Общество с ограниченной ответственностью
«НОВЫЕ РЕСУРСЫ»

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Раздел 10. Иная документация в случаях, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации

Часть 6. Информационная безопасность

Книга 1. Текстовая часть

НКНХ.5273-ПД-ИБ1

Том 10.6.1

2024

Общество с ограниченной ответственностью
«НОВЫЕ РЕСУРСЫ»

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Раздел 10. Иная документация в случаях, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации

Часть 6. Информационная безопасность

Книга 1. Текстовая часть

НКНХ.5273-ПД-ИБ1

Том 10.6.1

Руководитель проектов (подпись, дата) **А.С. Махов**

Главный инженер проекта (подпись, дата) **С.А. Дордий**

2024

Взам. инв. №

Подп. и дата

Инв. № подл.

АО НИП «ИНФОРМЗАЩИТА»

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Раздел 10. Иная документация в случаях, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации

Часть 6. Информационная безопасность

Книга 1. Текстовая часть

НКНХ.5273-ПД-ИБ1

Том 10.6.1

Руководитель проектов (подпись, дата) **Е.А. Козлова**

Главный инженер проекта (подпись, дата) **В.Б. Черкасов**

2024

Взам. инв. №

Подп. и дата

Инв. № подл.

СОДЕРЖАНИЕ ТОМА

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	НКНХ.5273-ПД-ИБ1-С		
Разраб.		Черкасов			11.09.24	Содержание тома	Стадия	Лист	Листов
							П		1
							Информзащита Системный интегратор		
Н. контр.		Скиткин			11.09.24				
ГИП		Черкасов			11.09.24				

АО НИП «ИНФОРМЗАЩИТА»

Информзащита
Системный интегратор

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Ведомость проекта

НКНХ.5273-ПД-ИБ1-ТП

2024

Взам. инв. №

Подп. и дата

Инв. № подл.

ВЕДОМОСТЬ ПРОЕКТА

Обозначение	Формат	Наименование	Примечание
		Раздел 10. Иная документация в случаях, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации	
		Часть 6. Информационная безопасность	
НКНХ.5273-ПД-ИБ1	А4	Книга 1. Текстовая часть	
НКНХ.5273-ПД-ИБ1-ТП	А4	Ведомость технического проекта	Лист 3
НКНХ.5273-ПД-ИБ1-П2	А4	Пояснительная записка по СОИБ	Лист 5
НКНХ.5273-ПД-ИБ1-ИД4	А4	Предварительные настройки комплекса средств защиты информации	Лист 147
НКНХ.5273-ПД-ИБ1-В4	А4,А3	Предварительная спецификация на СОИБ	Лист 187
НКНХ.5273-ПД-ИБ2	А4	Книга 2. Графическая часть	
НКНХ.5273-ПД-ИБ2-С1	А2	Структурная схема комплекса технических средств СОИБ	Лист 3
НКНХ.5273-ПД-ИБ2-С2	А2	Схема функциональной структуры СОИБ	Лист 4
НКНХ.5273-ПД-ИБ2-С3	А2	Схема соединений и подключений СОИБ	Лист 5
НКНХ.5273-ПД-ИБ2-С7	А2	План расположения оборудования СОИБ	Лист 6
НКНХ.5273-ПД-ИБ2-СА	А2	Чертёж установки технических средств	Лист 9

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	НКНХ.5273-ПД-ИБ1-ТП		
Разраб.		Черкасов			11.09.24	Ведомость проекта	Стадия	Лист	Листов
							П		1
Н. контр.		Скиткин			11.09.24		Информзащита Системный интегратор		
ГИП		Черкасов			11.09.24				

АО НИП «ИНФОРМЗАЩИТА»

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Пояснительная записка по СОИБ

НКНХ.5273-ПД-ИБ1-П2

2024

Взам. инв. №

Подп. и дата

Инв. № подл.

СОДЕРЖАНИЕ

Лист

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	НКНХ.5273-ПД-ИБ1-П2		
Разраб.		Черкасов			11.09.24	Пояснительная записка по СОИБ	Стадия	Лист	Листов
							П	1	135
Н. контр.		Скиткин			11.09.24		Информзащита Системный интегратор		
ГИП		Черкасов			11.09.24				

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Цель реализации проектных решений по обеспечению ИБ

Целью реализации проектных решений по обеспечению ИБ является обеспечение целостности и доступности защищаемых ресурсов – ОКИИ ПАО «Нижнекамскнефтехим». Внедрение проектных решений по обеспечению ИБ повысит уровень защищенности и устойчивости функционирования ЗОКИИ, что обеспечит предотвращение и (или) снижение ущерба от инцидентов ИБ и стабильности основных производственных процессов, а также обеспечит соответствие требованиям законодательства Российской Федерации в области защиты объектов критической информационной инфраструктуры.

ИБ обеспечивается на всех технологических этапах ее обработки и во всех режимах функционирования ОКИИ.

1.2 Сведения о системе

Полное наименование системы: Система обеспечения безопасности объектов критической информационной инфраструктуры ПАО «Нижнекамскнефтехим».

Краткое наименование системы: СОИБ ОКИИ, Система.

1.3 Перечень документов, на основании которых создается АС

Проектная документация разработана на основании следующих документов:

– Решение п. 4.1 Протокола технического совета по реализации Проекта «Строительство магистрального этиленопровода «Нижнекамск-Казань» от 13.10.2023 г;

– Договор № 0085.2023 на выполнение проектно-изыскательских работ от 10.01.2024;

– Задание № 2 на разработку проектной документации по объекту «Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600».

Заказчиком технической документации является Публичное акционерное общество «Нижнекамскнефтехим» (ПАО «Нижнекамскнефтехим»). Полный юридический адрес Заказчика – 423574, Республика Татарстан,Нижнекамский район, г. Нижнекамск, ул. Соболековская, зд. 23, офис 129.

1.4 Перечень организаций, участвующих в разработке АС

Генеральный заказчик: Публичное акционерное общество «Нижнекамскнефтехим» (ПАО «Нижнекамскнефтехим»).

Заказчик: Общество с ограниченной ответственностью «НОВЫЕ РЕСУРСЫ» (ООО «НОВЫЕ РЕСУРСЫ»).

Подрядчик: Акционерное общество НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ «ИНФОРМЗАЩИТА» (АО НИП «ИНФОРМЗАЩИТА»).

1.5 Сведения об использованных нормативно-технических документах

1) Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2) Федеральный закон Российской Федерации № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».

