | Руководство администратора | | |
| ЗИС.6 | Управление сетевыми потоками | – СрЗИ используемые в АСУ объекта с функцией межсетевого экранирования – использование безопасных протоколов обмена (https, ssh и пр.). | | | 6,34,73,98,122,132,140,145,177,183, 187 | |
| ЗИС.8 | Соккрытие архитектуры и конфигурации информационной (автоматизированной) системы | СрЗИ используемые в АСУ объекта с функцией межсетевого экранирования. | | Внутренний регламент объекта. Видеонаблюдение. СКУД | 30,98,103,104,114,132,155,185 | |
| ЗИС.19 | Защита | Мера исключена. | | | | |
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | |
| | | | П37.2021.01-ИБ.П2 | | | |
| | | | Лист | | | |
| | | | 22 | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | |

| | | | | | | |
|-------------------|--------------|------|------------------------|--|--|------------|
| Инв. № подл. | Подп. и дата | | Взам. инв. № | | | |
| | | | | | | |
| ИНЦ.0 | ИНЦ.1 | | Выявление компьютерных | Выполнение мер достигается применением | Регламент предоставления доступа. Руководство пользователя (администратора) Контроль выполнения всех требований ИБ отделом безопасности Компании | 205 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | Лист 23 |
| П37.2021.01-ИБ.П2 | | | | | | |

П37.2021.01-ИБ.П2

| | | | | | |
|--------|--|--|---|------------------|--|
| | информации при ее передаче по каналам связи | При эксплуатации защищаемой системы не предусматривается передача по каналам связи информации вне контролируемой зоны, так как система локальная. | | | |
| ЗИС.20 | Обеспечение доверенного канала, маршрута | Мера исключена. При эксплуатации защищаемой системы не предусматривается передача по каналам связи информации вне контролируемой зоны, так как система локальная. | | | |
| ЗИС.21 | Запрет несанкционированной удаленной активации периферийных устройств | Мера исключена. Среди компонентов защищаемых систем не предусматриваются периферийные устройства, активация которых возможна удаленно. | | | |
| ЗИС.32 | Защита беспроводных соединений | Мера исключена. При эксплуатации защищаемой системы не предусматривается использование беспроводных соединений. | | | |
| ЗИС.34 | Защита от угроз отказа в обслуживании (DOS, DDOS-атак) | Программные и аппаратно-программные СрЗИ, используемые в АСУ | — | 6,69,140,155,176 | |
| ЗИС.38 | Защита информации при использовании мобильных устройств | Мера исключена. При эксплуатации защищаемой системы применение мобильных технических средств не предусмотрено. | | | |
| ЗИС.39 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | Мера исключена. В составе защищаемой системы компоненты, используемые среду виртуализации, отсутствуют. | | | |

| | | |
|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № |
| | | |

| | | | | | | |
|-------------------|--|---|------|-------|---|-------------|
| | | | | | | |
| | инцидентов | программных компонентов, входящих в состав СрЗИ, имеющих следующую функциональность: | | | | |
| ИНЦ.2 | Информирование о компьютерных инцидентах | – контроль состава и целостности ПО; | | | Руководство пользователя (администратора), Планы занятий с пользователями. | |
| ИНЦ.3 | Анализ компьютерных инцидентов | – регистрация событий безопасности; – обнаружение атак; – контроль состояния устройств; – контроль целостности файловых объектов и реестра; – оповещение администратора по заданным событиям безопасности; – блокирование АРМ (сервера) по заданным событиям безопасности. | | | Руководство администратора. | 205 |
| ИНЦ.4 | Устранение последствий компьютерных инцидентов | Резервные копии данных, Средства защиты информации, СВТ используемые в АСУ объекта | | | – | |
| ИНЦ.5 | Принятие мер по предотвращению повторного возникновения компьютерных инцидентов | Средства защиты информации, СВТ используемые в АСУ объекта | | | Руководство администратора, Планы занятий с пользователями. | 205 |
| ИНЦ.6 | Хранение и защита информации о компьютерных инцидентах | Средства защиты информации, СВТ используемые в АСУ объекта | | | Руководство администратора. | 205 |
| УКФ | | XIII. Управление конфигурацией | | | | |
| УКФ.0 | Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы | | | | Выполнение Политики информационной безопасности Компании. Регламент предоставления доступа. Руководство пользователя (администратора) Контроль выполнения всех требований ИБ отделом безопасности | 6,12,23,205 |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | |
| П37.2021.01-ИБ.П2 | | | | | | Лист |
| | | | | | | 24 |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------|--------------|--------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------|--------------|--------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

| | | | | |
|-------|---|--|---|-----------|
| | обеспечению защиты информации | | Регламент предоставления доступа. Руководство администратора. Контроль выполнения всех требований ИБ отделом безопасности Компании | |
| ПЛН.1 | Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации | Выполнение мер достигается за счет: – проведение регулярных аудитов информационной безопасности; – периодический анализ для поддержания в актуальном виде рисков информационной безопасности, а также плановых мероприятий по устранению их последствий; – информирование и обучение персонала. | Организационно-распорядительные документы Компании | 156,205 |
| ПЛН.2 | Контроль выполнения мероприятий по обеспечению защиты информации | | | 4,156,205 |
| ДНС | XVI. Обеспечение действий в нештатных ситуациях | | | |
| ДНС.0 | Регламентация правил и процедур обеспечения действий в нештатных ситуациях | — | Выполнение Политики информационной безопасности Компании. Регламент предоставления доступа. Руководство администратора. Контроль выполнения всех требований ИБ отделом безопасности Компании | |
| ДНС.1 | Разработка плана действий в нештатных ситуациях | — | Организационно-распорядительные документы, Регламент по нейтрализации последствий деструктивных информационных воздействий, в том числе направленных на вирусное | |

| | | | | | | | | |
|-------|--|------|------|--|------|-------------------|--|---|
| | | | | | | | заражение и/или модификацию информационных ресурсов, Руководство администратора (пользователя) | |
| ДНС.2 | Обучение и отработка действий персонала в нестатных ситуациях | | | — | | | Организационно-распорядительные документы, Руководство администратора (пользователя) | 205 |
| ДНС.5 | Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций | | | Наличие экземпляра ПО на отторгаемом носителе, СВТ, наличие ЗИП, резервных копий данных, | | | Регламент по нейтрализации последствий деструктивных информационных воздействий, в том числе направленных на вирусное заражение и/или модификацию информационных ресурсов, Руководство администратора. | |
| ДНС.6 | Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения | | | — | | | Регламент по нейтрализации последствий деструктивных информационных воздействий, в том числе направленных на вирусное заражение и/или модификацию информационных ресурсов, Руководство администратора. | |
| ИПО | XVII. Информирование и обучение персонала | | | | | | | |
| ИПО.0 | Регламентация правил и процедур информирования и обучения персонала | | | — | | | Выполнение Политики информационной безопасности Компании. Регламент предоставления доступа. Руководство администратора. | 5,127,145,154,156,177,186,188,190,205,212 |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | |
| | | | | | | Лист | | |
| | | | | | | 27 | | |

| | | |
|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № |
| | | |

| | | | | |
|-------|--|---|---|---|
| | | | Организационно-распорядительные документы Компании. Контроль выполнения всех требований ИБ отделом безопасности Компании | |
| ИПО.1 | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы | — | Перед вводом в эксплуатацию и в течении жизненного цикла защищаемой системы с персоналом должны проводиться следующие обучения: – первичный контроль и инструктаж при приеме на работу; – обучение методам работы и обслуживанию ПО и технических средств эксплуатируемых систем; – первичное и периодическое обучение порядку действий в нештатных ситуациях; – ознакомление под подпись с положениями Политики информационной безопасности Компании и обязательностью выполнения их требований; – закрепление в должностных инструкциях личной ответственности | 5,6,127,145,154,156,177,186,188,190,205,212 |
| ИПО.2 | Обучение персонала правилам безопасной работы | — | | 127,145,154,177,186,188,190,205,212 |
| ИПО.4 | Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы | — | | 127,145,156,177,186,188,190,212 |

| | | | | | |
|------|--------|------|------|-------|------|
| | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |

П37.2021.01-ИБ.П2

Лист28

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|----|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | 29 |

| | | | | |
|--|--|--|---|--|
| | | | за несоблюдение требований Политики информационной безопасности автоматизированных систем управления; –информирование о результатах актуализации, в рамках проведения аудитов, рисков информационной безопасности; –информирование о внесении изменений (обновления, изменение конфигурации и т.п.) в ПО и технические средства эксплуатируемых систем. | |
|--|--|--|---|--|

Итоговый состав технических и организационных мер по обеспечению безопасности информации для АСУ объекта может быть реализован одним или несколькими программными, аппаратно-программными средствами защиты информации, как уже встроенными в функционирующие СВТ и телекоммуникаций, так и дополнительно внедряемыми СрЗИ в проектируемое АСУ, а также организационными мероприятиями.

8. Архитектура подсистемы обеспечения информационной безопасности

Архитектура подсистемы обеспечения информационной безопасности модернизируемой Системы или, иными словами, решения, которые будут являться реализацией всех мер по обеспечению безопасности информации в проектируемой АСУ объекта и оптимально нейтрализующие актуальные угрозы безопасности информации заключаются в следующем:

- 1) наличие установленных сертифицированных средств межсетевого экранирования,
- 2) наличие установленных сертифицированных антивирусных средств защиты в актуальном состоянии,
- 3) использование сертифицированного ПО и сетевого оборудования,
- 4) организация программно-аппаратного разграничения интерфейса сетевых приложений,
- 5) действие утверждённой парольной политики,
- 6) организация и функционирование инженерно-технических мер, обеспечивающих строгую пропускную систему на объект и эффективную контролируемую зону,
- 7) наличие службы, персонала (администратора информационной безопасности) и своевременное реагирование на имеющиеся и появляющиеся актуальные УБИ, а также инциденты.

Организация системы связи модернизируемой системы виброконтроля оборудования Иркутской ГЭС по своей структуре является локальной системой и не предполагает присоединение к внешним сетям связи, в том числе и общего пользования. Она предусматривает установку на генерирующих агрегатах в пределах одной контролируемой зоны 9 датчиков вибрации, каждый из которых по физической линии соединен с модулями обработки аналоговых сигналов специализированного ПЛК. При поступлении служебной (сигнальной) аналоговой информации от датчиков вибрации ПЛК по заранее установленному алгоритму обрабатывает её и по организованной с помощью средств маршрутизации и коммутации проводной ЛВС (кабель типа «витая пара», ВОЛС) через резервируемый (в «горячем резерве») межсетевой экран со скоростью 100 Мбит/сек., направляет её на сервера PC1 и PC2, работающие также в «горячем резерве». На этих серверах информация аккумулируется (обрабатывается) в специализированном приложении и затем по проводной ЛВС для целей мониторинга поступает на АРМы руководителей и иных лиц оперативно-производственных служб. По истечению установленного времени эта информация поступает для архивирования на сервера арх. 1 и арх. 2.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 30 |

Для обеспечения безопасности передачи информации с ПЛК на АРМы должностных лиц ИГЭС и сервера осуществляется межсетевое экранирование на границе разнородных сетей.

Кроме того, каждое оконечное средство вычислительной техники (АРМ, сервер) входящее в защищаемое АСУ должно быть надёжно защищено от НСД и вирусного ПО, а информация о их состоянии аккумулироваться в центре мониторинга и оперативно доводиться до администратора ИБ.

Шифрование трафика не предполагается, так как модернизируемая Система локальная и находится полностью в пределах контролируемой зоны.

На самом модернизируемом объекте – ИГЭС для безопасности используется как физическое, состоящее в использовании в оптическом кабеле отдельных волокон, так и логическое (виртуальное), на основе технологии VLAN разделение на отдельные подсети. Система виброконтроля оборудования ИГЭС выделяется в свой индивидуальный обособленный сегмент ЛВС.

В качестве межсетевого экрана применяется специализированный программно-аппаратный межсетевой экран (МЭ), контролирующий весь информационный обмен с внешними (по отношению к нему) информационно-управляющими системами. На межсетевом экране «открыты» только требуемые для доступа к данным АСУ (системы виброконтроля) порты и сервисы. Все остальные порты и сервисы блокируются его настройками.

Передача информации от ПЛК на сервера и в последствии на АРМы строго регламентируется настройками межсетевого экрана на этапе пуско-наладочных работ. Перечень передаваемой информации устанавливается регламентом по эксплуатации проектируемой АСУ.

С серверов PC1 и PC2 АРМы должностных лиц Компании получают всю необходимую для мониторинга Системы информацию. Тем самым обеспечивается буферизация доступа (демилитаризованная зона), заключающаяся в том, что доступ из сети иного порядка чем промышленная сеть объекта осуществляется не к оборудованию проектируемой АСУ, а непосредственно только к выделенным для этого серверам.

С целью реализации всех требуемых мер по защите информационных ресурсов модернизируемой Системы и для унификации организационно-технических решений предусматривается в целом разделение ПОИБ Иркутской ГЭС на функциональные подсистемы в соответствии с определенными ролями. Предусматривается встраивание условно следующих функциональных подсистем:

- 1) управления информационной безопасностью;

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 31 |

- 2) защиты технических средств;
- 3) сетевой безопасности;
- 4) управления учетными записями;
- 5) регистрации событий безопасности;
- 6) антивирусной защиты;
- 7) централизованного управления средствами защиты и контроля защищенности.

Схема функциональной структуры приведена в документе П37.2021.01-ИБ.С2.

Назначение и принципы функционирования функциональных подсистем ПОИБ ИГЭС приведены в таблицы 8.1.

Таблица 8.1. – Назначение и принципы функционирования функциональных подсистем ПОИБ ИГЭС

| Функциональная подсистема ПОИБ Иркутской ГЭС | Назначение | Принципы функционирования (методы, механизмы реализации) | Реализуемые меры, в соответствии с приказом ФСТЭК от 25.12.2017 № 239 |
|--|--|---|--|
| Управления информационной безопасностью | Организационное сопровождение процесса обеспечений ИБ ИГЭС. Контроль выполнения требований ИБ. | Разработка организационно-распорядительной документации: – политика информационной безопасности; – организационно-распорядительные документы, соответствующие требованиям Политики. | ИАФ.0, УПД.0, ЗНИ.0, АУД.0, АВЗ.0, ОЦЛ.0, ОДТ.0, ЗТС.0, ЗИС.0, ИНЦ.0, УКФ.0, ОПО.0, ПЛН.0, ДНС.0, ИПО.0, ЗИС.1, ЗИС.3. |
| | | Выполнение требований положений Политики информационной безопасности и организационно-распорядительных документов контролируется отделом безопасности Компании. Обеспечение комплексного подхода и организация эшелонированной защиты ИР. | |
| | | Инвентаризация защищаемых ИР. Проведение аудитов информационной безопасности, анализ компьютерных инцидентов. Контроль работоспособности защищаемых систем. Планирование мероприятий ИБ. | АУД.1, АУД.2, АУД.10, ИНЦ.3, ИНЦ.4, ИНЦ.5, ПЛН.1, ПЛН.2, ДНС.1, ДНС.6 |

| | | |
|---------------|--------------|--------------|
| Инва. № подл. | Подп. и дата | Взам. инв. № |
| | | |

| | | | | | |
|------|--------|------|------|-------|------|
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |
| | | | | | |

П37.2021.01-ИБ.П2

| | | | | | | | | | |
|--------------|--------------|--------------|------|--------|------|------|-------|------|------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 33 |
| | | | | | | | | | |
| | | | Изм. | Кол.уч | Лист | №Док | Подп. | Дата | |

| Функциональная подсистема ПОИБ Иркутской ГЭС | Назначение | Принципы функционирования (методы, механизмы реализации) | Реализуемые меры, в соответствии с приказом ФСТЭК от 25.12.2017 № 239 |
|--|--|--|---|
| | | Управление процессом изменения конфигурации защищаемых систем. Управление обновлениями средств защиты информации (средства антивирусной защиты, межсетевые экраны), ПО серверов и АРМ. | УКФ.2, УКФ.3, ОПО.1, ОПО.2, ОПО.3, ОПО.4, АВЗ.4 |
| | | Доведение информации по обеспечению ИБ до персонала, проведение инструктажей, обучений. | ДНС.2, ДНС.5, ИПО.1, ИПО.2, ИПО.4 |
| | | Учет и управление доступом к машинным носителям информации. Уничтожение конфиденциальной информации на компонентах защищаемых систем при выведении из эксплуатации и (или) при передаче сторонним организациям. | ЗНИ.1, ЗНИ.2, ЗНИ.8 |
| | | Резервное копирование и восстановление ОС серверов и файлов средств защиты информации из резервных копий в случаях сбоя. Периодичность создания резервных копий, процедуры восстановления для каждой защищаемой системы определяется и документируется на этапе ввода систем в эксплуатацию под контролем Отдела безопасности Компании. | ОДТ.4, ОДТ.5, ОДТ.6 |
| Защиты технических средств | Защита от физического несанкционированного доступа к защищаемым ИР. Защита от внешних негативных воздействий на ИР. | Управление доступом к физическим ресурсам защищаемых систем производится посредством системы контроля и управления доступом (СКУД), а также применением систем безопасности (охранная сигнализация, видеонаблюдение, охрана людьми и т.п.). | ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5 |

| | | |
|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № |
| | | |
| | | |

| Функциональная подсистема ПОИБ Иркутской ГЭС | | | | | | Назначение | Принципы функционирования (методы, механизмы реализации) | Реализуемые меры, в соответствии с приказом ФСТЭК от 25.12.2017 № 239 |
|--|--------|------|------|-------|------|--|--|--|
| | | | | | | | Прокладка линий связи способом, затрудняющим НСД. Обеспечение бесперебойного электропитания компонентов защищаемых систем и средств защиты информации. | |
| | | | | | | | Размещение компонентов защищаемых систем производится с учетом требований по необходимости выполнения условий: – размещение в запираемых помещениях, оборудованных системами поддержания микроклимата, охранными системами и СКУД; – размещение в шкафах, оборудованных запираемыми дверями; – размещение АРМ в местах, исключающих несанкционированное чтение данных с экранов. | |
| Сетевой безопасности | | | | | | Сегментирование сетей, физическое и логическое отделение сетей защищаемых систем. Защита от подмены доверенного оборудования. Защита аутентификационной информации при передаче Блокирование недокументированных точек подключения к внешним сетям. | Применением компонентов СрЗИ имеющих следующую функциональность: – межсетевое экранирование сетевого трафика (локальный программный МЭ на АРМ и серверах); – межсетевое экранирование сетевого трафика (аппаратные МЭ на границах периметра сегментов сети, а также на границах разнотипных сетей. – Организация демилитаризованной зоны Сегментирование сетей учитывая разграничение доступа пользователей/устройств к ИР разных сегментов сети на основании правил межсетевого взаимодействия. | ИАФ.7, УПД.14, ЗНИ.5, ЗНИ.7, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6, ЗИС.8, ЗИС.34 |
| | | | | | | | | |
| | | | | | | П37.2021.01-ИБ.П2 | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | Лист 34 | | |

| | | |
|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № |
| | | |

| Функциональная подсистема ПОИБ Иркутской ГЭС | Назначение | Принципы функционирования (методы, механизмы реализации) | Реализуемые меры, в соответствии с приказом ФСТЭК от 25.12.2017 № 239 |
|--|------------|---|---|
| | | Идентификация (фильтрация) по MAC-адресам на портах активного сетевого оборудования (при наличии технической возможности имеющегося телекоммуникационного оборудования). | |
| | | использование безопасных протоколов обмена при передаче аутентификационной информации (https, ssh и пр.) | |
| | | Создание изолированной сети для нужд защищаемой системы. | |
| | | Программное и аппаратное блокирование потенциальной возможности удаленного несанкционированного доступа и управления компонентами защищаемых систем (при наличии технической возможности). | |
| | | Блокирование (исключение) потенциально возможных подключений сегментов сетей защищаемых систем к сетям связи общего пользования (в частности, Интернет) и контроль доступа из внешних информационных (автоматизированных) систем. | |
| | | Отключение неиспользуемых интерфейсов (портов) ввода/вывода с применением встроенных в компоненты защищаемой системы инструментов. | |
| | | Опечатывание неиспользуемых интерфейсов (портов) ввода/вывода; контроль подключения носителей информации с применением специализированных инструментов, входящих в состав СрЗИ ИГЭС. | |

| | | | | | |
|------|--------|------|------|-------|------|
| | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |

П37.2021.01-ИБ.П2

Лист 35

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 36 |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | |

| Функциональная подсистема ПОИБ Иркутской ГЭС | Назначение | Принципы функционирования (методы, механизмы реализации) | Реализуемые меры, в соответствии с приказом ФСТЭК от 25.12.2017 № 239 |
|--|--|---|---|
| Управления учетными записями | Идентификация, авторизация, разграничение доступа пользователей и устройств защищаемых систем. | <p>Организация подсистемы управления учетными записями с применением дополнительных специализированных инструментов, входящих в состав СрЗИ ИГЭС:</p> <ul style="list-style-type: none"> – идентификация и проверка подлинности субъектов доступа при входе в ОС по идентификатору и паролю; – разграничение прав доступа и контроль доступа субъектов к защищаемым ИР на уровне; – ОС ограничение неудачных попыток аутентификации; – блокировка сеанса по истечению времени, а также вручную администратором и(или) пользователем; – идентификация серверов и АРМ по логическим именам; – разграничение прав доступа к сменным носителям информации на основе серийных номеров (при наличии технической возможности). | <p>ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.14</p> |
| | | Применение встроенных в компоненты защищаемых систем инструментов аутентификации. | |
| | | Контроль управления учетными записями Отделом безопасности Компании. | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|------|-------------------|--------------|--------------|--|--|--|--|--|--|--|--|--|-------------------|--|------|--|--|--|--|--|--|--|--|--|----|--|
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | Взам. инв. № | Подп. и дата | Изм. № подл. | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table><tr><td>Централизованного управления средствами защиты и контроля защищенности</td><td>Централизованное управление средствами защиты информации. Контроль защищённости.</td><td>компьютерных программ (вирусов); – формирование отчетов о попытках заражения; – защита от DOS, DDOS-атак).</td><td>Применение компонентов централизованного управления и мониторинга, входящих в состав СрЗИ ИГЭС: – контроль портов (интерфейсов) ввода/вывода; – контроль подключения машинных носителей; – формирование паспорта ПО</td><td>ОЦЛ.1, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6.</td></tr></table> | | | | | | | | | | | | Централизованного управления средствами защиты и контроля защищенности | Централизованное управление средствами защиты информации. Контроль защищённости. | компьютерных программ (вирусов); – формирование отчетов о попытках заражения; – защита от DOS, DDOS-атак). | Применение компонентов централизованного управления и мониторинга, входящих в состав СрЗИ ИГЭС: – контроль портов (интерфейсов) ввода/вывода; – контроль подключения машинных носителей; – формирование паспорта ПО | ОЦЛ.1, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6. | | | | | | | | | | | | | | | |
| Централизованного управления средствами защиты и контроля защищенности | Централизованное управление средствами защиты информации. Контроль защищённости. | компьютерных программ (вирусов); – формирование отчетов о попытках заражения; – защита от DOS, DDOS-атак). | Применение компонентов централизованного управления и мониторинга, входящих в состав СрЗИ ИГЭС: – контроль портов (интерфейсов) ввода/вывода; – контроль подключения машинных носителей; – формирование паспорта ПО | ОЦЛ.1, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table><tr><td colspan="6"></td><td colspan="2">П37.2021.01-ИБ.П2</td><td colspan="2">Лист</td></tr><tr><td colspan="6"></td><td colspan="2"></td><td colspan="2">37</td></tr></table> | | | | | | | | | | | | | | | | | | П37.2021.01-ИБ.П2 | | Лист | | | | | | | | | | 37 | |
| | | | | | | П37.2021.01-ИБ.П2 | | Лист | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | 37 | | | | | | | | | | | | | | | | | | | | | | | |

| Функциональная подсистема ПОИБ Иркутской ГЭС | Назначение | Принципы функционирования (методы, механизмы реализации) | Реализуемые меры, в соответствии с приказом ФСТЭК от 25.12.2017 № 239 |
|--|--|---|---|
| Регистрации событий безопасности | Контроль устройств и целостности ПО, сбор и регистрация событий безопасности. | Применение специализированных инструментов, входящих в состав СрЗИ ИГЭС, имеющих следующую функциональность: <ul style="list-style-type: none"> – контроль состава и целостности ПО; – регистрация событий безопасности; – централизованный сбор, хранение и архивирование журналов; – контроль устройств, подключаемых к АРМ и Серверам; – контроль состояния устройств с возможностями блокирования АРМ (Сервера) при изменении состояния заданных устройств; – оповещение ответственных лиц о событиях безопасности. | АУД.3, АУД.4, АУД.6, АУД.7, АУД.8 |
| Антивирусной защиты | Защита АРМ и серверов от деструктивных действий вредоносного ПО. | Применение компонентов антивирусной защиты, входящих в состав СрЗИ ИГЭС: <ul style="list-style-type: none"> – антивирусное ПО (установка на серверы и АРМ); – защита АРМ и серверов (потокковая и периодическая проверка на наличие вирусов); – обновление базы данных признаков вредоносных компьютерных программ (вирусов); – формирование отчетов о попытках заражения; – защита от DOS, DDOS-атак). | АВЗ.1, АВЗ.2, АВЗ.4, ЗИС.3, ЗИС.34 |
| Централизованного управления средствами защиты и контроля защищенности | Централизованное управление средствами защиты информации. Контроль защищенности. | Применение компонентов централизованного управления и мониторинга, входящих в состав СрЗИ ИГЭС: <ul style="list-style-type: none"> – контроль портов (интерфейсов) ввода/вывода; – контроль подключения машинных носителей; – формирование паспорта ПО | ОЦЛ.1, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6. |

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------------|--|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 38 | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | |

| Функциональная подсистема ПОИБ Иркутской ГЭС | Назначение | Принципы функционирования (методы, механизмы реализации) | Реализуемые меры, в соответствии с приказом ФСТЭК от 25.12.2017 № 239 |
|--|------------|---|---|
| | | (инвентаризация систем); – контроль целостности файлов и папок на АРМ и серверах; – блокировка АРМ по событиям безопасности; – централизованное управление межсетевыми экранами; – реагирование на события безопасности путем воздействия на средства защиты информации для блокирования угроз; – контроль целостности программных компонентов средств защиты информации. Для мониторинга защищаемых систем на предмет наличия уязвимостей предусматривается применение программного сканера уязвимостей. | |

| Инв. № подл. | Подп. и дата | Взам. инв. № |
|--------------|--------------|--------------|
| | | |

В качестве аппаратно-программного СРЗИ будет применяться шлюз безопасности (аппаратный модуль) CheckPoint в аппаратной реализации Appliance 3100, внешний вид, которого представлен на рисунке 1.



- 1) межсетевого экрана (Firewall);
- 2) построение частных виртуальных сетей VPN (IPSec VPN);
- 3) отображения журналов, основанных на учётных записях пользователей, вместо журналов, основанных на их IP-адресах, (осведомлённость пользователей - User Awareness);
- 4) приоритезация трафика (QoS);

- 5) межсетевой экран уровня приложений (Application Control);
- 6) безопасность Web с функционалом proxy (URL Filtering);
- 7) система предотвращения вторжений (IPS);
- 8) защита от ботнет сетей (Anti-Bot);
- 9) потоковый антивирус (Antivirus);
- 10) защита корпоративной почты (Anti-Spam).

Аппаратный модуль CheckPoint Appliance 3100 в настольном форм-факторе (рис.1) имеет следующие основные технические характеристики:

- 1) 6 встроенных портов (интерфейсов) 10/100/1000Base-T RJ-45;
 - 2) 2 порта (интерфейса) USB 2.0;
 - 3) 1 консольный порт (интерфейс) RJ45 (для последовательного подключения к устройству);
 - 4) 1 консольный порт MiniUSB (для последовательного подключения к устройству);
 - 5) 1 скрытая кнопка аппаратного сброса (для булавки);
 - 6) 1 скрытая кнопка (для булавки) восстановления заводских настроек;
 - 7) 1 ЦПУ (4 физических ядра, 4 виртуальных ядра);
 - 8) 8 ГБ ОЗУ;
 - 9) 1 блок питания (40Вт, переменный ток 110-240В, 47-63Гц,);
 - 10) 29,5Вт потребляемой мощности;
 - 11) один SSD на 240ГБ (или HDD на 320ГБ);
 - 12) пропускная способность:
 - Брэндмауэра – 4000 Мбит/с,
 - VPN – 1700 Мбит/с,
 - IPS/IDS – 1100 Мбит/с.
 - 13) до 3200000 подключений фаервола;
 - 14) до 40000 подключений фаервола за секунду;
 - 15) операционная система – Gaia (R77.30, так и R80.X0);
 - 16) резервирование BIOS в модуле (резервный образ BIOS);
 - 17) сертификация: - UL, CB, CE, TUV GS - FCC, CE, VCCI, RCM/C-Tick.
 - 18) общее количество физических и виртуальных (VLAN) интерфейсов на устройство: 1024/4096 (единый шлюз/с виртуальными системами);
 - 19) пассивная и активная агрегация соединений 802.3ad;
 - 20) режимы (уровни) функционирования – прозрачный (2) и маршрутизация (3);
- В программное обеспечение CheckPoint Appliance 3100 входит несколько программных модулей:

| | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | Лист |
| | | | | | | | |
| | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | |
| | | | | | | 40 | |

1) шлюз безопасности (Security Gateway) – программный модуль шлюза безопасности, устанавливаемый на аппаратную часть CheckPoint и выполняющий функции межсетевого экрана, потокового антивируса, антибота, IPS и иных, контролирующий выполнение корпоративной политики безопасности в качестве системы обеспечения безопасности;

2) сервер управления безопасностью (или шлюзами) (Security Management Server) – сервер, используемый администратором для управления (централизованного управления) политикой безопасности и на котором хранятся базы данных и политики безопасности Компании, в последующем загружаемые в шлюз безопасности, а также для хранения Лог-сервера и обработки встроенной системой анализа и корреляции событий;

3) смарт консоль (Smart Console) – приложение с графическим интерфейсом (клиентская консоль), устанавливаемое, как правило на АРМ администратора для подключения к серверу управления безопасностью и позволяющее управлять (изменять) различными аспектами выполнения политик безопасности на сервере управления, а уже после этого и применять настройки к шлюзу безопасности.

В свою очередь для сервера управления безопасностью также предусмотрен следующий функционал («программные блейды»):

- 1) централизованное управление политиками (Network Policy Management);
- 2) централизованное управление агентами Check Point (Endpoint Policy Management);
- 3) централизованный сбор и обработка логов (Logging & Status);
- 4) управление безопасностью из браузера (Management Portal);
- 5) контроль над изменением политик, аудит изменений и т.д. (Workflow);
- 6) интеграция с LDAP (User Directory);
- 7) автоматизация управления шлюзами (Provisioning);
- 8) система отчетности (Smart Reporter);
- 9) анализ и корреляция событий (SIEM) (Smart Event);
- 10) автоматическая проверка настроек и выдача рекомендаций (Compliance).