3) Федеральный закон от 21 июля 2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

4) Указ Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

5) Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня лей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

6) Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

7) Приказ ФСТЭК России от 21.12.2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

8) Приказ ФСТЭК России от 22.12.2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (в ред. приказа ФСТЭК России от 21.03.2019 № 59)»;

9) Приказ ФСТЭК от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

10) «Методический документ. Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 5 февраля 2021 г.).

11) ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»;

12) ГОСТ Р 59793-2021 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

13) ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

14) ГОСТ Р 21.101–2020 «Основные требования к рабочей и проектной документации»;

15) ГОСТ Р 59792-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем».

2 ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

Объектами защиты являются информационные системы, информационно-телекоммуникационных сетей и автоматизированные системы управления технологическими процессами магистрального этиленопровода «Нижнекамск - Казань» ПАО «Нижнекамскнефтехим», которые обрабатывают информацию, необходимую для обеспечения критических процессов.

2.1 Автоматизированные системы

2.1.1 Описание защищаемых объектов

Автоматизированные системы магистрального этиленопровода «Нижнекамск - Казань» ПАО «Нижнекамскнефтехим» объединены в следующие ОКИИ:

– Автоматизированная система управления технологическим процессом (АСУТП), включая следующие подсистемы:

  - Система линейной телемеханики (СЛТМ);
  - Система обнаружения утечек (СОУ);
  - Система мониторинга протяженных объектов (СМПО);
  - Структурированная система мониторинга и управления инженерными системами зданий и сооружений (СМИС);
  - Автоматизированная система диспетчерского управления электроснабжением (АСДУЭ);

– Автоматическая система противопожарной защиты (АСПЗ);

– Локальная система оповещения (ЛСО);

– Система пожарной сигнализации (СПС);

– Комплекс инженерно-технических средств охраны (КИТСО).

Все включаемые в ОКИИ автоматизированные системы используют единые линии связи (ВОЛС) для передачи данных (основная ВОЛС / резервная ВОЛС), имеют схожий уровень ущерба в случае вывода из строя или нарушения штатного функционирования автоматизированных систем вследствие преднамеренной или непреднамеренной компьютерной атаки.

Структурные схемы защищаемых ОКИИ, а также перечень компонентов описаны в документе НКНХ.5273-ПД-ИБ-ОТ «Отчет о результатах предварительного категорирования потенциальных значимых объектов критической информационной инфраструктуры».

2.1.1.1 Автоматизированная система управления технологическим процессом (АСУТП)

СЛТМ предназначена для обеспечения дистанционного автоматизированного режима управления рассредоточенными (линейными) объектами Магистрального продуктопровода (МП) без постоянного присутствия обслуживающего персонала на объектах, обеспечения необходимого качества, надёжности контроля и управления.

СОУ предназначена для определения факта нарушения целостности МП и определения координат места утечки во всех режимах функционирования, включая стационарные и нестационарные, на участках с полным и неполным заполнением сечения трубопроводов.

СМПО предназначена для определения факта нарушения целостности МП и определения координат места утечки во всех режимах функционирования, включая стационарные и нестационарные, на участках с полным и неполным заполнением сечения трубопроводов. Так же должен быть обеспечен функционал контроля утечек в вытяжных свечах на ответственных переходах.

СМИС предназначена для недопущения потерь, ущерба здоровью людей, материального ущерба в условиях действия дестабилизирующих факторов, а также информационной поддержки принятия решений дежурными службами по предупреждению и ликвидации пожаров, аварий.

АСДУЭ предназначена для автоматизированного контроля и управления в реальном масштабе времени оборудованием энергоснабжения

2.1.1.2 Автоматическая система противопожарной защиты (АСПЗ)

АСПЗ предназначена для:

– исключение условий (уменьшением количества) образования горючей среды на территории, отведенной под строительство линейного объекта;

– исключение условий образования в горючей среде (внесения в нее) источников зажигания, что соответствует требованиям п. 2.1. ГОСТ 12.1.004-91 и ст.48 №123-ФЗ от 22.07.2008.

2.1.1.3 Локальная система оповещения (ЛСО)

ЛСО предназначена для своевременного доведения сигнала «ВНИМАНИЕ ВСЕМ» и информации об угрозе чрезвычайной ситуации (аварии), а также информации о развитии событий и рекомендаций населению по дальнейшим действиям в автоматизированном режиме до персонала и людей в границах зоны действия ЛСО.

2.1.1.4 Система пожарной сигнализации (СПС)

СПС предназначена для автоматизации сбора, обработки информации, управления в автоматическом и ручном режимах исполнительными устройствами систем противопожарной защиты по заданному алгоритму, формирования сигналов управления инженерным и технологическим оборудованием, участвующим в обеспечении пожарной безопасности объекта.

2.1.1.5 Комплекс инженерно-технических средств охраны (КИТСО)

КИТСО предназначена для обеспечения безопасности контролируемых зон объекта, объединенных на основе единого программного комплекса в общую информационную среду с единой базой данных.

2.1.1.6 Сведения о защищаемых ОКИИ

Сведения о структуре ОКИИ, функциональных характеристиках, архитектуре, а также составе программно-технических компонентов ОКИИ представлены в документе

«Отчет о результатах предварительного категорирования потенциальных значимых объектов критической информационной инфраструктуры» (НКНХ.5273-ПД-ИБ-ОТ).

2.1.2 Архитектура ОКИИ

Архитектура защищаемых ОКИИ представляет территориально распределенные, многоуровневые системы, которые включают в себя три взаимосвязанных между собой уровня:

– уровень 0: уровень контрольно-измерительных приборов и исполнительных механизмов (уровень КИПиА);

– уровень 1 (нижний): уровень локальных САУ технологических установок, цехов, блоков;

– уровень 2 (верхний): уровень оперативно-производственных служб, включающий серверное оборудование и АРМ;

– уровень 3: информационная сеть верхнего уровня, в которой размещаются хосты верхнего уровня (АРМ, серверы управления и контроля технологических процессов);

– уровень 4: демилитаризованная зона для взаимодействия технологических сетей с КСПД.

2.2 Персональные данные

Персональные данные в ОКИИ не обрабатываются.

2.3 Объекты защиты

Объектами защиты являются компоненты ОКИИ верхнего уровня: АРМ, серверы.

2.4 Интеграция и унификация

При анализе объекта рассматривается возможность унификации и интеграции с решениями по ИБ, существующими в эксплуатирующей организации или предусмотренными иными проектами.