Архитектура блейдов позволяет использовать только действительно нужные для разрабатываемой Системы функции.

Существует два основных сценария функционирования (внедрения) CheckPoint Appliance 3100 для защиты информационных ресурсов Компании:

1. Основной шлюз (Standalone) – Check Point устанавливается как устройство защиты периметра и администрируется локально, а все его компоненты, ответственные как за управление, так и за реализацию политики безопасности (сервер

| | | | | | | | | |
|--------------|--------------|--------------|---|--------|------|------|-------|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | <p>9) анализ и корреляция событий (SIEM) (Smart Event);</p> <p>10) автоматическая проверка настроек и выдача рекомендаций (Compliance).</p> <p>Архитектура блейдов позволяет использовать только действительно нужные для разрабатываемой Системы функции.</p> <p>Существует два основных сценария функционирования (внедрения) CheckPoint Appliance 3100 для защиты информационных ресурсов Компании:</p> <p>1. Основной шлюз (Standalone) – Check Point устанавливается как устройство защиты периметра и администрируется локально, а все его компоненты, ответственные как за управление, так и за реализацию политики безопасности (сервер</p> | | | | | |
| | | | П37.2021.01-ИБ.П2 | | | | | |
| | | | Изм. | Кол.уч | Лист | №Док | Подп. | Дата |

| |
|------|
| Лист |
| 41 |

управления безопасностью и шлюз безопасности), устанавливаются на одном аппаратном устройстве (компьютере или модуле).

2. Шлюз для филиала (Distributed) – аппаратная часть Check Point с установленным на ней программным модулем шлюза безопасности монтируется в подразделении Компании, а сервер управления безопасностью устанавливается на отдельном от шлюза безопасности аппаратном или виртуальном средстве, а управляется осуществляется централизованно с помощью смарт консоли, например из головного офиса Компании.

Шлюз безопасности может работать в двух основных режимах:

1. Routed — маршрутизация, когда шлюз используется как L3 устройство и маршрутизирует трафик через себя, т.е. Check Point является шлюзом по умолчанию для защищаемой сети.

2. Bridge — прозрачный, когда шлюз устанавливается как обычный «мост» и пропускает через себя трафик на втором уровне (OSI).

Режим Routed является основным и самым распространенным вариантом, а Bridge обычно применяется, когда нет возможности изменить уже существующую инфраструктуру, в том числе менять топологию сети и IP – адресации, а также в нём имеются некоторые ограничения по функционалу,

В защищаемой Системе будет использоваться режим Routed.

На усмотрение Заказчика возможна реализация CheckPoint 3100 в «горячем резервировании», то есть в качестве аппаратно-программного кластера, состоящего из одновременно работающих 2-х одинаковых аппаратных модулей CheckPoint 3100. В этом варианте защиты оба члена кластера с полной высокой доступностью используют продукты Security Management Server и Security Gateway, где один член кластера активен, а другой находится в режиме ожидания. Если в активном члене кластера возникает сбой, который влияет на продукт сервера управления безопасностью и продукт шлюза безопасности, то оба этих продукта переключаются на резервный член кластера. Если продукт Security Management Server на активном элементе кластера выходит из строя, то только продукт Security Management Server переключается на резервный элемент кластера, а продукт шлюза безопасности на первом элементе кластера продолжает функционировать.

Если продукт шлюза безопасности на активном члене кластера выходит из строя, то только продукт шлюза безопасности переключается на резервный член кластера, а продукт Security Management Server на первом элементе кластера продолжает функционировать.

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|----|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | 42 |

Для монтажа CheckPoint 3100 (в том числе и в кластерном варианте) в стандартную 19" телекоммуникационную стойку возможно приобретение дополнительного комплекта крепления сразу на 2 модуля.

Специально для целей непрерывности технологических процессов АСУ ТП компания «Лаборатория Касперского» разработала комплексное решения Kaspersky Industrial Cyber Security (Далее - KICS), которое состоит из 3-х самостоятельных программных модулей:

1) Kaspersky Industrial Cyber Security for Nodes (Далее - KICS for Nodes) – для комплексной защиты серверов и рабочих станций (АРМ) от угроз ИБ в промышленной сети и обеспечивающий в них:

–контроль целостности на основе результатов анализа журналов событий Windows, в том числе и с помощью отдельного компонента (PLC Integrity checker) осуществляется мониторинг целостности (изменения) проектов ПЛК на основе ее hash суммы,

–контроль активности ПО (запуска приложений, программ),

–обнаружение уязвимых приложений на АРМ и серверах,

–контроль использования устройств (USB-носители, внешние устройства иного типа),

–контроль подключения к Wi-Fi сетям,

–антивирусную защиту, предотвращающую заражение узлов вредоносным ПО, в том числе и защиту от шифрования,

–управление локальным сетевым экраном обеспечивая блокирование внешних сетевых соединений на уровне хоста (сервера, АРМ).

KICS for Nodes обеспечивает надежную защиту конечных устройств и не влияет на технологический процесс, сертифицирован ведущими производителями средств автоматизации (АСУ ТП), потребляет намного меньше вычислительных ресурсов чем современные корпоративные программные СрЗИ конечных устройств из-за наличия функционала самоограничения потребления ресурсов. Он также не требует перезагрузки системы при установке, обновлении и может работать без перезагрузки до 6 месяцев, обеспечивает работы в полностью неблокирующем режиме, а также обнаружения угроз нулевого дня.

2) Kaspersky Industrial Cyber Security for Networks (Далее - KICS for Networks) – для пассивного мониторинга сетевого трафика промышленной сети и обнаружение угроз, разворачиваемый на специально выделенном для этих целей аппаратном сервере, подключаемом к промышленной сети. Модуль предназначен для обнаружения атак, ошибок и аномалий в промышленной сети, реализует функционал сетевого

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 43 |

мониторинга и глубокого анализа промышленного трафика. Он работает с копией трафика взятой (подключенной) через SPAN интерфейс коммутатора (маршрутизатора) промышленной сети, поэтому не замедляет скорость передачи данных, не влияет на ход технологического процесса и реализует:

- пассивную идентификацию и инвентаризацию устройств в сети и тем самым обнаруживает новые подключения в промышленной сети, в том числе сетевые коммуникации между промышленными узлами,
- нахождение сетевых атак с помощью компоненты обнаружения вторжений IDS,
- телеметрический анализ технологических процессов практически в режиме реального времени,
- глубокий анализ промышленного трафика, обеспечивая мониторинг за несанкционированными конфигурационными командами, поступающими на ПЛК, а также нахождением значений параметров технологического процесса в допустимых пределах и состояниях,
- интеграцию через API-интерфейс со сторонними системами обнаружения.

3) Kaspersky Security Center (Далее – KSC) – для централизованного мониторинга и управления компонентами безопасности KICS и реализует:

- управление системами, состоящее в централизованном сборе системных данных, централизованном развертывании программного обеспечения (установка агентов), мониторинге уязвимостей и управление исправлениями, расширении клиентских средства управления,
- централизованное обновление сигнатурных баз,
- централизованное управление политиками безопасности, удаленное планирование и выполнение задач, ролевое управление,
- отчеты и уведомления, состоящие в ведении журналов событий, информационных панелей, отчетов, уведомлений,
- интеграцию с SIEM-системами, с человеко-машинным интерфейсом.

На все защищаемые объекты (АРМ и сервера) проектируемой АСУ, специально для защиты сложных промышленных сред должны быть установлены компоненты KICS for Nodes, а на АРМ администратора информационной безопасности кроме этого модуля ещё и модуль KSC.

Оборудование межсетевого экранирования на проектируемой АСУ устанавливается на границах подключений технологической сети уровня САУ к серверам и АРМ должностных лиц Компании (уровня ОПС). Для защищаемой АСУ оборудование, по существу, представляет собой аппаратные изделия размерами 1U для монтажа в 19" стойку и монтируется в шкаф сейсмоконтроля ШСК в соответствии с

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 44 |

внутренним составом этого шкафа, изложенного в документе П37.2021.01.001 и размещаемого в «Аппаратной» технического здания ИГЭС.

ПОИБ проектируемой (модернизируемой) АСУ построена по эшелонируемому, многоуровневому принципам с «горячим» резервированием основных элементов (кластеризацией) и ЗИП, достаточным для обеспечения приемлемого, в соответствии с Политикой информационной безопасности для Компании риска в возможных нештатных ситуациях.

При выборе средств активного сетевого оборудования и аппаратно-программных средств защиты информации обязательно учитываются требования Политики Компании-заказчика и установленные корпоративные стандарты по ИБ.

Кроме того, все аппаратно-программные (технические) средства в проектируемой АСУ должны обладать (и выполнять) следующими возможностями:

1. Отключение всех служб и сервисов на АРМах и серверах АСУ, не используемых в процессе эксплуатации и сопровождения АСУ (при наличии технической возможности). При необходимости данные службы, сервисы и функции должны иметь возможность включения, уполномоченными лицами Компании (администраторами), на определенный период времени в соответствии с требованиями по управлению конфигурацией АСУ.

2. Все коммуникационные интерфейсы (порты), порты ввода-вывода и интерфейсы на оборудовании элементов АСУ, включая АРМы, сервера, телекоммуникационного оборудования, не используемого непосредственно в процессе эксплуатации и сопровождения АСУ, должны быть отключены в BIOS или надёжно, аппаратно-программно, программно заблокированы и (или) опечатаны. Такая возможность реализуется при вводе ПОИБ в эксплуатацию. Обеспечивается настройка атрибутов доступа, отличных от значений «по умолчанию», привязка интерфейсов (портов) к MAC-адресам хостов;

3. Для ограничения доступа к ресурсам в BIOS АРМ, серверов, используемых в АСУ, должна быть реализована возможность запрета загрузки операционных систем с иных носителей, кроме жесткого диска компьютеров и серверов, а также установка пароля на вход в BIOS, обеспечение целостности BIOS.

4. Функция автозапуска сменных носителей должна быть заблокирована в BIOS.

5. Защитой проектируемой АСУ от НСД предусматривается разграничением доступа к оборудованию на уровне авторизации. Проверка подлинности осуществляется с помощью предъявления логина и пароля. Кроме локальной проверки пользователя имеется возможность интеграции со службами аутентификации

| | |
|--------------|--|
| Взам. инв. № | |
| Подп. и дата | |
| Инв. № подл. | |

| | | | | | | | |
|------|--------|------|------|-------|------|-------------------|------|
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | Лист |
| | | | | | | | 45 |

серверной ОС и СРЗИ. Доступ к проектируемой Системе должен предоставляться по принципу минимальной достаточности, заключающегося в том, что у оператора или иного должностного лица Компании должны быть права только на просмотр или мониторинг информации в рамках выполняемых производственных функций, а у инженера (администратора) – права на изменение настроек или иными словами реализация меры УПД 5 - Назначение минимально необходимых прав и привилегий.

Основное техническое решение ПОИБ проектируемого объекта представлено на структурной схеме комплекса технических средств защиты информации ПЗ7.2021.01-ИБ.С1, а схема функциональной структуры на ПЗ7.2021.01-ИБ.С2.

Все технические решения условно можно отнести к функциональным подсистемам

- 1) сетевой безопасности;
- 2) управления учетными записями;
- 3) регистрации событий безопасности;
- 4) антивирусной защиты;
- 5) централизованного управления средствами защиты и контроля защищенности;

9.1. Подсистема сетевой безопасности

Подсистема сетевой безопасности предназначена для сегментирования информационно-телекоммуникационных сетей, то есть физического и логического их разделения для безопасного функционирования защищаемой АСУ, а также защиты от подмены доверенного объекта (оборудования), организация демилитаризованной зоны, блокирования недокументированных (потенциально несанкционированных) точек подключения к внешним сетям за пределами КЗ. Она включает в себя реализацию следующих мер по обеспечению безопасности информации: ИАФ.7, УПД.14, ЗНИ.5, ЗНИ.7, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6, ЗИС.8, ЗИС.34 и состоит в следующем.

1. Межсетевое экранирование сетевого трафика, предусматривающее программно-аппаратные МЭ на границах защищаемого сегмента сети, а также локальный программный МЭ на АРМ и серверах.

2. Сегментирование сетей с учётом разграничения доступа пользователей/устройств к информационным ресурсам разных сегментов сети на основании правил межсетевого взаимодействия.

3. Идентификация (фильтрация) по MAC-адресам на портах активного сетевого оборудования.

| | | | | | | | | | |
|--------------|--------------|--------------|--|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | <p>1. Межсетевое экранирование сетевого трафика, предусматривающее программно-аппаратные МЭ на границах защищаемого сегмента сети, а также локальный программный МЭ на АРМ и серверах.</p> <p>2. Сегментирование сетей с учётом разграничения доступа пользователей/устройств к информационным ресурсам разных сегментов сети на основании правил межсетевого взаимодействия.</p> <p>3. Идентификация (фильтрация) по MAC-адресам на портах активного сетевого оборудования.</p> | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | ПЗ7.2021.01-ИБ.П2 | | | Лист |
| | | | | | | | | | 46 |

4. Использование безопасных протоколов обмена при передаче аутентификационной информации (https, ssh и пр.).
5. Создание изолированной сети для нужд проектируемой АСУ.
6. Программное и аппаратное блокирование возможности несанкционированного удаленного доступа и управления компонентами АСУ.
7. Блокирование (исключение) подключений сегментов АСУ к несанкционированным, открытым сетям связи общего пользования (в частности, Интернет).
8. Отключение (блокирование) неиспользуемых интерфейсов (портов) ввода/вывода с применением механизмов, встроенных в операционные системы АРМ и серверов, и сетевых компонентов АСУ.
9. Опечатывание неиспользуемых интерфейсов ввода/вывода.
10. Контроль подключения носителей информации с применением специализированных инструментов, входящих в состав ПОИБ проектируемой АСУ объекта, а также блокировки в ОС функции автозапуска сменных носителей.

Подсистема сетевой безопасности условно структурно состоит из внешнего и внутреннего промышленно-информационных контуров, разделённых межсетевым экраном, которые взаимно дополняют друг друга и реализуют все меры эшелонируемой защиты информации. Внешний контур обеспечивает безопасность защищаемых объектов уровня ОПС при взаимодействии между собой и при возможном взаимодействии с производственными (корпоративными) сетями и иными внешними сетями за исключением сетей общего пользования. Внутренний контур обеспечивает безопасность всех защищаемых объектов на уровнях САУ и полевого, что будет являться реализацией ЗИС 5. (организация демилитаризованной зоны).

Техническими решениями по организации локально-вычислительной сети на объекте для нужд проектируемой Системы (задач АСУ ТП) предусмотрено использование физически выделенной ЛВС (обособленной) от иных сетей.

IP-адресация разрабатывается (корректируется) специализированными подразделениями Заказчика с учётом корпоративных, структурных, географических или топологических особенностей на этапе ввода в эксплуатацию объекта и непосредственного проведения пуско-наладочных работ.

Разделение сетей уровня ОПС и САУ, проектируемой АСУ осуществляться посредством резервируемого аппаратно-программного МЭ.