3 КРИТИЧЕСКИЕ ПРОЦЕССЫ

Проектируемые системы включают в себя информационную инфраструктуру, в связи с этим требуется рассмотрение ОКИИ на отнесение к КИИ Российской Федерации согласно требованиям Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 №187-ФЗ.

Субъектом информационной инфраструктуры согласно 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» является российское юридическое лицо, которому на праве собственности принадлежат (при эксплуатации проектируемого энергоцентра) автоматизированные системы управления в сфере топливно-энергетического комплекса.

В рамках обследования ОКИИ осуществляется анализ критических процессов, автоматизируемых рассматриваемыми системами.

Процессы, автоматизируемые ОКИИ, являются критическими, если их нарушение может привести в свою очередь к нарушению процесса управления технологическим оборудованием. Основные критические процессы ОКИИ представлены в Таблица 3.1.

Таблица 3.1 – Критические процессы защищаемых ОКИИ

Наименование ОКИИ	Адреса размещения	Назначение ОКИИ	Критические процессы	Архитектура ОКИИ
АСУТП	Республика Татарстан, территории Нижнекамского муниципального района (в т.ч. г. Нижнекамск); Тукаевского муниципального района, Мамадышского муниципального района; Сабинского муниципального района, Тюлячинского муниципального района, Арского муниципального района, Пестречинского муниципального района, Высокогорского муниципального района, Зеленодольского муниципального района, муниципальное образование город Казань	Управление объектами Магистрального продуктопровода (МП), в том числе и контроль целостности. Управление энергоснабжением.	Транспортировка этилена. Обеспечение автоматического и автоматизированного управления оборудованием электроснабжения.	SCADA-система
АСПЗ		Исключение условий образования горючей среды на территории, источников зажигания в горючей среде	Отсутствуют	АСУ
ЛСО		Доведение информации об угрозе чрезвычайной ситуации (аварии), рекомендаций населению по дальнейшим действиям	Отсутствуют	АСУ
СПС		Управление устройствами систем противопожарной защиты	Отсутствуют	АСУ
КИТСО		Обеспечение безопасности контролируемых зон объекта	Отсутствуют	АСУ

Перечисленные ОКИИ подлежат предварительному категорированию.

4 АНАЛИЗ УГРОЗ ИБ И ОПИСАНИЕ МОДЕЛИ ПОТЕНЦИАЛЬНОГО НАРУШИТЕЛЯ

4.1 Угрозы ИБ

Под угрозами безопасности информации при ее обработке в ОКИИ понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности информации при ее обработке в ОКИИ могут быть связаны как с непреднамеренными действиями работников, осуществляющих обслуживание и поддержку ОКИИ, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от пользователей и эксплуатирующего персонала, осуществляющих обслуживание и поддержку ОКИИ, в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности информации.

4.2 Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

В ходе оценки возможных негативных последствий также был произведен анализ нарушений свойств конфиденциальности (К), целостности (Ц) и доступности (Д) информации, обрабатываемой в ОКИИ, в результате которых возможно наступление тех или иных негативных последствий.

С учетом перечня основных процессов обработки информации и иных процессов, реализуемых с использованием ОКИИ, была проведена экспертная оценка возможных негативных последствий от реализации угроз безопасности информации, результаты которой представлены в Таблица 4.1.

Таблица 4.1 – Перечень видов рисков (ущербов) и негативных последствий, которые могут наступить в случае нарушения или прекращения основных процессов, реализуемых с использованием ОКИИ

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
У1	Ущерб физическому лицу	Угроза жизни или здоровью	Применимо	В случае возникновения компьютерных инцидентов в ОКИИ возможно причинение вреда жизни или здоровью людей (до 50 человек)	нет	да	да
		Унижение достоинства личности	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Нарушение свободы, личной неприкосновенности	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Нарушение неприкосновенности частной жизни	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Нарушение личной, семейной тайны, утрата чести и доброго имени	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Нарушение тайны переписки, телефонных переговоров, иных сообщений	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Финансовый, иной материальный ущерб физическому лицу	Неприменимо	В ОКИИ не обрабатываются персональные данные, банковская тайна	-	-	-
		Нарушение конфиденциальности (утечка) персональных данных	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		«Травля» гражданина в сети «Интернет»	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Разглашение персональных данных граждан	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Нарушение законодательства Российской Федерации	Неприменимо	ОКИИ не обеспечивает реализацию процессов, требования к функционированию которых установлено законодательством Российской Федерации, в ОКИИ не обрабатывается информация, необходимая для выполнения таких процессов	-	-	-
		Потеря (хищение) денежных средств	Неприменимо	В ОКИИ не обрабатывается финансовая информация, а также отсутствуют подключения к финансовым системам	-	-	-
		Недополучение ожидаемой (прогнозируемой) прибыли	Применимо	В случае нарушения функционирования ОКИИ возможна остановка технологического процесса или снижение его производительности и, как следствие, недополучение прибыли	нет	да	да
		Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	Применимо	Нарушение или остановка технологических процессов, обеспечиваемых с использованием ОКИИ, может привести к возникновению дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	нет	да	да

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка ПО, ТС, вышедших из строя, замена, настройка, ремонт указанных средств)	Применимо	В случае возникновения компьютерных инцидентов в ОКИИ возможны негативные последствия, которые могут привести к повреждению отдельного технологического оборудованию, необходимости его дальнейшего ремонта/ замены	нет	да	да
		Нарушение штатного режима функционирования АСУ и управляемого объекта и/или процесса	Применимо	В случае возникновения компьютерных инцидентов в ОКИИ возможно нарушение штатного режима функционирования управляемого ОКИИ технологического оборудования	нет	да	да
		Срыв запланированной сделки с партнером	Применимо	Нарушение или остановка технологических процессов, обеспечиваемых с использованием ОКИИ, может привести к срывам запланированных сделок	нет	да	да
		Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Применимо	Выход из строя технологического оборудования, управляемого с использованием ОКИИ, может повлечь необходимость дополнительных затрат на восстановление деятельности	нет	да	да
		Потеря клиентов, поставщиков	Неприменимо	Возможный выхода из строя ОКИИ и управляемого с использованием ОКИИ технологического оборудования не повлечет за собой потерю клиентов и поставщиков	-	-	-
		Потеря конкурентного преимущества	Применимо	Выход из строя, управляемого средствами ОКИИ технологического оборудования, может повлиять на финансовые показатели организации	нет	да	да
		Невозможность заключения договоров, соглашений	Применимо	Длительный период восстановления после возможного выхода из строя ОКИИ может привести к невозможности заключения новых договоров, соглашений	нет	да	да
		Нарушение деловой репутации	Применимо	В результате выхода из строя ОКИИ и управляемого с использованием ОКИИ технологического оборудования возможно нарушение сроков и объемов выполнения договорных обязательств, что негативно скажется на репутации	нет	да	да