Аппаратный модуль CheckPoint 3100 (рис.1) на фронтальной (передней) панели содержит: 5-ть интерфейсов RJ45 для подключения устройств, один интерфейс RJ45 для управления модулем и обозначенный буквами MGMT, 2-а интерфейса USB2.0 для

| | | | | | | | | | |
|--------------|--------------|--------------|-------------------|-------|------|--|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | П37.2021.01-ИБ.П2 | | | | | | |
| | | | 47 | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | | | | |

инсталляции ISO, по одному консольному интерфейсу RJ45 и MiniUSB для последовательного подключения к устройству и обозначенные буквами CONSOLE. На задней панели модуль CheckPoint 3100 располагаются гнездо для подключения кабеля адаптера электропитания и главный переключатель электропитания.

Аппаратный модуль CheckPoint 3100 смонтирован на правой боковой панели шкафа сейсмоконтроля и средствами администрирования для него назначены внутренние интерфейсы (порты) 1, 2, подключаемые Ethernet-кабелями (патч-кордами) к интерфейсам (портам) защищаемых модулей ПЛК, а назначенные внешними интерфейсами (портами) 3, 4 подключаются патч-кордами через промышленные медиаконвертеры по ВОЛС к существующим маршрутизаторам, к интерфейсам которого так же подключены сервера и АРМ руководителей и работников ИГЭС. Администрирование CheckPoint 3100 осуществляется через его специальный интерфейс, обозначенный буквами MGMT с АРМ администратора. Резервный аппаратный модуль CheckPoint 3100 находится в ЗИП.

МЭ может создаваться и как отказоустойчивый кластер из 2-х одновременно работающих модулей CheckPoint 3100 (Кластер МЭ – Далее). Кластер МЭ будет обеспечивать «горячее» аппаратно-программное резервирование и автоматическое переключение с основного устройства и программного обеспечения на резервные (аппаратное и программное) при выходе основного из строя.

Для создания Кластера МЭ необходимо смонтировать в 19” телекоммуникационную стойку 2-а модуля CheckPoint 3100, возможно и при помощи приобретаемого дополнительного комплекта крепления (полка в стойку на одно/два шасси для шлюзов безопасности 3000) и соединить их между собой (например 5-ми интерфейсами, назначенными для синхронизации) Ethernet-кабелем (патч-кордом). Необходимо учесть, что для интерфейсов синхронизации используется перекрестный кабель (или специальный коммутатор).

Детальная информация об установке, настройке и порядке использования (эксплуатации) аппаратного модуля CheckPoint 3100 или Кластера МЭ на его основе содержится в эксплуатационной документации на него – Руководстве администратора, выпускаемой производителем «CheckPoint» и охраняется авторским правом по её распространению, копированию и декомпиляции. Воспроизведение любой части указанной документации по CheckPoint 3100 в любой форме и любыми средствами без предварительного письменного разрешения компании «Check Point» запрещено. Поэтому в данной документации представлен только общий порядок основной установки и настройки модуля CheckPoint 3100 и кластера МЭ CheckPoint 3100, включающий следующий план действий.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 48 |

Первым этапом необходимо произвести начальную настройку аппаратного модуля или подготовку последовательно членов кластера МЭ при условии, что на них уже установлены ОС и специализированное ПО. Для этого после включения на каждом из них электропитания и подключившись компьютером (ноутбуком) администратора к разъему управления (MGMT) на передней панели модуля (посредством имеющегося в комплекте поставки сетевого Ethernet-кабеля) произвести необходимые установки в соответствующих полях ПО.

К таким установкам следует отнести первоначальный «IP-адрес», назначенный каждому модулю (например, 192.168.1.2), «Маска подсети» (например, 255.255.255.0), оставив незаполненными поля «Шлюз по умолчанию» и «Параметры DNS».

Затем на компьютере необходимо запустить веб-браузер и ввести в поле адреса: <https://192.168.1.1>, а в открывшемся окне авторизации выполнить вход с помощью установленных по умолчанию имени пользователя и пароля от учетной записи системного администратора (admin/admin) нажав после их введения кнопку «Login» («Войти»). После этого автоматически запустится мастер начальной настройки, который проведет через процедуру настройки соединения, где необходимо будет указать все необходимые параметры, в том числе и установку на каждый модуль ПО шлюза безопасности (Security Gateway) и сервера управления безопасностью (Security Management Server) с функционалом «менеджмент сервер».

Итогом начальной настройки должно стать, что каждый модуль кластера МЭ настроен как сервер управления безопасностью (с установленной и активированной лицензией для кластера) и как шлюз безопасности, а в дополнительных параметрах каждого модуля выбраны объект, являющийся частью кластера и какой модуль является «Основной», а какой «Дополнительный» элементами, а также настроены учетные данные администратора для сервера управления безопасностью.

Вторым этапом необходимо установить на компьютер (APM) администратора Смарт консоль (SmartConsole). Для этого зайдя на веб-интерфейс одного из модулей либо же менеджмент сервера и выбрав для скачивания в разделе «Maintenance», пункт «Download Smart Console», нажать в последствии кнопку «Download». После скачивания смарт консоли необходимо запустить процесс её инсталляции, где для её успешной установки понадобятся дополнительные программные компоненты (MS NET Framework 4 и т.п.). Определить разрешенных клиентов SmartConsole и протокол обмена с модулями.

Следующим этапом необходимо определить и настроить тип (внешний или внутренний) и IP-адрес для интерфейсов всех участников кластера, а также точно синхронизировать часы модулей с точностью до одной секунды.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 49 |

Убедится, что каждая сеть (внутренняя, внешняя, синхронизация, DMZ и т. д.) при установке IP-адресации настроена на отдельную VLAN (коммутатор или концентратор). Следует иметь ввиду, что IP-адреса кластера являются виртуальными, поскольку они не принадлежат какому-либо физическому интерфейсу, поэтому для внутренней сети IP-адреса модулям кластера МЭ могут быть назначены, например соответственно: 10.10.0.1 и 10.10.0.2, а для внешней соответственно каждому модулю: 192.168.10.1 и 192.168.10.2. Необходимо назначить по одному сетевому интерфейсу синхронизации для каждого члена кластера, например: 10.0.10.1 и 10.0.10.2, соединив их друг с другом.

После всех необходимых установок необходимо перезагрузить аппаратные модули.

Для администрирования CheckPoint 3100 необходимо организовать отдельную VLAN и для этого его специальные интерфейсы управления на каждом модуле патч-кордами через промышленные медиаконвертеры по ВОЛС подключить к существующим маршрутизаторам, к которым также подключен сетевыми интерфейсами АРМ администратора и согласно руководству администратора настроить все необходимые функции («программные блейды») МЭ.

Необходимо в соответствии с регламентом функционирования защищаемой Системы настроить в ПО CheckPoint 3100 маршрутизацию. Целесообразно настроить статические маршруты для всех устройств, которые определяют «пункт назначения» и один или несколько путей (маршрутов) с определением приоритетов для выбора пути маршрута.

Обязательно необходимо администрировать «Политики безопасности», состоящие из набора правил и настроек, которые управляют сетевым трафиком и обеспечивают соблюдение руководящих принципов Компании по защите данных и доступу к ресурсам Системы с проверкой пакетов. И для это необходимо внести соответствующие данные в определённые поля. В Check Point предоставляется несколько типов политик безопасности.

1. Политика контроля доступа, состоящая из следующих частей:

1) База правил контроля доступа, содержащая унифицированные простые и детализированные правила для управления доступом из указанных источников к указанным местам назначения по указанным протоколам. При активации программного блейда «Identity Awareness» на шлюзах безопасности, возможно использовать объекты роли доступа в качестве источника и назначения в правиле, что позволяет легко создавать правила для отдельных пользователей или различных их групп.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 50 |

2) База правил NAT, содержащая автоматические и ручные правила трансляции сетевых адресов (NAT).

3) База правил рабочего стола, устанавливаемая на сервере управления безопасностью для контроля доступа на удаленные APM пользователей (удаленного доступа)

2. Политика предотвращения угроз, состоящая в проверки соединения на наличие ботов и вирусов, на основе данных вредоносных программ и сетевые объекты (Базы правил).

3. Политика проверки HTTPS, позволяющая проверять трафик HTTP / HTTPS на программных блейдах: антибот, антивирус, контроль приложений, осведомленность о содержании (осведомленность о данных), предотвращение потери данных, IPS, эмуляция угрозы, URL-фильтрация.

4. Политика предотвращения потери данных, заключающаяся в предотвращении непреднамеренной утечки данных, обнаруживающая защищенные данные до того, как они покинут ресурсы Компании.

5. Географическая политика, состоящая в географическом расположении объектов защиты.

6. Политика мобильного доступа, управляющая группами пользователей, имеющих доступ к определённым приложениям и подключенных через шлюз безопасности мобильного доступа.

Функционал SmartConsole, установленной на APM администратора имеет ряд инструментов, позволяющих ему решать задачи управления политиками как на этапе определения (группировка пакетов политик различных типов для совместной установки на одних и тех же объектах установки, связав их с определённым шлюзом) так и для дальнейшей эксплуатации (универсальные возможности поиска сетевых объектов и правил в базе правил и отслеживание прошлых изменений в базе данных).

После установки шлюз безопасности применяет все политики в пакете сформированным администратором, то есть набор политик разных типов. Пакет политик может иметь один или несколько из следующих типов политик:

1. Контроль доступа, состоящий из следующих типов правил: Брандмауэр, NAT, фильтрация приложений и URL, осведомленность о содержании,

2. Правила качества обслуживания для управления полосой пропускания (QoS)

3. Политика брандмауэра для конечных компьютеров, на которых клиент удаленного доступа Endpoint Security VPN установлен как автономный клиент (Desktop Security).

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 51 |

4. Предотвращение угроз, состоящее из: IPS, Anti-Bot, антивирус, эмуляция угроз, извлечение угроз.

5. Правила для проверки трафика, зашифрованного протоколом TLS, между внутренними клиентами браузера и веб-серверами (HTTPS-Inspection).

Администратору необходимо сформировать пакеты политик в зависимости от внутреннего регламента обработки защищаемой информации в Системе.

Перечень передаваемой информации из АСУ (уровень САУ) на сервера уровня ОПС, размещённые за МЭ в изолированном сегменте (демилитаризованной зоне, являющейся реализации меры ЗИС.5) ИТ-инфраструктуры АСУ, регламентируется эксплуатационной документацией. Для «санкционированного» пропуска этой информации на сервера, а в последствии и на АРМы необходимо настроить режим межсетевого экранирования кластера, применяя пакет политик: Брандмауэр, где осуществляется контроль доступа во внутреннюю сеть и из нее, фильтрации приложений и иные, состоящие в том, что со стороны внутреннего информационно-промышленного контура должны быть открыты только требуемые для пропуска данных АСУ ТП порты и сервисы, а все остальные должны быть заблокированы и разрешены только определённые протоколы обмена. Со стороны внешнего информационно-промышленного контура должны быть запрещены (протоколы, порты и сервисы): удаленный доступ к устройствам АСУ ТП для технического сопровождения системного и прикладного ПО, доступ к ресурсам АСУ ТП из информационно-вычислительных сетей общего пользования (сети Интернет), прямой доступ в технологическую сеть.

Межсетевой экран (кластер) по умолчанию должен работать в режиме блокировки проходящего через него трафика, а его настройка осуществляется путем определения списков правил фильтрации и трансляции трафика согласно топологии сети и требованиям безопасности на объекте.

Таким образом, прохождение любого IP-пакета запрещено, если это явно не разрешено соответствующими политиками безопасности.

Детальное описание процесса настройки МЭ изложено в Руководстве администратора по межсетевому экранированию программного обеспечения CheckPoint 3100.

АРМ администратора ИБ, на которое устанавливают Смарт консоль (SmartConsole), должно входить в сегментированную существующим телекоммуникационным оборудованием (маршрутизаторами) для этих целей сеть (VLAN) и иметь характеристики не хуже приведённых в таблице 9.1.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 52 |

Таблица 9.1. - Характеристики АРМ администратора ИБ

| Элемент | Параметры |
|--|--|
| Процессор | Не ниже Intel Core i5 |
| Оперативная память | 16 ГБ |
| Жесткий диск (свободное пространство) | Не менее 500 ГБ. Только NTFS, установка на FAT не поддерживается |
| Устройство ввода ключевой информации | Не менее 2-х USB 2.0, 3 USB-флэш-накопителя |
| Интерфейсы (свободные) | 2 x USB 2.0 — при использовании USB-флэш-накопителя |
| Сетевой адаптер | Не менее 2-х Ethernet-интерфейса |
| Операционная система | Windows 10 x86/x64 (кроме всех выпусков Starter и Home Edition) |
| Установленное ПО | Для хранения журналов используется СУБД MS SQL Server Express 2017 x32/x64 |

9.2. Подсистема управления учётными записями

Подсистема управления учётными записями является первым рубежом ПОИБ (СЗИ) объекта и предназначена для идентификации, аутентификации, авторизация, разграничение доступа пользователей и устройств в проектируемой АСУ и является инструментом для нейтрализации угроз несанкционированного доступа к информационным ресурсам. Она включает в себя реализацию следующих мер по обеспечению безопасности информации в основном на базе встроенных средств в ОС и ПО и применения дополнительных специализированных инструментов, входящих в состав СрЗИ проектируемых АСУ: ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.14 и включает в себя:

1. Идентификация и проверка подлинности субъектов доступа при входе в ОС по идентификатору и паролю.
2. Разграничение прав доступа и контроль доступа субъектов к защищаемым ИР на уровне ОС.
3. Настройка встроенных механизмов аутентификации на компонентах АСУ.
4. Ограничение неудачных попыток аутентификации.
5. Блокировка сеанса по истечению времени, а также вручную администратором ИБ и (или) пользователем.
6. Идентификация серверов и АРМ по логическим именам.
7. Идентификация (фильтрация) по MAC-адресам на интерфейсах (портах) активного сетевого оборудования.

| | | | | | | | | |
|--------------|--------------|--------------|---|-------|------|--|--|--|
| Инв. № подл. | Подп. и дата | Взам. инв. № | <div>П37.2021.01-ИБ.П2</div> <div>Лист 53</div> | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | | | |

8. Разграничение прав доступа к сменным носителям информации на основе серийных номеров (при наличии технической возможности).

9. Контроль управления учетными записями Отделом безопасности Компании.

Подсистема реализуется за счет применения следующих механизмов безопасности:

- 1) механизмы безопасности системного программного обеспечения (СПО) на базе ОС СВТ;
- 2) механизмы безопасности СрЗИ KICS for Nodes «Лаборатории Касперского» и ПО CheckPoint 3100;
- 3) механизмы безопасности прикладного программного обеспечения (ППО);
- 4) механизмы безопасности сетевых соединений.

Механизмы защиты СПО выбраны в качестве основных мер по реализации информационной безопасности, поскольку выполняют комплекс мероприятий по обеспечению функционирования подсистем: управления доступом, регистрации и учета, обеспечения целостности, и позволяют в полной мере реализовать комплекс требований, предъявляемых к реализации данной подсистемы.

В качестве механизмов защиты СПО рассматриваются встроенные механизмы безопасности операционных систем СВТ. Их назначение – обеспечение замкнутой защищенной программной среды операционной системы.

Функциональные возможности механизмов безопасности:

- 1) назначение прав пользователей;
- 2) определение политики паролей;
- 3) контроль учетных записей;
- 4) противодействие переполнению буфера;
- 5) защита от вредоносного ПО;
- 6) случайное расположение адресного пространства;
- 7) ведение политик аудита.

Настройка механизмов СПО предполагается на всех СВТ Объекта.