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Снижение престижа	Применимо	В результате выхода из строя ОКИИ и управляемого с использованием ОКИИ технологического оборудования возможно возникновение последствий, повлекших причинение ущерба жизни и здоровья людей и т.д., что негативно скажется на престиже	нет	да	да
		Дискредитация работников	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Утрата доверия	Применимо	В результате выхода из строя ОКИИ и управляемого с использованием ОКИИ технологического оборудования возможно нарушение сроков и объемов выполнения договорных обязательств, что негативно скажется на доверии к Компании	нет	да	да
		Причинение имущественного ущерба	Применимо	Выход из строя технологического оборудования, управляемого с использованием ОКИИ, может повлечь необходимость дополнительных затрат на восстановление деятельности	нет	да	да
		Неспособность выполнения договорных обязательств	Применимо	В результате выхода из строя ОКИИ и управляемого с использованием ОКИИ технологического оборудования возможно нарушение сроков и объемов выполнения договорных обязательств	нет	да	да
		Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	Применимо	В результате выхода из строя ОКИИ и управляемого с использованием ОКИИ технологического оборудования возможно нарушение или прекращение технологических и производственных процессов	нет	да	да
		Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	Неприменимо	Возможный выход из строя ОКИИ не приведет к необходимости перестроения основных процессов Компании	-	-	-
		Принятие неправильных решений	Неприменимо	Возможный выход из строя ОКИИ не повлечет за собой принятие неправильных организационных и руководительских решений в масштабах Компании	-	-	-
		Простой информационной системы или сети	Применимо	В случае возникновения компьютерных инцидентов в ОКИИ возможно нарушение функционирования ОКИИ в целом или ее отдельных компонентов	нет	да	да

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Публикация недостоверной информации на веб-ресурсах организации	Неприменимо	ОКИИ не связана с веб-ресурсами организации	-	-	-
		Использование веб-ресурсов для распространения и управления вредоносным ПО	Неприменимо	ОКИИ не связана с веб-ресурсами организации	-	-	-
		Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени	Неприменимо	ОКИИ не связана с веб-ресурсами организации, из с использованием которых возможна отправка информационных сообщений от имени организации	-	-	-
		Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	Неприменимо	В ОКИИ не обрабатываются данные, относящиеся к коммерческой тайне, а также иные коммерческие конфиденциальные данные	-	-	-
У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Причинение ущерба жизни и здоровью людей	Применимо	В случае возникновения компьютерных инцидентов на ОКИИ возможно причинение вреда жизни или здоровью людей (в масштабе до 50 человек)	нет	да	да
		Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не обеспечивает функционирование объектов жизнедеятельности населения	-	-	-
		Прекращение или нарушение функционирования объектов транспортной инфраструктуры	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не относятся к объектам транспортной инфраструктуры	-	-	-
		Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не относятся к объектам, участвующим в функционировании государственных органов	-	-	-
		Прекращение или нарушение функционирования сети связи	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не относятся к объектам, участвующим в функционировании сетей связи	-	-	-
		Отсутствие доступа к государственной услуге	Неприменимо	С использованием ОКИИ и управляемого ОКИИ технологического оборудования не осуществляется предоставление государственных услуг	-	-	-

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации	Неприменимо	Компания не является лицом, уполномоченным для заключения международных договоров от имени Российской Федерации	-	-	-
		Снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием	Неприменимо	Компания не относится к государственным корпорациям или организациям с государственным участием	-	-	-
		Возникновение ущерба бюджетам Российской Федерации	Неприменимо	В случае нарушения функционирования ОКИИ возможна остановка технологического процесса или снижение его производительности и, как следствие, недополучение прибыли, что, в свою очередь, потенциально приведет к снижению налоговых выплат в бюджеты Российской Федерации и субъектов Российской Федерации	-	-	-
		Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не относится к объектам финансового сектора	-	-	-
		Вредные воздействия на окружающую среду	Неприменимо	Нарушение функционирования ОКИИ и управляемого с использованием ОКИИ технологического оборудования не может повлечь вредные воздействия на окружающую среду	-	-	-

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Прекращение или нарушение функционирования пункта управления (ситуационного центра)	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не используются для поддержания выполнения своих функций пунктами управления (ситуационными центрами)	-	-	-
		Снижение показателей государственного оборонного заказа	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не используется для выполнения государственных оборонных заказов	-	-	-
		Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не используется для целей обеспечения обороны страны, безопасности государства и правопорядка	-	-	-
		Нарушение законодательства Российской Федерации	Неприменимо	ОКИИ не обеспечивает реализацию процессов, требования к функционированию которых установлено законодательством Российской Федерации, в ОКИИ не обрабатывается информация, необходимая для выполнения таких процессов	-	-	-
		Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др.	Неприменимо	ОКИИ не относится к системам СМИ, не предоставляет информацию в СМИ, не является источником данных, на основании которых формируется информация для СМИ	-	-	-
		Нарушение штатного режима функционирования АСУ и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов	Применимо	Нарушение работы ОКИИ может привести к нарушению штатного режима функционирования управляемого объекта и привести к выводу из строя технологических объектов и их компонентов	нет	да	да
		Нарушение общественного правопорядка, возможность потери или снижения уровня контроля за общественным правопорядком	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не связаны с процессами поддержания общественного правопорядка и контролем за общественным правопорядком	-	-	-

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Нарушение выборного процесса	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не связаны с выборными процессами	-	-	-
		Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не связаны с процессами оперативного оповещения населения о чрезвычайной ситуации	-	-	-
		Организация пикетов, забастовок, митингов и других акций	Неприменимо	Нарушение функционирования ОКИИ и управляемого с использованием ОКИИ технологического оборудования не приведет к организации пикетов, забастовок, митингов и других акций	-	-	-
		Массовые увольнения	Неприменимо	Нарушение функционирования ОКИИ и управляемого с использованием ОКИИ технологического оборудования не приведет к массовым увольнениям	-	-	-
		Увеличение количества жалоб в органы государственной власти или органы местного самоуправления	Неприменимо	Нарушение функционирования ОКИИ и управляемого с использованием ОКИИ технологического оборудования не приведет к увеличению количества жалоб в органы государственной власти или органы местного самоуправления	-	-	-
		Появление негативных публикаций в общедоступных источниках	Применимо	Нарушение функционирования ОКИИ и управляемого с использованием ОКИИ технологического оборудования может повлечь негативные последствия, связанные с возникновениями аварий, информация о которых может быть опубликована в средствах массовой информации и иных общедоступных источниках	да	да	да
		Создание предпосылок к внутриполитическому кризису	Неприменимо	Нарушение функционирования ОКИИ и управляемого с использованием ОКИИ технологического оборудования не приведет к созданию предпосылок к внутриполитическому кризису	-	-	-

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия	Применимость	Обоснование оценки (кратко)	Нарушаемые свойства		
					К	Ц	Д
		Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов	Неприменимо	В ОКИИ не обрабатываются персональные данные	-	-	-
		Доступ к системам и сетям с целью незаконного использования вычислительных мощностей	Применимо	Вычислительные мощности отдельных компонентов ОКИИ технически могут быть несанкционированного использованы	нет	нет	да
		Использование веб-ресурсов государственных органов для распространения и управления вредоносным ПО	Неприменимо	ОКИИ не относится к веб-ресурсам государственных органов	-	-	-
		Утечка информации ограниченного доступа	Применимо	В случае злонамеренного воздействия на ОКИИ возможна утечка информации ограниченного доступа (например, сведений об учетных записях, конфигурационной информации и др.)	да	нет	нет
		Непредоставление государственных услуг	Неприменимо	ОКИИ и управляемое с использованием ОКИИ технологическое оборудование не связаны с процессами предоставления государственных услуг	-	-	-

Нарушение свойств К, Ц, Д информации, обрабатываемой в ОКИИ, может повлечь за собой возникновение компьютерных инцидентов и негативных последствий.

По результатам анализа возможных негативных последствий, а также нарушаемых свойств информации, обрабатываемой в ОКИИ, были определены следующие виды воздействий на ОКИИ, которые могут привести к негативным последствиям:

- отказ в обслуживании, модификация (подмена) данных;
- нарушение функционирования ТС;
- утечка данных (нарушение конфиденциальности);
- НСД;

– несанкционированное использование вычислительных ресурсов ОКИИ.

4.3 Возможные объекты воздействия угроз безопасности информации в ОКИИ

В качестве источника исходных данных о применяемых информационных технологиях и методах обработки информации, а также объектах воздействия угроз, используемых в ходе осуществления сценария таких угроз, используется банк данных угроз безопасности ФСТЭК России (bdu.fstec.ru). Рассматриваемые в настоящем документе информационные технологии и методы обработки информации, а также объекты воздействия, сгруппированы по типам, а их обозначения адаптированы для удобства использования.

4.3.1 Определение применяемых информационных технологий и объектов воздействия угроз

Сгруппированные по классам объекты воздействия в соответствии с банком данных угроз безопасности ФСТЭК России (bdu.fstec.ru), которые входят в состав ОКИИ, представлены в Таблица 4.2.

Таблица 4.2 – Применимые объекты воздействия угроз безопасности информации, обрабатываемой в ОКИИ

№ п/п	Объект воздействия	Применимость в ОКИИ
Объекты воздействия общего типа		
1	Информационная система/ АСУ/ информационно-телекоммуникационная сеть	Применимо
2	Средства защиты информации	Применимо
Объекты воздействия информационного типа		
3	Защищаемые данные	Применимо
4	Сетевой трафик	Применимо
5	Инфраструктура информационной системы	Применимо
6	Объекты файловой системы	Применимо
7	Метаданные	Применимо
Объекты воздействия аппаратного (физического) типа		
8	Аппаратное обеспечение	Применимо
9	Каналы связи	Применимо
10	Носители информации	Применимо
11	Рабочие станции	Применимо
12	Серверы	Применимо
13	Сетевое оборудование	Применимо
14	ТС воздушного кондиционирования, включая трубопроводные системы для циркуляции охлажденного воздуха в центре обработки данных, ПЛК, распределенные системы контроля, управленческие системы и другие программные средства контроля	Применимо
Объекты воздействия программного типа		
15	СПО	Применимо
16	ППО	Применимо
17	Сетевое ПО	Применимо
18	Реестр	Применимо

№ п/п	Объект воздействия	Применимость в ОКИИ
Объекты воздействия BIOS/UEFI		
19	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Применимо
Объекты воздействия средств виртуализации		
20	Гипервизоры	Применимо
21	Консоли управления гипервизорами	Применимо
22	Виртуальные устройства	Неприменимо
23	Виртуальные машины	Применимо
24	Образы виртуальных машин	Неприменимо
25	Виртуальные диски	Неприменимо
Объекты воздействия мобильных устройств		
26	Мобильные устройства и запущенные на них приложения (ПО, аппаратное устройство)	Неприменимо
27	Данные пользователя мобильных устройств	Неприменимо
Объекты воздействия АСУ ТП и технологического оборудования		
28	ПО АСУ ТП	Применимо
29	ПЛК	Применимо
Объекты воздействия облачных сервисов		
30	Облачная инфраструктура	Неприменимо
31	Облачная инфраструктура, созданная с использованием технологий виртуализации	Неприменимо
32	Консоли управления облачной инфраструктурой	Неприменимо
33	Облачные системы	Неприменимо
34	Информационные системы, иммигрированные в облако	Неприменимо
35	Облачные серверы	Неприменимо
Объекты воздействия грид-систем		
36	Грид-система	Неприменимо
37	Ресурсные центры грид-системы	Неприменимо
38	Узлы грид-системы	Неприменимо
Объекты воздействия хранилищ больших данных		
39	Хранилище больших данных	Неприменимо
40	Узлы хранилища больших данных	Неприменимо
41	Система разграничения доступа хранилища больших данных	Неприменимо
Объекты воздействия суперкомпьютеров		
42	Вычислительные узлы суперкомпьютера	Неприменимо
43	Системы хранения данных суперкомпьютера	Неприменимо
44	Каналы передачи данных суперкомпьютера	Неприменимо

Исходя из приведенных выше применимых объектов воздействия и описаний сценариев реализации угроз безопасности можно выделить общие классы уязвимостей, представленные в Таблица 4.3.