Механизмы безопасности СрЗИ KICS for Nodes от «Лаборатории Касперского» также выбраны в качестве основных мер по реализации информационной безопасности и дополняют механизмы защиты СПО. При локальной аутентификации они используются для защиты входа в систему и являются одной из нескольких подсистем средства локального управления базовой защиты программного пакета «Клиент» и совместно с ОС Windows обеспечивают:

- 1) проверку возможности входа пользователя в систему;

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 54 |

- 2) оповещение пользователя о реализованных в системе мерах защиты информации и о последнем входе в систему;
- 3) оповещение остальных модулей о начале или завершении работы пользователя;
- 4) блокировку работы пользователя;
- 5) загрузку данных с персональных идентификаторов пользователя;
- 6) усиленную аутентификацию пользователя при входе в систему.

При обработке входа пользователя в систему осуществляется определение его привилегий, уровня допуска и другие параметры.

Идентификация и аутентификация любого пользователя выполняются при каждом его входе в систему. Для ОС Windows штатная процедура входа предусматривает ввод логического имени (логина) и пароля пользователя или использование аппаратных средств, поддерживаемых операционной системой. При их совпадении с хранящимися в соответствующей базе данных происходит авторизация пользователя с соответствующей его ролью (статусом).

Кроме того, с помощью функционала ПО CheckPoint 3100 «управления учетными записями пользователей» назначаются роли и соответствующие этим ролям права (только для чтения, запись и т.п.). Необходимо в ПО CheckPoint 3100 установить роли и права для каждого пользователя АРМ и сервера функционирующих в Системе, например «monitorRole», которая предоставляет пользователю доступ только для чтения ко всем функциям или назначить иные роли с необходимыми правами.

Механизмы защиты ППО предполагаются на СВТ АСУ и выбраны в качестве дополнительных мер по реализации информационной безопасности и выполняют комплекс мероприятий по обеспечению функционирования подсистем: управления доступом, регистрации и учета.

В ППО применяются следующие механизмы безопасности:

- ролевое разграничение доступа к функциям системы;
- протоколирование действий пользователей.

В состав KICS for Nodes, дополняя механизмы защиты ППО входит также механизм дискреционного управления доступом к ресурсам файловой системы, обеспечивая:

- 1) разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа;
- 2) контроль доступа к объектам при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;

| | | | | | | | | | |
|--------------|--------------|--------------|-------------------|-------|------|--|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | П37.2021.01-ИБ.П2 | | | | | | |
| | | | 55 | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | | | | |

- 3) невозможность доступа к объектам в обход установленных прав доступа (если используются стандартные средства ОС или прикладные программы без собственных драйверов для работы с файловой системой);
- 4) независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows.

Таким образом, установленные права доступа к файловым объектам в KICS for Nodes не влияют на аналогичные права доступа в ОС Windows и наоборот.

Матрица доступа аналогично реализации в ОС Windows и представляет собой списки файловых объектов, в которых определены учетные записи с правами доступа. Права устанавливают разрешения или запреты на выполнение операций, которые для файлового объекта могут быть заданы явно или наследоваться от вышестоящего элемента иерархии.

Явно заданные права имеют более высокий приоритет по сравнению с наследуемыми правами. Права доступа считаются заданными явно, если для объекта отключен режим наследования прав.

Для управления списками доступа к любым файловым объектам предусматривается специальная привилегия – «дискреционное управление доступом». Обладающие этой привилегией пользователи (Администратор ИБ, системный администратор), могут изменять права доступа независимо от установленных прав доступа к объектам, для всех каталогов и файлов на локальных дисках.

У администраторов объекта достаточно большой инструментарий по настройке подсистемы управления учетными записями, в том числе и по ролям пользователей и по месту функционированию, а также регистрации всех событий и мониторингу, подробно изложенный в эксплуатационной документации производителя (руководство администратора) – Компании «Лаборатория Касперского» на KICS for Nodes.

9.3. Подсистема регистрации событий безопасности

Подсистема регистрации событий безопасности предназначена для осуществления контроля всех элементов проектируемой АСУ и целостности их ПО, а также сбора и регистрация событий безопасности и по существу является средством мониторинга и аудита ПОИБ проектируемого объекта для администратора ИБ.

Она включает в себя применение специализированных инструментов, входящих в состав ПТК ПОИБ проектируемой АСУ совместно со встроенными в операционную систему Windows компонентами регистрации событий безопасности, реализующих меры по обеспечению безопасности информации: АУД.3, АУД.4, АУД.6, АУД.7, АУД.8 и имеющих следующую функциональность:

| | | | | | | | | | |
|---------------|--------------|--------------|------|-------|------|-------------------|------------|--|--|
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | Лист 56 | | |
| Интв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | |
| | | | | | | | | | |

| |
|--|
| Подсистема регистрации событий безопасности предназначена для осуществления контроля всех элементов проектируемой АСУ и целостности их ПО, а также сбора и регистрация событий безопасности и по существу является средством мониторинга и аудита ПОИБ проектируемого объекта для администратора ИБ. |
| Она включает в себя применение специализированных инструментов, входящих в состав ПТК ПОИБ проектируемой АСУ совместно со встроенными в операционную систему Windows компонентами регистрации событий безопасности, реализующих меры по обеспечению безопасности информации: АУД.3, АУД.4, АУД.6, АУД.7, АУД.8 и имеющих следующую функциональность: |

1. Контроль состава и целостности ПО.
2. Регистрация событий безопасности.
3. Централизованный сбор, хранение и архивирование журналов.
4. Контроль устройств, подключаемых к АРМ и Серверам.
5. Контроль состояния устройств с возможностями блокирования АРМ (Сервера) при изменении состояния заданных устройств.
6. Оповещение ответственных лиц (администратора ИБ) о событиях безопасности.

Подсистема служит для мониторинга и регистрации событий безопасности, а также сбора статистических данных с разным уровнем детализации, оповещении о событиях безопасности ответственных и реализуется за счет применения следующих механизмов безопасности:

- 1) механизмы аудита СПО;
- 2) механизмы аудита СрЗИ KICS for Nodes;
- 3) механизмы аудита ППО.

В качестве механизмов аудита СПО рассматриваются встроенные механизмы безопасности операционных систем СВТ. Функциональные возможности механизмов безопасности:

- 1) ведение политик аудита;
- 2) ведение журналов: безопасности, приложений, установок, системы.

Настройка механизмов аудита предполагается на всех СВТ Объекта.

Механизмы аудита СрЗИ KICS for Nodes от «Лаборатории Касперского» дополняют механизмы аудита СПО и предоставляют администратору ИБ более универсальные терминалы для мониторинга ПОИБ проектируемой АСУ, а также возможность оптимального реагирования на события безопасности. В процессе функционирования программных СрЗИ события, происходящие на СВТ и связанные с безопасностью систем, регистрируются в соответствующих журналах. Все записи журналов хранятся в соответствующих файлах на системных дисках. Формат этих данных идентичен формату журнала безопасности ОС Windows.

Администратору ИБ предоставляются возможности для оптимизации работы настройка перечня регистрируемых событий безопасности, а также параметров хранения журнала, при которой можно изменить ограничение максимального объема журналов и политику перезаписи хранящейся информации. Эти возможности позволяют обеспечить оптимально необходимый объем сохраняемых сведений с учетом размера журналов и нагрузки на систему.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 57 |

В качестве механизмов аудита в ППО также рассматриваются встроенные механизмы безопасности ПО проектируемой АСУ. Функциональные возможности их заключаются в:

- 1) регистрации действий пользователей в системе по отношению к представлению информации (мнемосхем, графиков, отображений и т.д.);
- 2) регистрации системных изменений;
- 3) регистрации изменений атрибутов доступа.

Настройка механизмов ППО предполагается на всех СВТ АСУ.

Первоисточником для регистрации событий безопасности является встроенная подсистема обеспечения целостности, предназначенная для контроля состояния неизменности программной среды СВТ, а также для восстановления работоспособности СВТ и информации после сбоев. Она функционирует за счет применения средств обеспечения целостности и механизма контроля программ из состава средства антивирусной защиты.

Средства обеспечения целостности применяются для проверки контрольных сумм компонентов СЗИ и элементов СПО и ППО во время загрузки ОС. Основной их функционал состоит в обеспечении целостности программной среды, а также фиксации и динамического контроля неизменности состояния файлов, каталогов СВТ путем считывания контрольных сумм, в настройке политик безопасности СПО в автоматизированном режиме.

Контроль программ из состава средства антивирусной защиты применяется для регулирования доступа к файловой системе СВТ активного ПО, регулирования взаимодействий между ПО и регулированию доступа к ресурсам СВТ.

Непосредственная настройка СЗИ подробно изложена в эксплуатационных документах производителя (Руководство администратора).

9.4. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для защиты АРМ и серверов от деструктивных действий вредоносного программного обеспечения и служит ещё одним «рубежом» эшелонированной СЗИ (ПОИБ).

Антивирусная защита реализуется одним из механизмов защиты в составе комплексного решения KICS Компании «Лаборатория Касперского» - KICS for Nodes при наличии действующей (приобретенной) лицензий и позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. В ходе антивирусных проверок СВТ

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|----|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | 58 |

осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и иных элементов, настраиваемых администратором ИБ, что позволяет обнаружить и заблокировать внешние и внутренние сетевые атаки, направленные на защищаемый объект.

Применение компонентов сетевой антивирусной защиты, входящей в состав KICS for Nodes проектируемой АСУ реализует следующие меры по обеспечению безопасности информации: АВЗ.1, АВЗ.2, АВЗ.4, ЗИС.3, ЗИС.34 и заключается в следующем:

- 1) реализация антивирусной защиты (АВЗ.1),
- 2) антивирусная защита иных сервисов (АВЗ.2),
- 3) обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.4),
- 4) эшелонированная защита информационной (автоматизированной) системы (ЗИС.3);
- 5) защита от угроз отказа в обслуживании (DOS, DDOS-атак) (ЗИС.34).

В KICS for Nodes проверка и защита конечных устройств осуществляется с помощью следующих основных компонентов:

- 1) файловый антивирус, постоянно находящийся в оперативной памяти рабочей станции и проверяющий все открываемые, сохраняемые и запускаемые файлы;
- 2) управление брандмауэром Windows, позволяющее настраивать сетевой экран Windows и управлять политиками, блокировать любые возможности настройки брандмауэра извне;
- 3) защита от шифрования, позволяющее обнаруживать и блокировать активность, связанную с вредоносным шифрованием сетевых файловых ресурсов на защищаемой рабочей станции со стороны сети;
- 4) отслеживание попыток подключения защищаемого компьютера к сетям Wi-Fi и блокирование или разрешение подключения;
- 5) мониторинг файловых операций, имеющий особую значимость в АСУ ТП, так как любое изменение в файлах может говорить о нарушении режима безопасности;
- 6) анализ журналов, отвечающий за контроль целостности защищаемой среды, изучая журналы событий Windows.

Помимо основных компонентов, обеспечивающих защиту промышленных рабочих станций от информационных угроз, KICS for Nodes содержит ряд служебных функций, предусмотренных для того, чтобы поддерживать защиту в актуальном

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 59 |

состоянии, расширять возможности использования продукта, оказывать помощь в работе, в том числе и при мониторинге:

1) отчеты, предоставляющие статистику, касающуюся защищаемых устройств, а также выборки событий, содержащие списки событий и всех выполненных программой операций;

2) управление карантинном (содержит потенциально опасные файлы или вирусы), резервным хранилищем (в него помещаются копии вылеченных и удаленных файлов);

3) защита от эксплойтов, состоящее в защите памяти процессов от эксплуатации уязвимостей Windows с помощью, внедряемого в них Агента защиты;

4) блокировка удаленных рабочих станций, которые пытаются получить доступ к общим сетевым ресурсам, при обнаружении вредоносной активности с их стороны;

5) доверенная зона, представляющая собой список исключений из области защиты или проверки, подготовленный администратором KICS for Nodes (администратором ИБ);

6) поддержка, включающая доступ к обновлению баз и модулей KICS for Nodes,

Программа KICS for Nodes структурно включает в себя следующие модули:

1) функциональный модуль, фиксирующий информацию о состоянии узлов промышленной сети и выполняющий защиту узлов от информационных угроз;

2) консоль, являющейся локальным графическим интерфейсом пользователя, с помощью которого работа KICS for Nodes может управляться на узлах промышленной сети как непосредственно одним компьютером, на котором она установлена, так и несколькими компьютерами с KICS for Nodes.

KICS for Nodes взаимодействует с KSC – утилитой (бесплатной), которая используется как единая точка мониторинга и управления всеми решениями KICS, поэтому управление задачами и функциональными возможностями, настраивание параметров работы KICS for Nodes может осуществляться как из сервера администрирования KSC, так и из Консоли KICS for Nodes.

Консоль KICS for Nodes может устанавливаться на компьютере с установленным функциональным модулем KICS for Nodes или на любом другом компьютере защищаемой сети и в этом случае управление KICS for Nodes с помощью Консоли выполняется удаленно. Возможно управлять несколькими компьютерами, которые защищены KICS for Nodes, с помощью одной Консоли.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 60 |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | |

KICS for Nodes устанавливается на конечных узлах производственной сети, осуществляет защиту и контроль состояния безопасности промышленных компьютеров, а также контролирует целостность прошивок на ПЛК, включенных в область проверки. В случае возникновения инцидента информационной безопасности на защищаемом устройстве его статус защищенности изменяется. Статус защищенности устройства отображается в KSC. Инциденты безопасности передаются в Консоль KICS for Nodes и сервер администрирования KSC для обработки администратором ИБ на объекте.

Программный модуль KSC, устанавливаемый непосредственно на АРМ администратора ИБ, предназначен для осуществляется управления всеми решениями KICS из единой консоли, что позволяет добиться оптимального контроля в части доступа к детальной информации об уровне безопасности защищаемой сети, а также простоты администрирования и прозрачности всех компонентов защиты включает в себя следующие основные компоненты:

1) сервер администрирования KSC (далее – Сервер KSC), осуществляющий функции централизованного хранения информации об установленных в защищаемой сети программах и управления ими;

2) консоль администрирования (далее – Консоль KSC), представляющая собой основной инструмент администратора ИБ с пользовательским интерфейсом к административным службам Сервера KSC и Агента KSC, выполненная в виде компонента расширения к Microsoft Management Console (MMC), поставляемая вместе с Сервером KSC, но может также устанавливаться отдельно на одно или несколько устройств администратора;

3) web console (далее – Веб-консоль KSC), представляющая собой веб-интерфейс («тонкий клиент») для создания и управления системой защиты сети Компании, находящейся под управлением KSC с иного АРМ сети.

4) KSN–серверы, представляющие собой серверы с оперативной базой знаний «Лаборатории Касперского» о репутации файлов, веб-ресурсов и программного обеспечения служащие для обновления всех программных решений KICS до актуального состояния;

5) агент администрирования (далее – Агент KSC), представляющие собой плагин, устанавливаемый на защищаемые оконечные (клиентские) устройства, где установлена одна из программных компонент KICS и служит для управления (администрирования) ею, а также для получения информации о защищаемом устройстве и передаче этой информации на Сервер KSC.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 61 |

Основным вариантом администрирования решения KICS является через консоль KSC программного модуля KSC, установленного на АРМ администратора ИБ. Использование же в этом программном модуле Веб-консоли KSC позволяет запускать установку решений KICS и иных программ «Лаборатории Касперского» через браузер с иных АРМ в сети по усмотрению администратора ИБ и является дополнительным инструментарием.

KICS for Nodes пользователей обменивается информацией с KSC, устанавливаемой на АРМ администратора ИБ, и тем самым управляется из единой точки мониторинга и управления всеми решениями KICS. Управление задачами и функциональными возможностями, настраивание параметров работы KICS for Nodes может осуществляться как из сервера администрирования KSC, так и из Консоли KICS for Nodes.