Таблица 4.3 – Классы уязвимостей объектов воздействия угроз ОКИИ

№	Классы уязвимостей объектов воздействия угроз ОКИИ
1. Уязвимости СПО:	
1.1	уязвимости в средствах СПО, предназначенных для управления локальными ресурсами ОКИИ (управление процессами, памятью, устройствами ввода/вывода и т.п.), драйверах, утилитах
1.2	уязвимости в средствах СПО, предназначенных для вспомогательных функций (архивирование, дефрагментация и пр.), библиотеках процедур различного назначения
1.3	уязвимости в сетевых средствах СПО
2. Уязвимости ППО:	
2.1	уязвимости функций, процедуры, изменение параметров которых определенным образом позволяет использовать их для НСД без обнаружения таких изменений ППО
2.2	отсутствие необходимых средств защиты (проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.)
2.3	ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации
2.4	уязвимости функций и процедур, относящихся к разным прикладным программам и несовместимым между собой (не функционирующие в одной ОС) из-за конфликтов, связанных с распределением ресурсов системы
2.5	уязвимости функций, процедур, изменение определенным образом параметров которых позволяет использовать их для проникновения в СПО компонентов ОКИИ и использования штатных функций СПО, выполнения НСД без обнаружения таких изменений СПО
3. Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных:	
3.1	аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)
3.2	права доступа по умолчанию
3.3	наличие открытых портов
3.4	отсутствие механизма предотвращения перегрузок буфера
3.5	отсутствие аутентификации управляющих сообщений об изменении маршрута
3.6	отсутствие механизма проверки корректности заполнения служебных заголовков пакета
3.7	отсутствие средств проверки аутентификации полученных данных от источника
3.8	отсутствие поддержки аутентификации заголовков сообщений
4. Уязвимости, вызванные недостатками организации защиты информации:	
4.1	отсутствие необходимых организационно-распорядительных документов
4.2	недостаточный контроль эффективности мероприятий по защите информации в структурных подразделениях, имеющих доступ к ОКИИ
4.3	незнание или игнорирование работниками требований ИБ при работе в ОКИИ
5. Уязвимости применяемых СрЗИ	
6. Уязвимости программно-технических средств, входящих в состав ОКИИ, вызванные их сбоями и отказами в работе	

4.3.2 Определение видов воздействия на объекты воздействия угроз

С учетом определенных ранее применимых объектов воздействия угроз безопасности информации и возможных негативных последствий были определены виды воздействия на объекты воздействия угроз безопасности информации в ОКИИ, они представлены в таблице (Таблица 4.4).

Таблица 4.4 – Виды воздействия на объекты воздействия угроз безопасности информации в ОКИИ

Негативные последствия	Объект воздействия	Виды воздействия
(У1) Угроза жизни или здоровью (У2) Недополучение ожидаемой (прогнозируемой) прибыли/ Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка ПО, ТС, вышедших из строя, замена, настройка, ремонт указанных средств)/ Нарушение штатного режима функционирования АСУ и управляемого объекта и/или процесса/ Необходимость дополнительных (незапланированных) затрат на восстановление деятельности/ Потеря конкурентного преимущества/ Невозможность заключения договоров, соглашений/ Нарушение деловой репутации/ Снижение престижа/ Утрата доверия/ Причинение имущественного ущерба/ Неспособность выполнения договорных обязательств/ Невозможность решения задач (реализации функций) или снижение эффективности/ решения задач (реализации функций)/ (У3) Причинение ущерба жизни и здоровью людей/ Нарушение штатного режима функционирования АСУ и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов/ Появление негативных публикаций в общедоступных источниках	Объекты воздействия общего типа	
	Информационная система / АСУ / информационно-телекоммуникационная сеть	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	СрЗИ	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Объекты воздействия информационного типа	
	Защищаемые данные	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Сетевой трафик	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Инфраструктура информационной системы	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Объекты файловой системы	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Метаданные	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Объекты воздействия аппаратного (физического) типа	
	Аппаратное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
		Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Каналы связи	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
		Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Носители информации	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Рабочие станции	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации

Негативные последствия	Объект воздействия	Виды воздействия
	Серверы	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
		Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Сетевое оборудование	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
		Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	ТС воздушного кондиционирования, включая трубопроводные системы для циркуляции охлажденного воздуха в центре обработки данных, ПЛК, распределенные системы контроля, управленческие системы и другие программные средства контроля	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Объекты воздействия программного типа	
	СПО	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	ППО	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Сетевое ПО	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	Объекты воздействия BIOS/UEFI	
	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
		Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Объекты воздействия АСУ ТП и технологического оборудования	
	ПО АСУ ТП	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных
	ПЛК	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных

Негативные последствия	Объект воздействия	Виды воздействия
(У3) Доступ к системам и сетям с целью незаконного использования вычислительных мощностей	Объекты воздействия общего типа	
	Информационная система/ АСУ/ информационно-телекоммуникационная сеть	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	СрЗИ	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Объекты воздействия аппаратного (физического) типа	
	Аппаратное обеспечение	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Каналы связи	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Носители информации	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Рабочие станции	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Серверы	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Сетевое оборудование	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	ТС воздушного кондиционирования, включая трубопроводные системы для циркуляции охлажденного воздуха в центре обработки данных, ПЛК, распределенные системы контроля, управленческие системы и другие программные средства контроля	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Объекты воздействия BIOS/UEFI	
	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
	Объекты воздействия АСУ ТП и технологического оборудования	
	ПЛК	Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации
(У3) Утечка информации ограниченного доступа	Объекты воздействия общего типа	
	Информационная система/ АСУ/ информационно-телекоммуникационная сеть	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	СрЗИ	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Объекты воздействия информационного типа	
	Защищаемые данные	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Сетевой трафик	Перехват защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Инфраструктура информационной системы	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)

Негативные последствия	Объект воздействия	Виды воздействия
	Объекты файловой системы	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Метаданные	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Объекты воздействия программного типа	
	СПО	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	ППО	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Сетевое ПО	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Объекты воздействия BIOS/UEFI	
	Микропрограммное и аппаратное обеспечение BIOS/UEFI	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	Объекты воздействия АСУ ТП и технологического оборудования	
	ПО АСУ ТП	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)
	ПЛК	НСД к защищаемой информации (техническая и конфигурационная информация, аутентификационные данные и т.д.)

4.4 Формирование общего перечня нарушителей

Исходя из состава информации, обрабатываемой в ОКИИ, а также выполняемых с использованием ОКИИ процессов и реализуемых ОКИИ функций, используемых технологий обработки информации, архитектуры, технических особенностей ОКИИ проведена оценка возможных целей реализации нарушителями угроз безопасности информации, определены виды нарушителей, актуальных для ОКИИ. Результаты оценки представлены в Таблица 4.5.