Детальный порядок настройки и эксплуатации KICS for Nodes на АРМ и сервера изложен в руководстве администратора, поставляемом компанией-производителем «Лаборатория Касперского» на этот программный продукт, а за незаконное копирование и распространение в ней информации и его отдельных частей предусматривается ответственность в соответствии с законодательством Российской Федерации об авторском праве. В этой связи в данном документе приводятся только общие, основные этапы настройки KICS for Nodes.

Установка KICS for Nodes должна быть произведена на СБТ, не содержащее иного антивирусного программного обеспечения, поэтому необходимо удалить с устройства, если таковые имелись, другие антивирусные программы.

В соответствии с руководством администратора на защищаемый объект необходимо установить программные компоненты KICS for Nodes (есть возможность их выборочной установки) и программные компоненты набора Средства администрирования (справка, документация, управления через Консоль). Первоначальную установку рекомендуется производить с помощью мастера установки, а в последующем с помощью Kaspersky Security Center (KSC) по инструкции производителя и по заранее составленному плану основных этапов установки (включающего средства администрирования, устанавливаемые программные компоненты, способ установки).

Основным средством администрирования KICS for Nodes будет являться консоль администрирования KSC, а дополнительным - консоль самой KICS for Nodes. Поэтому при установке ПО обязательно необходимо установить:

- 1) модуль интеграции с агентом администрирования KSC на защищаемое СБТ;

| | | | | | | | | | |
|--------------|--------------|--------------|-------------------|--------|------|------|-------|------|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | П37.2021.01-ИБ.П2 | | | | | | |
| | | | Изм. | Кол.уч | Лист | №Док | Подп. | Дата | |

- 2) агент администрирования KSC на защищаемое СБТ;
- 3) плагин управления KICS for Nodes на АРМ администратора ИБ.

Установка KICS for Nodes с помощью мастера установки детально изложена в Руководстве администратора. По её окончании сразу запускаются задачи защиты и проверки, если активирована программа, с помощью файла ключа приобретаемой коммерческой лицензии (был установлен флажок «Включить постоянную защиту после установки программы (по умолчанию)»), объектов файловой системы защищаемого устройства при доступе к ним и, например, каждую пятницу в 20:00 задача «Проверка важных областей». В последствии это возможно изменить средствами администрирования по усмотрению администратора ИБ.

После установки KICS for Nodes необходимо запустить механизм по обновлению баз программы через отторгаемые носители информации, для чего настроить с последующим запуском задачу «Обновление баз программы».

На порядок и периодичность обновления антивирусных баз накладывается требование Политики ИБ Компании об исключении непосредственного подключения к всемирной сети «Интернет» защищаемой сети и её элементов. Для выполнения этого требования в помещении объекта для администратора ИБ дополнительно устанавливается отдельное СБТ (ноутбук, АРМ), имеющее доступ (подключение) к всемирной сети «Интернет» и не имеющее непосредственного подключения к защищаемой сети и отдельным её элементам. На этом СБТ устанавливается KICS for Nodes или Сервер администрирования KSC с действующей лицензией, и оно используется в качестве посредника, копируя к себе все срочные и иные обновления баз установки, а затем скопировав «вручную» на отторгаемый (съёмный) носитель информации эти обновления необходимо распределить на защищаемые конечные устройства в сети через АРМ администратора ИБ, на котором установлены компоненты KSC. Для этого необходимо использовать задачу «Копирование обновлений».

Для настройки получение обновлений KICS for Nodes через Сервер администрирования KSC необходимо:

- 1) загрузить обновления с серверов обновлений «Лаборатории Касперского» на Сервер администрирования KSC установленный на отдельном СБТ имеющее доступ (подключение) к всемирной сети «Интернет», настроив задачу «Получение обновлений Сервером администрирования» для указанного набора защищаемых устройств, а в качестве источника обновлений указав серверы обновлений «Лаборатории Касперского»;
- 2) распределить обновления на защищаемые устройства, перенеся их с помощью съёмного носителя информации в аналогичную папку на АРМ

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|----|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | 63 |

администратора ИБ, а в KSC установленной на нем настроить групповую задачу обновления антивирусных баз (модулей программы) для распределения обновлений на защищаемые устройства, в расписании задачи указав частоту запуска после получения обновлений Сервером администрирования, так как Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым);

3) настроить на каждом из защищаемых устройств задачи «Обновление баз программы» и «Обновление модулей программы», где в качестве источника обновлений указать Сервер администрирования KSC, а также настроить расписание задачи.

В процессе функционирования имеется возможность добавлять или удалять некоторые компоненты KICS for Nodes, а также после установки и обновления баз осуществить проверку функций постоянной защиты файлов с помощью тестового вируса EICAR в соответствии с Руководством. Этот вирус, разработанный The European Institute for Computer Antivirus Research (EICAR), предназначен для проверки работы антивирусных программ и не является вредоносным объектом, так как не содержит исполняемого кода, который может нанести вред защищаемому устройству, но антивирусное ПО большинства производителей идентифицируют его как угрозу.

Централизованное управление защищаемыми устройствами с помощью KSC позволяет отдельно настраивать параметры работы для каждого такого устройства, входящего в группу администрирования - несколько устройств с KICS for Nodes, для которых настраиваются единые параметры управления и защиты, следующими способами:

1) с помощью политик KSC удаленно настраиваются единые параметры защиты для группы устройств, такие как: общие параметры работы программы, параметры задач постоянной защиты, контроля активности на СБТ, параметры запуска системных задач по расписанию,

2) с помощью групповых задач KSC настраиваются единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств (активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления, параметры задачи формирования правил контроля запуска программ),

3) с помощью задач для набора устройств удаленно настраиваются единые параметры задач, имеющих ограниченный срок выполнения для устройств, не входящих ни в одну группу администрирования,

4) с помощью окна настройки параметров отдельного сервера настраиваются как общие параметры работы программы, так и параметры работы всех

| | | | | | | | | | |
|--------------|--------------|--------------|-------------------|-------|------|--|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | П37.2021.01-ИБ.П2 | | | | | | |
| | | | 64 | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | | | | |

задач KICS for Nodes на отдельно выбранном защищаемом устройстве не находящимся под управлением активной политики KSC.

С помощью KSC как для группы защищаемых устройств, так и для отдельного защищаемого устройства настраиваются параметры программы, дополнительные возможности и работа журналов и уведомлений.

Для настройки общих параметров KICS for Nodes из политики KSC необходимо развернув узел «Управляемые устройства» в дереве Консоли администрирования KSC и выбрав, требуемую для настройки задачи группу администрирования, зайти на вкладку «Политики» и открыть окно свойств политики для настройки по соответствующему имени политики. В открывшемся окне необходимо перейдите в раздел «Параметры программы» и нажать «Настройка» для группы параметров, которую выбраны для настройки. Пользуясь Руководством администратора и статистической информацией о режимах работы оборудования необходимо внести с последующим сохранением в соответствующие поля информацию по настройке.

В соответствии с Руководством администратора, аналогичным образом через KSC необходимо настроить и сохранить иные параметры (безопасности, соединения, запуска по расписанию, карантин и резервного хранилища) ПО, а также возможно заблокировать удаленные устройства и настроить параметры хранилища заблокированных узлов, журналов и уведомлений и множество дополнительных возможностей (доверенная зона, проверка съемных дисков, права пользователей на управление программой, контроль запуска программ, контроль устройств, контроль Wi-Fi, управление сетевым экраном, защита от шифрования и другие).

Выполнение предусмотренного функционала ПО обеспечивается с помощью создания, настройки параметров выполнения, расписания запуска и остановки в KSC задач следующих типов:

- 1) активация программы,
- 2) копирование обновлений,
- 3) обновление баз программы,
- 4) обновление модулей программы,
- 5) откат обновления баз программы,
- 6) проверка по требованию,
- 7) проверка целостности программы,
- 8) мониторинг целостности файлов на основе эталона,
- 9) формирование правил контроля запуска программ,
- 10) формирование правил контроля устройств.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 65 |

Механизм их создания и реализации детально изложен в Руководстве администратора, как для локальных, так и групповых объектов.

Кроме того, в KSC формируются отчёты о состоянии управляемых устройств на основании информации, хранящейся на Сервере администрирования следующих типов:

- 1) о статусе компонентов или состояния защиты всех устройств в сети (работает, приостановлен, остановлен, неисправен, не установлен, запускается);
- 2) о запрещенных запусках (заблокированных) запрещенных программах (если задача запущена в активном режиме);
- 3) о тестовых запрещенных запусках (заблокированных) запрещенных программах в тестовом режиме (если задача запущена в режиме только статистика).

Аналогичные действия по настройке мониторинга и управления ПО можно осуществлять в Консоли KICS for Nodes, используемой как дополнительный инструментарий в решении KICS и детально изложенный в Руководстве администратора.

У администратора ИБ достаточно большой инструментарий по настройке антивирусной защиты, в том числе и по её уровню, а также регистрации всех событий и мониторингу, подробно изложенный в эксплуатационной документации (руководстве администратора) производителя – Компании «Лаборатория Касперского» комплексного решения KICS.

В проектируемой СЗИ объекта KICS for Nodes устанавливается на следующие конечные устройства (для АРМ используется операционная система Win10 lot Ent 2016, а для серверных станций - Win Server 2016 Std 64-bit):

- 1) 8-м АРМ оперативно-диспетчерского и управляющего персонала: директора, главного инженера, начальника ОЭЦ, специалиста СРЗиА, специалиста МГА ГЩУ, специалиста ДЭМ ГЩУ, 2-а АРМ специалиста НСС ГЩУ;
- 2) 1 АРМ администратора ИБ;
- 3) серверы PC1 и PC2;
- 4) серверы архива 1 и 2.

Итого устанавливается 4 комплекта (лицензий) KICS for Nodes для серверной операционной системы и 9 комплектов (лицензий) KICS for Nodes для рабочих станций. По настоянию Заказчика не учитывается 5-6% резерв лицензий от установленных (серверных и рабочих станций). Непосредственно на ПЛК программный модуль KICS for Nodes не устанавливаются. Защищаются все объекты вокруг ПЛК, а для мониторинга целостности (изменения) проектов ПЛК на сервере (АРМ) непосредственно управляющим выбранным ПЛК задействуется опция «Мониторинг

| | | | | | | | | | |
|--------------|--------------|--------------|-------------------|-------|------|--|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | П37.2021.01-ИБ.П2 | | | | | | |
| | | | 66 | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | | | | |

файловых операций» из функционала «Контроль информационного окружения», устанавливаемого на него KICS for Nodes.

KSC со своими компонентами Сервер, Консоль, Веб-консоль устанавливается на АРМ администратора ИБ.

9.5. Подсистема централизованного управления средствами защиты и контроля защищенности

Подсистема централизованного управления средствами защиты и контроля защищенности предназначена для централизованного управления компонентами ПОИБ, контроля и анализа защищенности проектируемой АСУ. Она реализуется за счет применения компонентов централизованного управления и мониторинга, входящих в состав ПТК ПОИБ проектируемой АСУ, реализует меры по обеспечению безопасности информации: ОЦЛ.1, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6 и выполняет следующие основные функции:

1. Контроль портов ввода/вывода.
2. Контроль подключения машинных носителей.
3. Формирование паспорта ПО (инвентаризация систем).
4. Контроль целостности файлов и папок на АРМ и серверах.
5. Блокировка АРМ по событиям безопасности.
6. Централизованное управление межсетевыми экранами.
7. Реагирование на события безопасности путем воздействия на средства защиты информации для блокирования угроз.
8. Контроль целостности программных компонентов СрЗИ.
9. Применение программного сканера уязвимостей для мониторинга систем.

Практическая реализация подсистемы централизованного управления средствами защиты и контроля защищенности заключается в обеспечении администратора ИБ максимально полной информацией для принятия решений о состоянии всех элементов защищаемого объекта и СрЗИ, оптимальными механизмами реагирования на события безопасности и набором удобного для этого инструментария, устанавливаемого на АРМ администратора ИБ.

Таким инструментарием является KSC из KICS и Смарт консоль (SmartConsole) ПО CheckPoint 3100. Эти программные компоненты СрЗИ устанавливаются на АРМ администратора ИБ.

Контроль состояния защищенности и работоспособности также осуществляется с помощью функционала KSC из KICS и SmartConsole ПО CheckPoint 3100.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 67 |

Аудит осуществляется посредством анализа произошедших событий, зарегистрированных в соответствующих журналах, в том числе и СрЗИ. Он проводится администратором ИБ объекта и решает следующие задачи:

- 1) регулярный просмотр содержимого журналов регистрации;
- 2) оптимальная настройка параметров хранения журналов;
- 3) управление содержимым журналов (записями о событиях).

Так как возможность просмотра содержимого журналов определяется правами учетных записей пользователей на доступ к базе данных, в которой хранятся журналы, поэтому администратору ИБ должна быть назначена одна из следующих ролей:

- 1) главный администратор;
- 2) аудитор;
- 3) администратор сети;
- 4) администратор ключей.

Централизованное управления защищаемыми СБТ и контроль за их защищенностью осуществляется отдельно устанавливаемой компонентой KCS KICS от «Лаборатории Касперского» на АРМ администратора ИБ, которая совместно с SmartConsole ПО CheckPoint 3100 комплексно реализует подсистему централизованного управления средствами защиты и контроля защищенности проектируемого объекта.

KCS KICS от «Лаборатории Касперского» предоставляет основные возможности:

- 1) настройка параметров защиты и управления СБТ;
- 2) мониторинг состояния системы;
- 3) конфигурирование сетевой структуры системы;
- 4) работа с централизованными журналами.

Для анализа содержимого журналов предусмотрены режимы отображения:

- 1) события, являющийся основным режимом для просмотра и управления записями, где выводится список загруженных записей журналов в табличной форме;
- 2) угрозы, являющийся сжатым или разъясняющие сведения о зарегистрированных событиях режимом, где выводится список угроз, полученных в результате анализа загруженных записей и предназначен для представления администратору ИБ наиболее важной информации из журналов.

Кроме того, имеется возможность просмотра и анализа записей журнала безопасности CheckPoint 3100 и его лог-сервера.

У администратора ИБ достаточно большой инструментарий по централизованному управлению и контролю защищенности сети объекта, подробно изложенный в эксплуатационной документации производителей.

| | | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|----|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | 68 |

10. Организационные решения

Организационные решения представляют собой неотъемлемую часть ПОИБ модернизируемого Объекта и предназначены для обеспечения регламентации процессов обработки информации в АСУ в соответствии с перечнем реализуемых мер, нейтрализующих угрозы безопасности информации и Политикой Компании по ИБ.

Организационные мероприятия в основном включают в себя следующий состав:

- 1) рекомендации по работе с персоналом и подразделениями (распределение ролей между службами, назначение ответственных);
- 2) рекомендации по режимным мероприятиям (планирование мероприятий, регламентация действий в нештатных ситуациях);
- 3) рекомендации по разработке организационно-распорядительной документации;
- 4) рекомендации по работе с внешними носителями информации.
- 5) рекомендации по физической защите элементов Систем и исключения к ним НСД.

Эти рекомендации условно можно отнести в подсистемы:

1. Подсистема управления информационной безопасностью.
2. Подсистема защиты технических средств.