Таблица 4.5 – Оценка актуальности видов нарушителей

Вид нарушителя	Категория нарушителя	Уровень возможностей нарушителя[1]	Актуальность нарушителя
Специальные службы иностранных государств	Внешний	Н4	Неактуален
Террористические, экстремистские группировки	Внешний	Н3	Актуален
Преступные группы (криминальные структуры)	Внешний	Н2	Актуален
Отдельные физические лица (хакеры)	Внешний	Н1	Актуален
Конкурирующие организации	Внешний	Н2	Актуален

[1] Уровень возможностей нарушителя (потенциал) определяется в соответствии с Методическим документом «Методика оценки угроз безопасности информации», утв. ФСТЭК России 05.02.2021, согласно которому «Н1» – нарушитель, обладающий базовыми возможностями, «Н2» – нарушитель, обладающий базовыми повышенными возможностями, «Н3» – нарушитель, обладающий средними возможностями, «Н4» – нарушитель, обладающий высокими возможностями.

Вид нарушителя	Категория нарушителя	Уровень возможностей нарушителя[1]	Актуальность нарушителя
Разработчики программных, программно-аппаратных средств	Внутренний	Н3	Актуален
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1	Актуален
Поставщики услуг связи, вычислительных услуг	Внутренний	Н2	Актуален
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2	Актуален
Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1	Актуален
Авторизованные пользователи систем и сетей	Внутренний	Н1	Актуален
Системные администраторы и администраторы безопасности	Внутренний	Н2	Актуален
Бывшие (уволенные) работники (пользователи)	Внешний	Н1	Актуален

Перечень видов нарушителей ИБ, исключенных из рассмотрения, с обоснованием такого исключения представлен в Таблица 4.6.

Таблица 4.6 – Обоснование исключения из рассмотрения части потенциальных видов нарушителей

Вид нарушителя	Обоснование исключения вида нарушителя из рассмотрения
Специальные службы иностранных государств (блоков государств)	ОКИИ не является государственной информационной системой и не используется для обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для специальных служб иностранных государств

Возможные цели реализации угроз безопасности информации нарушителями ИБ, рассматриваемых в качестве актуальных для ОКИИ, представлены в Таблица 4.7.

Таблица 4.7 – Возможные цели реализации угроз безопасности информации нарушителями ИБ

Вид нарушителя	Возможные цели реализации угроз безопасности
Террористические, экстремистские группировки	— Совершение террористических актов, угроза жизни граждан. — Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. — Дестабилизация общества. — Дестабилизация деятельности органов государственной власти, организаций
Преступные группы (криминальные структуры)	— Получение финансовой или иной материальной выгоды. — Желание самореализации (подтверждение статуса)

Вид нарушителя	Возможные цели реализации угроз безопасности
Отдельные физические лица (хакеры)	— Получение финансовой или иной материальной выгоды. — Любопытство или желание самореализации (подтверждение статуса)
Конкурирующие организации	— Получение конкурентных преимуществ. — Получение финансовой или иной материальной выгоды
Разработчики программных, программно-аппаратных средств	— Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. — Получение конкурентных преимуществ. — Получение финансовой или иной материальной выгоды. — Непреднамеренные, неосторожные или неквалифицированные действия
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	— Получение финансовой или иной материальной выгоды. — Непреднамеренные, неосторожные или неквалифицированные действия. — Получение конкурентных преимуществ
Поставщики услуг связи, вычислительных услуг	— Получение финансовой или иной материальной выгоды. — Непреднамеренные, неосторожные или неквалифицированные действия. — Получение конкурентных преимуществ
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	— Получение финансовой или иной материальной выгоды. — Непреднамеренные, неосторожные или неквалифицированные действия. — Получение конкурентных преимуществ
Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	— Получение финансовой или иной материальной выгоды. — Непреднамеренные, неосторожные или неквалифицированные действия
Авторизованные пользователи систем и сетей	— Получение финансовой или иной материальной выгоды. — Любопытство или желание самореализации (подтверждение статуса). — Месть за ранее совершенные действия. — Непреднамеренные, неосторожные или неквалифицированные действия
Системные администраторы и администраторы безопасности	— Получение финансовой или иной материальной выгоды. — Любопытство или желание самореализации (подтверждение статуса). — Месть за ранее совершенные действия. — Непреднамеренные, неосторожные или неквалифицированные действия
Бывшие (уволенные) работники (пользователи)	— Получение финансовой или иной материальной выгоды. — Месть за ранее совершенные действия

4.5 Определение актуальных нарушителей при реализации угроз безопасности информации

По результатам определения перечня видов потенциальных нарушителей безопасности информации и возможных целей реализации ими угроз безопасности информации, проведено соответствие целей реализации угроз безопасности информации видам риска (ущерба) и возможных негативных последствий, результаты которого представлены в Таблица 4.8.

Описание уровней возможностей актуальных нарушителей по реализации угроз безопасности информации представлено в Таблица 4.9.

Таблица 4.8 – Соответствие целей реализации нарушителями угроз безопасности информации и возможных негативных последствий и видов ущерба от их реализации

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Террористические, экстремистские группировки	+ (совершение террористических актов, угроза жизни граждан)	-	+ (совершение террористических актов, угроза жизни граждан/ дестабилизация деятельности органов государственной власти, организаций)	У1 (угроза жизни и здоровью) У3 (причинение ущерба жизни и здоровью людей /появление негативных публикаций в общедоступных источниках)
Преступные группы (криминальные структуры)	-	+ (получение финансовой или иной материальной выгоды)	+ (желание самореализации)	У2 (недополучение ожидаемой прибыли/ необходимость дополнительных затрат/ нарушение штатного режима функционирования ОКИИ/ причинение имущественного ущерба/ невозможность решения задач (реализации функций) или снижение эффективности решения задач) У3 (Причинение ущерба жизни и здоровью людей/ появление негативных публикаций в общедоступных источниках/ доступ к системам и сетям с целью незаконного использования вычислительных мощностей/ утечка информации ограниченного доступа)