10.1. Подсистема управления информационной безопасностью

Подсистема управления информационной безопасностью предназначена для организационного сопровождения процесса обеспечений ИБ, проектируемой АСУ, а также контроля выполнения требований по ИБ. Она реализует следующие меры по обеспечению безопасности информации: ИАФ.0, УПД.0, ЗНИ.0, АУД.0, АВЗ.0, ОЦЛ.0, ОДТ.0, ЗТС.0, ЗИС.0, ИНЦ.0, УКФ.0, ОПО.0, ПЛН.0, ДНС.0, ИПО.0, ЗИС.1, ЗИС.3 и включает в себя:

1. Формирование штатного расписания и должностных инструкций к нему в соответствии с требованиями ИБ, в которых назначаются ответственные работники за определённым функционалом, разделяются их полномочия, исключается возможность принятия единоличного решения, влияющего на информационную безопасность и иные функции.

2. Разработка организационно-распорядительной документации Компании в целом и на проектируемый объект, соответствующие требованиям Политики информационной безопасности Компании.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 69 |

3. Контроль службой корпоративной безопасности Компании и выполнение требований положений собственной Политики ИБ и организационно-распорядительных документов.
4. Обеспечение комплексного подхода и организация эшелонированной защиты АСУ.
5. Инвентаризация защищаемых ИР.
6. Организация и проведение аудитов информационной безопасности.
7. Анализ компьютерных инцидентов.
8. Контроль работоспособности защищаемых систем.
9. Планирование мероприятий ИБ.
10. Управление процессом изменения конфигурации защищаемых систем.
11. Управление обновлениями средств защиты информации (средства антивирусной защиты, межсетевые экраны), ПО серверов и АРМ.
12. Доведение информации по обеспечению ИБ до персонала, проведение инструктажей, обучений.
13. Учет и управление доступом к машинным носителям информации.
14. Уничтожение конфиденциальной информации на компонентах защищаемых систем при выведении из эксплуатации и (или) при передаче сторонним организациям.
15. Резервное копирование, периодичность создания резервных копий и восстановление ОС серверов и файлов средств защиты информации из резервных копий в случаях сбоя.

10.1.1. Штатное расписания и назначение ответственных

Для эффективной организации системы защиты информации необходимо наличие компетентных работников, проверенных по установленным правилам Компании на предмет благонадежности. Проверка соответствующей службой безопасности таких работников существенно снизит проникновение на объект нарушителей информационной безопасности.

Состав обслуживающего персонала определяется руководством Компании в соответствии со штатным расписанием и с учетом требований и рекомендаций настоящей документации. Специалисты обслуживающего персонала СЗИ АСУ должны иметь знания и квалификацию, необходимую для работы с оборудованием и ПО, иметь специальное образование и иметь установленный Компанией допуск к работам.

Пунктом 1 указа Президента России от 01.05.2022 № 250, предписывается руководителям государственных корпораций (компаний) и иных организаций,

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист 70 |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | |

созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение и обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направляются на регулярной основе в органы (организации) с учетом меняющихся угроз в информационной сфере.

Вместе с тем, в нарушении этих положений Указа, согласно информационному письму Заказчика от 12.10.2022 № Вх-22-0559 (приложение 1), где в п. 2 отсутствуют возражения против введение на ИГЭС должности администратора ИБ, в штате ИГЭС не будет вводиться специально выделенный работник выполняющий функции администратора ИБ, а эти необходимые функции будут возложены на специалистов группы автоматизированных систем управления и состоят в следующем:

- 1) разработка предложений по совершенствованию организационно-распорядительных документов по безопасности объектов и представлять их руководителю субъекта КИИ (уполномоченному лицу);
- 2) проведение анализа угроз безопасности информации в отношении объектов КИИ и выявление уязвимости в них;
- 3) обеспечение реализации требований по обеспечению безопасности объектов КИИ, установленных в соответствии со ст. 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;
- 4) обеспечение в соответствии с требованиями по безопасности реализацию организационных мер и применение средств защиты информации, эксплуатации средств защиты информации;
- 5) осуществление реагирования на компьютерные инциденты в порядке, установленном п. 6 ч. 4 ст. 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;
- 6) организации проведения оценки соответствия объектов КИИ требованиям по безопасности;

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 71 |

7) подготовка предложений по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности объектов КИИ.

Для обеспечения адекватного профессионального уровня при эксплуатации комплексов СВТ, ПЛК, ЛВС, СТК и ИБ специалистам группы автоматизированных систем управления рекомендуются подобрать в регионе нахождения соответствующие учебные курсы в учебных заведениях повышения профессиональной подготовки.

Такие учебные заведения должны осуществлять обучение на русском языке по всем технологиям и функциональности, поддерживаемым выпускаемым в настоящее время сетевым оборудованием, методам их настройки на этом оборудовании, поиска и устранения неисправностей в работе устройств и иных нештатных ситуаций.

Возможны формы обучения специалистов - очная, заочная (дистанционная), индивидуальная. Уровень преподавания, методические материалы, оборудование и условия обучения должны соответствовать действующим требованиям Министерства науки и высшего образования Российской Федерации.

Обучение должно предполагать возможность проведения текущих (промежуточных) и итоговых квалификационных экзаменов на знание областей ИТ-технологий и способов настройки их на сетевом оборудовании и средствах защиты информации, а также осуществление подготовки к сдаче данных экзаменов и при успешном результате – выдача установленного в Российской Федерации документа о повышении квалификации.

10.1.2. Разработка организационно-распорядительной документации

Для надёжного функционирования модернизируемой Системы (АСУ) необходимо разработать и утвердить по установленным в Компании правилам пакет документ, регламентирующий непрерывность системы защиты информации в АСУ объекта; порядок резервного копирования информации; перечень технических средств, подлежащих дублированию (резервированию); регламентирующие доступ всех пользователей в Систему и другие документы для выполнения организационных мероприятий по ИБ.

В состав организационно-распорядительных документов, которые должны быть разработаны в течении жизненного цикла модернизируемой Системы, входят документы, приведенные в таблице 10.1.

Таблица 10.1 – Перечень организационно-распорядительной документации.

| | | | | | | | | | | | | | | | |
|--------------|--------------|--------------|--|--|--|--|--|--|---|--|--|--|-----------------------------|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | <p>пользователей в Систему и другие документы для выполнения организационных мероприятий по ИБ.</p> <p>В состав организационно-распорядительных документов, которые должны быть разработаны в течении жизненного цикла модернизируемой Системы, входят документы, приведенные в таблице 10.1.</p> <p>Таблица 10.1 – Перечень организационно-распорядительной документации.</p> | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | Наименование документа | | | | | | Требование к содержанию | | | | Ответственный за разработку | | |
| | | | Эксплуатационная документация на | | | | | | В соответствии с ГОСТ 34.201-2020, для защищаемой автоматизированной системы: | | | | Поставщик (Производитель) | | |
| | | | | | | | | | П37.2021.01-ИБ.П2 | | | | | | Лист |
| | | | | | | | | | | | | | | | 72 |
| | | | | | | | | | | | | | | | |
| | | | Изм. Кол.уч Лист №Док Подп. Дата | | | | | | | | | | | | |

| | | | | | | Наименование документа | Требование к содержанию | Ответственный за разработку | |
|--------------|--------------|--------------|------|-------|------|---|--|---|------|
| | | | | | | автоматизированную систему | <ul style="list-style-type: none">– инструкции (руководства) администратора;– инструкции (руководства) пользователей;– состав и назначение оборудования и программного обеспечения;– программа и методика испытаний;– формуляр. | автоматизированной системы | |
| | | | | | | Перечень защищаемых информационных ресурсов | <ul style="list-style-type: none">– исчерпывающий перечень информационных ресурсов модернизируемой Системы ИГЭС, подлежащих защите от угроз информационной безопасности– категория значимости информационного ресурса (Системы) или её отсутствие;– описание информации, которую содержит информационные ресурсы;– критичность нарушений свойств безопасности информации; | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании | |
| | | | | | | Правила работы с системным и прикладным ПО | <ul style="list-style-type: none">– правила и процедуры ограничения программной среды, включая требование инсталляция только разрешенного к использованию программного обеспечения и (или) его компонентов;– правила и процедуры обновления системного и прикладного программного обеспечения;– правила назначения ответственного за обновления программного обеспечения;– порядок и периодичность получения файлов обновления программного обеспечения;– порядок проведения тестирования файлов обновления перед их установкой;– правила и порядок документирования обновлений программного обеспечения; | Поставщик (Производитель) Системы под контролем Управления (службы) информационной безопасности головной Компании | |
| | | | | | | Руководство администратора безопасности | <ul style="list-style-type: none">– правила и процедуры управления доступом субъектов доступа к объектам доступа, идентификации и аутентификации субъектов и объектов доступа;– порядок определения и назначения лиц, которым разрешены действия по управлению доступом;– порядок выдачи средств аутентификации пользователям;– требования к характеристикам паролей;– правила и процедуры управление учётными записями пользователей (заведение, активация, блокирование и уничтожение);– правила разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование Системы;– правила назначения необходимых прав и привилегий администраторам и лицам, | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании | |
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | Лист |
| | | | | | | | | | 73 |

| | | | | | | Наименование документа | Требование к содержанию | Ответственный за разработку | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------|------|--------|------|------|-------|--|---|---|--|--|--|--|------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | защищаемой Системы; – установление перечня разрешенных действий неавторизованным (до прохождения процедуры авторизации) пользователям Системы; – обозначение границ контролируемой зоны на объекте; – правила разграничение физического доступа в контролируемую зону к компонентам защищаемой Системы; – правила и процедуры разграничения доступа (уровни пользователя, администратора) к компонентам и конфигурации защищаемых ресурсов; | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | Инструкция антивирусной защиты | – правила применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения; – правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов); – периодичность и порядок обновлений баз решающих правил (при необходимости); – порядок назначения ответственного за обновление баз решающих правил; | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | Инструкция по работе со съемными носителями информации | – порядок и периодичность резервного копирования информации на резервные машинные носители (план резервного копирования); – правила назначения ответственного лица за проведение резервного копирования; – правила и процедуры защиты машинных носителей; – перечень технические средств, подлежащих дублированию (резервированию); – учет машинных носителей информации, используемых в защищаемой Системе для хранения и обработки информации; – правила и процедуры доступа к машинным носителям информации; – правила и процедуры контроля использования интерфейсов ввода (вывода); – правила и процедуры контроля подключения машинных носителей информации; | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | Инструкции по действиям в нештатных ситуациях | – правила и процедуры обеспечения действий в нештатных (непредвиденных) ситуациях; | Поставщик (Производитель) Системы, | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Инв. № подл. | Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | | | | Лист | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | 74 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | |
|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № |
| | | |

| Наименование документа | Требование к содержанию | Ответственный за разработку |
|---------------------------------------|--|--|
| | <ul style="list-style-type: none">– план действий на случай возникновения нештатных (непредвиденных) ситуаций;– порядок и периодичность обучения персонала действиям в нештатных ситуациях;– правила и процедуры, периодичность проведения информирования об угрозах безопасности и обучения (в том числе практические занятия) персонала правилам эксплуатации защищаемых информационных ресурсов, а также лиц, временно допущенных на территорию контролируемой зоны;– порядок определения и назначения лиц, ответственных за проведение информирования и обучения;– правила и процедуры выявления инцидентов и реагирования на них;– порядок определения и назначения лиц, ответственных за выявление инцидентов и реагирование на них;– правила и порядок документирования инцидентов; | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании |
| Руководство обеспечения непрерывности | <p>1. Управление конфигурацией Системы:</p> <ul style="list-style-type: none">– порядок определения и назначения лиц, которым разрешены действия по внесению изменений в конфигурацию защищаемой Системы;– порядок внесения изменений в конфигурацию защищаемой Системы;– порядок и правила документирования изменений конфигурации;– периодичность и порядок проведения работ по техническому обслуживанию технических средств и программного обеспечения компонентов, защищаемых информационных ресурсов; <p>2. Аудит информационной безопасности:</p> <ul style="list-style-type: none">– правила и процедуры проведения анализа текущего уровня защищенности защищаемой Системы;– правила и процедуры проведения контроля текущих параметров и конфигурации компонентов защищаемой Системы;– правила и процедуры, периодичность проведения анализа угроз безопасности информации и рисков от их реализации;– порядок определения и назначения лиц, ответственных за проведение анализа и контроля; <p>3. Регистрация событий безопасности:</p> | Поставщик (Производитель) Системы, Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании |

| | | | | | |
|------|--------|------|------|-------|------|
| | | | | | |
| | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |

П37.2021.01-ИБ.П2

| |
|------|
| Лист |
| 75 |

П37.2021.01-ИБ.П2

| Наименование документа | | Требование к содержанию | | | | Ответственный за разработку | |
|--|--------------|--|------|-------|------|---|------|
| Журнал обучения и информирования персонала | | <ul style="list-style-type: none"> – дата проведения обучения; – причина проведения обучения (очередное обучение, обучение в связи с инцидентом и т.п.); – краткое описание темы (программы) обучения; – ответственное лицо, проводившее обучение; – перечень лиц, прошедших обучение; | | | | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании | |
| Журнал инцидентов, ликвидации их причин и последствий | | <ul style="list-style-type: none"> – дата выявления инцидента; – дата передачи информации об инциденте в подразделение ГосСОПКА (при необходимости); – информационные ресурсы, в которых произошел инцидент; – подробное описание инцидента; – последствия инцидента; – причины инцидента; – мероприятия по устранению последствий инцидента; – мероприятия, направленные на исключения возможности повторения инцидента; | | | | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании | |
| Журнал учета машинных носителей информации | | <ul style="list-style-type: none"> – дата регистрации машинного носителя; – тип машинного носителя; – идентификационный номер машинного носителя; – информационные ресурсы, в которых используется машинный носитель; – описание информации, хранящейся на машинном носителе; – место хранения машинного носителя; – отметка о получении машинного носителя должностным лицом (фамилия, дата, подпись); – отметка о сдаче машинного носителя на хранение; – отметка об уничтожении машинного носителя; – отметка об уничтожении конфиденциальной информации с машинного носителя; – причина уничтожения машинного носителя. | | | | Ответственный за ИБ на ИГЭС под контролем Управления (службы) информационной безопасности головной Компании | |
| <p>Перечень документации является рекомендуемым. Наименование, количество и содержание документов должно быть согласовано с Управлением по ИБ головной Компании на этапе ввода Системы в эксплуатацию.</p> <p>Организационно-распорядительные документы, регламентирующие вопросы обеспечения информационной безопасности разрабатываются в соответствии с положениями Политики информационной безопасности, имеющейся в Компании.</p> | | | | | | | |
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | Лист |
| | | | | | | | |
| | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 <div>77</div> | |

10.2. Подсистема защиты технических средств

Подсистема защиты технических средств предназначена для защиты от физического несанкционированного доступа к защищаемым ИР, а также для защиты от внешних негативных воздействий на ИР модернизируемой Системы. Она включает в себя реализацию следующих мер по обеспечению безопасности информации: ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5 и включает в себя:

1. Управление доступом к физическим ресурсам Системы производится посредством системы контроля и управления доступом (СКУД), а также применением систем безопасности ИГЭС, таких как охранно-пожарная сигнализация, видеонаблюдение, непосредственная охрана подразделениями Росгвардии России.

2. Прокладка линий связи способом, затрудняющим НСД к ним.

3. Обеспечение бесперебойного электропитания компонентов модернизируемой Системы и её средств защиты информации.

4. Размещение компонентов Системы производится в запираемых помещениях, оборудованных системами поддержания микроклимата, охранными системами и СКУД, а также в шкафах, оборудованных запираемыми дверями с сигнализацией на их открытие, а размещение средств визуализации АСУ в местах, исключающих несанкционированное чтение данных с их экранов.

Непосредственная реализация этих мер заключается в том, что для физической защиты технических средств и оборудования организуется, охраняемая территориальными подразделениями Росгвардии контролируемая зона, в которой развернута систем круглосуточного видеонаблюдения, а также функционируют СКУД и охранно-пожарная сигнализация периметра и всех помещений в КЗ. В пределах этой контролируемой зоны постоянно размещаются СВТ, средства защиты информации и средства обеспечения функционирования модернизируемой Системы.

Оборудование Системы размещается в аппаратных помещениях объекта, оснащенных системами кондиционирования и обогрева воздуха для обеспечения температурного режима оборудования. Для размещения оборудования (серверов, АРМ, ПЛК и т.п.) в аппаратных помещениях используются проектируемые серверные шкафы, оснащенные запорными устройствами на открытие дверей. Охрана и организация режима в данном помещении должна исключать возможность неконтролируемого проникновения или пребывания в нём посторонних лиц (потенциальных нарушителей ИБ), а также просмотра посторонними лицами ведущихся там работ.

Прокладка линий связи внутри Объекта осуществляется в труднодоступных местах (эстакады, лотки, за подвесными потолками, под фальшполами, в трубе

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч. | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 78 |

гофрированной). АСУ объекта не имеет подключений к сетям связи общего пользования.

Электроснабжение Объекта выполнено по первой категории особой группы. Источники бесперебойного питания (ИБП) обеспечивают бесперебойную работу модернизируемой Системы Объекта на период времени, достаточный для безаварийного останова технологического процесса при отсутствии внешнего электропитания.

Основное электропитание оборудования СЗИ выполняется от сети переменного тока однофазным напряжением 220В, 50 Гц, с соблюдением требований в части обеспечения надежности электроснабжения к электроприёмникам первой категории. Цепи питания внутренних устройств модернизируемой Системы и полевых устройств защищены автоматами соответствующей мощности.

Питание оборудования в нормальном режиме предусмотрено от резервируемого источника бесперебойного питания 220В двойного преобразования с двойным запасом по мощности не менее 6000 Вт со встроенными аккумуляторными батареями, в аварийном режиме от резервного ввода электрической сети переменного тока (независимого фидера) и резервированных источников питания с аккумуляторными батареями. В случаи перехода питания на резервный ввод, для поддержания Системы в рабочем состоянии предусматриваются источники бесперебойного питания (ИБП) СВТ и сетевого оборудования, с временем резервирования не менее 1 часа.

Видовая информация защищается оптимальным расположением мониторов АРМ, в рабочих помещениях, аппаратных и на иных объектах, исключающим несанкционированный просмотр информации через окна, двери и иные строительные конструкции объекта. На окна в обязательном порядке устанавливаются жалюзи и наклеивается специальная плёнка, предотвращающая возможность утечки видовой информации со средств отображения информации и бумажных носителей. Соблюдается политика «чистого стола», сущность которой заключается в отсутствии на рабочем месте персонала документов или иных носителей информации или их присутствие на время, необходимое для осуществления производственной деятельности и под постоянным контролем за ними ответственного работника. Запрещается держать открытыми двери во все помещения с оборудованием, а также несанкционированное проникновению в эти помещения лиц, не имеющих отношения к функционированию и обеспечению деятельности модернизируемой Системы объекта.

| | | | | | | | | | |
|--------------|--------------|--------------|------|-------|------|-------------------|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | | | | | | | Лист |
| | | | | | | | | | |
| | | | | | | | | | |
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата | П37.2021.01-ИБ.П2 | | | 79 |

ОК, ОК
срочно, Ен+.
Для сведения
12.10.2022



ЕВРОСИБЭНЕРГО

ГИДРОГЕНЕРАЦИЯ

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ЕВРОСИБЭНЕРГО-ГИДРОГЕНЕРАЦИЯ»

(ООО «ЕвроСибЭнерго-Гидрогенерация»)

Тимирязева ул., строение. 4, Иркутская область, г. Иркутск, 664003, тел: +7(3952) 379-359, E-mail: ese-hg@eurosib.ru, ОКПО 22859639, ОГРН 1123850033042, ИНН/КПП 3812142445/997650001

Директору
Иркутская ГЭС
Чеверда В.А.

№ _____
На № _____



О согласовании проектной
документации

Уважаемый Вадим Анатольевич!

В ответ на письмо от 28.09.2022 г. № 244-ПЭСК/0922 от ООО «ПЭСК» сообщаем:

- По первому вопросу - в соответствии с проектом модернизации информационных систем ИГЭС, по требованию архитектурной группы Эн+, в сетях АСУ ТП должны применяться межсетевые экраны CheckPoint сертифицированные ФСТЭК. В соответствии с информационным сообщением ФСТЭК России от 28 апреля 2016 г. N 240/24/1986 в автоматизированных системах управления технологическими или производственными процессами должны применяться межсетевые экраны уровня промышленной сети (тип «Д»), оборудование ООО «Код безопасности» не имеет сертификата ФСТЭК о соответствии требованиям к межсетевым экранам типа «Д». Система виброконтроля из проекта «Комплексная система управления ГА для участия в АВРЧМ. Инв. № КСУ000097931. Модернизация систем виброконтроля» не является значимой и на нее не распространяется требования Указа Президента №166 от 30.03.2022.
- По второму вопросу - не возражаем против введения должности Администратора ИБ.

Начальник управления по ИБ

А.А. Афанасьев

Самусенко А.А.
(3952) 790-158



| | | |
|---------------|--------------|--------------|
| Инва. № подл. | Подп. и дата | Взам. инв. № |
| | | |

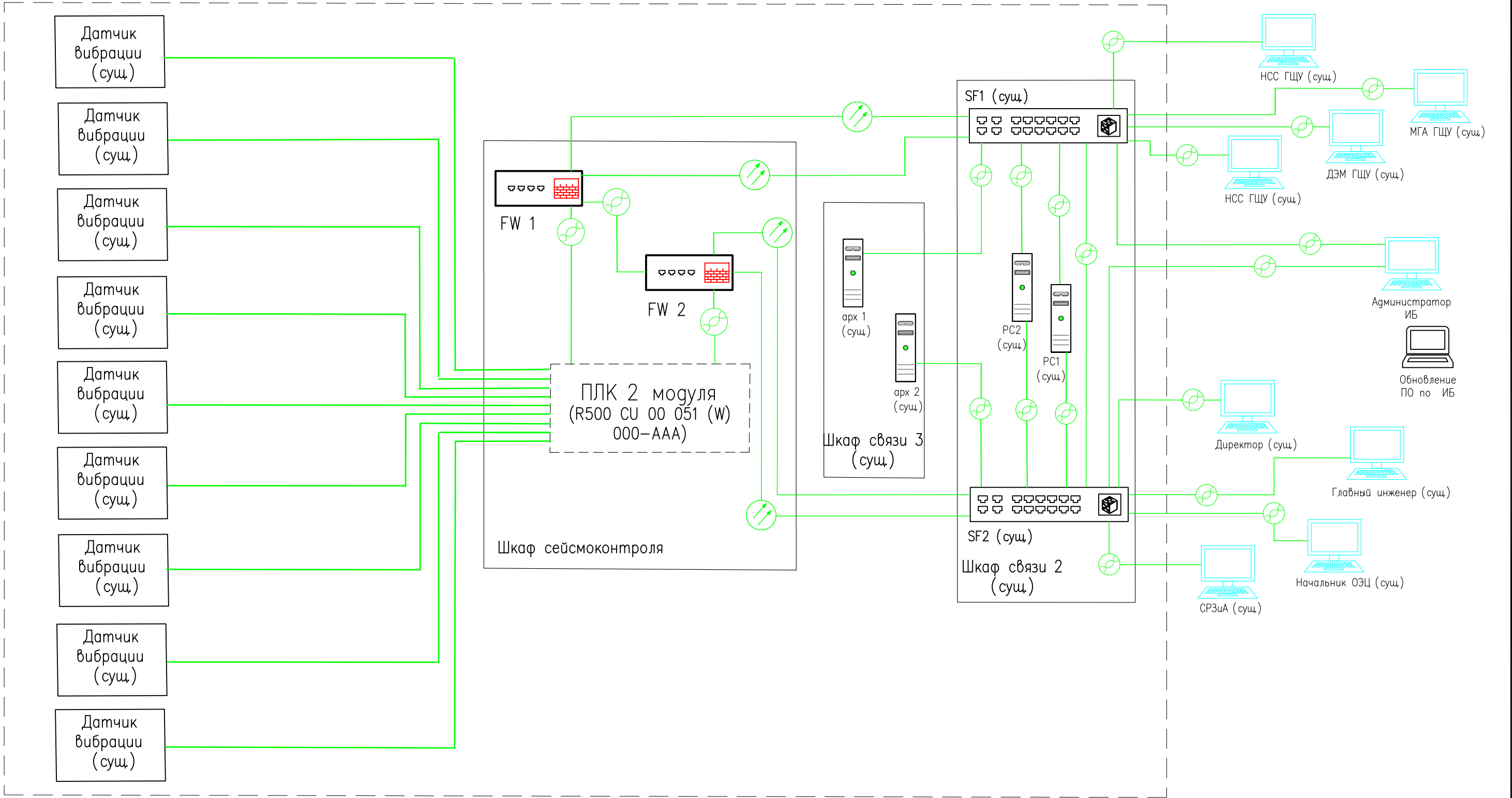
| | | | | | |
|------|--------|------|------|-------|------|
| Изм. | Кол.уч | Лист | №Док | Подп. | Дата |
| | | | | | |

П37.2021.01-ИБ.П2



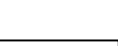



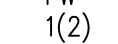


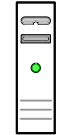
Лист

80

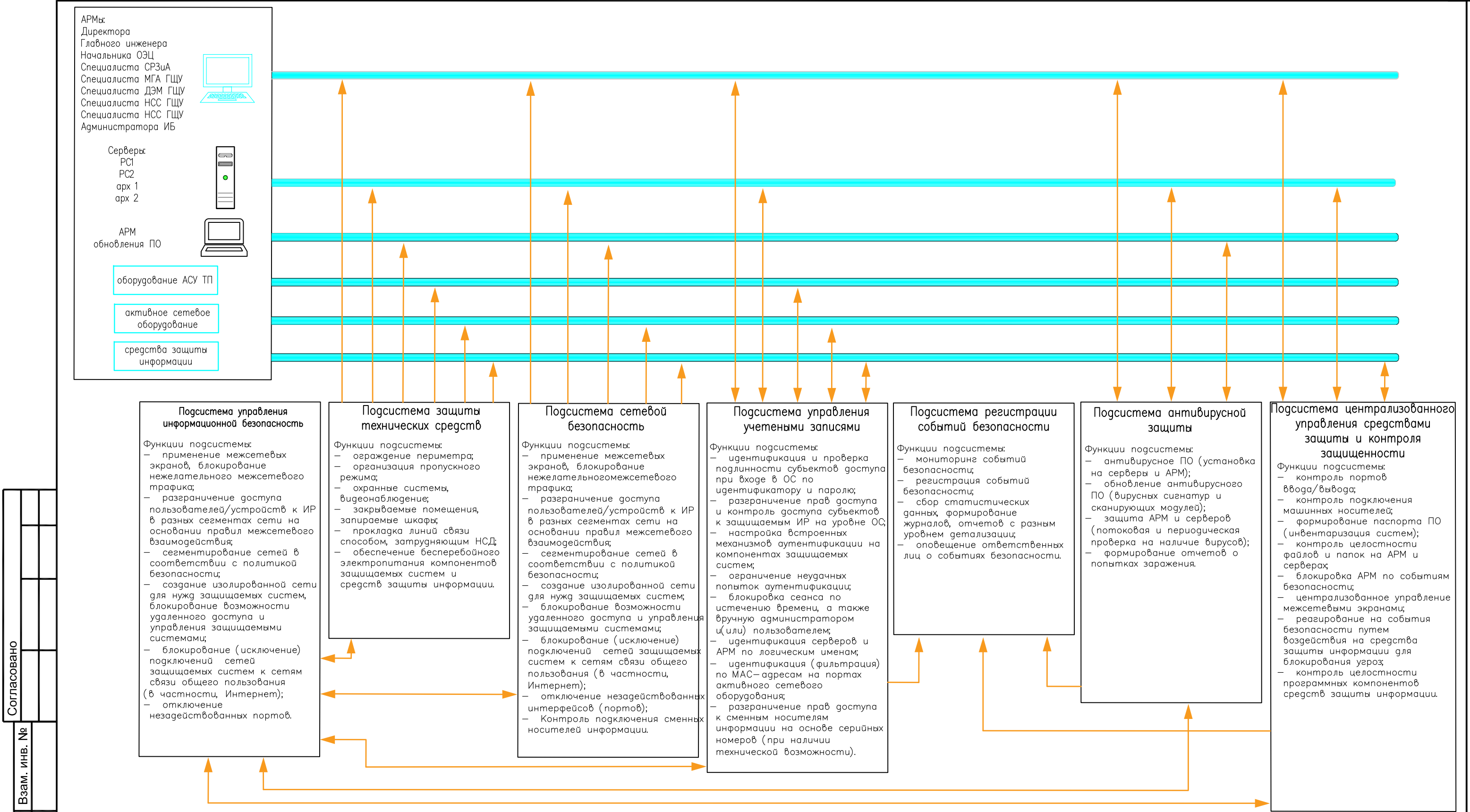
| | | | | | |
|--------------|--|--|--|--|--|
| Согласовано | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Взам. инв. № | | | | | |
| | | | | | |
| Подп. и дата | | | | | |
| | | | | | |
| Инв. № подл. | | | | | |
| | | | | | |



Условные обозначения:

-  — волоконно-оптическая линии связи (ВОЛС)
-  — линии связи витая пара
-  — соединительные линии
-  — маршрутизатор
-  SF 1(2)
-  — модуль CheckPoint 3100
-  FW 1(2)
-  — АРМ
-  — ноутбук
-  — сервер

| | | | | | | | | | |
|-----------|---------|-----------|-------|---|-------|--|---|------|--------|
| | | | | | | П37.2021.01-ИБ.С1 | | | |
| | | | | | | Комплексная система управления ГА для участия в АВРЧМ. Инв. № КСУ000097931. Модернизация систем виброконтроля. | | | |
| Изм. | Кол.уч. | Лист | №Док. | Подп. | Дата | Информационная безопасность | Стадия | Лист | Листов |
| Разраб. | | Денисевич | |  | 07.22 | | П | 1 | |
| Пров. | | Егоров | | | 07.22 | | | | |
| | | | | | | Схема схема комплекса технических средств защиты информации |  | | |
| Н. контр. | | | | | 07.22 | | | | |
| Утв. | | Афендигов | | | | | | | |



| | | | | | |
|--------------|--|--|--|--|--|
| Согласовано | | | | | |
| Взам. инв. № | | | | | |
| Подп. и дата | | | | | |
| Инв. № подл. | | | | | |

Условные обозначения:

— линии функционального взаимодействия (управления)



| | | | | | | | | | |
|-----------|---------|------------|-------|---|-------|--|---|------|--------|
| | | | | | | П37.2021.01-ИБ.С2 | | | |
| | | | | | | Комплексная система управления ГА для участия в АВРЧМ. Инв. № КСУ000097931. Модернизация систем виброконтроля. | | | |
| Изм. | Кол.уч. | Лист | №Док. | Подп. | Дата | Информационная безопасность | Стадия | Лист | Листов |
| Разраб. | | Денисевич | |  | 07.22 | | П | 1 | |
| Пров. | | Егоров | | | 07.22 | | | | |
| | | | | | | Схема функциональной структуры |  | | |
| Н. контр. | | | | | | | | | |
| Утв. | | Афендииков | | | 07.22 | | | | |