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Отдельные физические лица (хакеры)	+ (любопытство или желание самореализации)	+ (получение финансовой или иной материальной выгоды)	-	У1 (угроза жизни или здоровью) У2 (недополучение ожидаемой прибыли / необходимость дополнительных затрат / нарушение штатного режима функционирования АСУ и управляемого объекта или процесса / причинение имущественного ущерба / невозможность решения задач (реализации функций) или снижение эффективности решения задач)
Конкурирующие организации	-	+ (получение конкурентных преимуществ / получение финансовой или иной материальной выгоды)	-	У2 (недополучение ожидаемой прибыли/ необходимость дополнительных затрат/ причинение имущественного ущерба/ потеря конкурентного преимущества/ невозможность заключения договоров, соглашений/ нарушение деловой репутации/ снижение престижа/ утрата доверия/ неспособность выполнения договорных обязательств/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)
Разработчики программных, программно-аппаратных средств	-	+ (внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки/ непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (необходимость дополнительных затрат/ нарушение штатного режима функционирования ОКИИ/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	+ (непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (необходимость дополнительных затрат/ нарушение штатного режима функционирования ОКИИ/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)
Поставщики услуг связи, вычислительных услуг	-	+ (непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (нарушение штатного режима функционирования ОКИИ/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	-	+ (непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (нарушение штатного режима функционирования ОКИИ/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)
Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	-	+ (любопытство или желание самореализации/ непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (нарушение штатного режима функционирования ОКИИ/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Авторизованные пользователи систем и сетей	+ (любопытство или желание самореализации / месть за ранее совершенные действия / непреднамеренные, неосторожные или неквалифицированные действия)	+ (любопытство или желание самореализации / месть за ранее совершенные действия / непреднамеренные, неосторожные или неквалифицированные действия)	-	У1 (угроза жизни или здоровью) У2 (недополучение ожидаемой прибыли/ необходимость дополнительных затрат/ нарушение штатного режима функционирования ОКИИ/ причинение имущественного ущерба/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)
Системные администраторы и администраторы безопасности	+ (непреднамеренные, неосторожные или неквалифицированные действия)	+ (непреднамеренные, неосторожные или неквалифицированные действия)	+ (любопытство или желание самореализации)	У1 (угроза жизни или здоровью) У2 (недополучение ожидаемой прибыли/ необходимость дополнительных затрат/ нарушение штатного режима функционирования ОКИИ/ причинение имущественного ущерба/ невозможность решения задач (реализации функций) или снижение эффективности решения задач) У3 (причинение ущерба жизни и здоровью людей/ нарушение штатного режима функционирования ОКИИ/ появление негативных публикаций в общедоступных источниках/ доступ к системам и сетям с целью незаконного использования вычислительных мощностей/ утечка информации ограниченного доступа)

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Бывшие (уволенные) работники (пользователи)	-	+ (получение финансовой или иной материальной выгоды / месть за ранее совершенные действия)	-	У2 (недополучение ожидаемой прибыли / необходимость дополнительных затрат / причинение имущественного ущерба/ потеря конкурентного преимущества/ невозможность заключения договоров, соглашений / нарушение деловой репутации/ снижение престижа/утрата доверия/ неспособность выполнения договорных обязательств/ невозможность решения задач (реализации функций) или снижение эффективности решения задач)

Таблица 4.9 – Уровни возможностей актуальных нарушителей

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного ПО, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на ТС обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов	— Физическое лицо (хакер) — Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем — Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) — Авторизованные пользователи систем и сетей — Бывшие работники (пользователи)

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н2	Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, ОС, а также имеет знания защитных механизмов, применяемых в ПО, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	— Преступные группы (два лица и более, действующие по единому плану) — Конкурирующие организации — Поставщики вычислительных услуг, услуг связи — Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ — Системные администраторы и администраторы безопасности
Н3	Нарушитель, обладающий средними возможностями	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому ПО аппаратных платформ, системному и прикладному ПО, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, ОС, а также имеет глубокое понимание защитных механизмов, применяемых в ПО, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	— Террористические, экстремистские группировки — Разработчики программных, программно-аппаратных средств

Результаты определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности представлены в Таблица 4.10.

Таблица 4.10 – Результаты определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности

Виды риска (ущерба) и возможные негативные последствия	**Виды актуального нарушителя**	**Категория нарушителя**	**Уровень возможностей нарушителя**
У1: Угроза жизни или здоровью	Террористические, экстремистские группировки	Внешний	Н3
	Отдельные физические лица (хакеры)	Внешний	Н1
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У2: Недополучение ожидаемой (прогнозируемой) прибыли	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Конкурирующие организации	Внешний	Н2
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У2: Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка ПО, ТС, вышедших из строя, замена, настройка, ремонт указанных средств)	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Конкурирующие организации	Внешний	Н2
	Разработчики программных, программно-аппаратных средств	Внутренний	Н3
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Нарушение штатного режима функционирования ОКИИ	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Разработчики программных, программно-аппаратных средств	Внутренний	Н3

Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
	Поставщики услуг связи, вычислительных услуг	Внутренний	Н2
	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У2: Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Конкурирующие организации	Внешний	Н2
	Разработчики программных, программно-аппаратных средств	Внутренний	Н3
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Потеря конкурентного преимущества	Конкурирующие организации	Внешний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Невозможность заключения договоров, соглашений	Конкурирующие организации	Внешний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Нарушение деловой репутации	Конкурирующие организации	Внешний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1

Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
У2: Снижение престижа	Конкурирующие организации	Внешний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Утрата доверия	Конкурирующие организации	Внешний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Причинение имущественного ущерба	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Конкурирующие организации	Внешний	Н2
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Неспособность выполнения договорных обязательств	Конкурирующие организации	Внешний	Н2
	Бывшие (уволенные) работники (пользователи)	Внешний	Н1
У2: Невозможность решения задач (реализации функций) или снижение эффективности решения задач	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Разработчики программных, программно-аппаратных средств	Внутренний	Н3
	Поставщики услуг связи, вычислительных услуг	Внутренний	Н2
	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У2: Невозможность решения задач (реализации функций) или снижение эффективности	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Разработчики программных, программно-аппаратных средств	Внутренний	Н3

Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
решения задач	Поставщики услуг связи, вычислительных услуг	Внутренний	Н2
	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У3: Причинение ущерба жизни и здоровью людей	Террористические, экстремистские группировки	Внешний	Н3
	Преступные группы (криминальные структуры)	Внешний	Н2
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У3: Нарушение штатного режима функционирования АСУ и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов	Преступные группы (криминальные структуры)	Внешний	Н2
	Отдельные физические лица (хакеры)	Внешний	Н1
	Разработчики программных, программно-аппаратных средств	Внутренний	Н3
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
	Поставщики услуг связи, вычислительных услуг	Внутренний	Н2
	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
	Авторизованные пользователи систем и сетей	Внутренний	Н1
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У3; Появление негативных публикаций в общедоступных	Террористические, экстремистские группировки	Внешний	Н3
	Преступные группы (криминальные структуры)	Внешний	Н2

Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
источниках	Системные администраторы и администраторы безопасности	Внутренний	Н2
У3: Доступ к системам и сетям с целью незаконного использования вычислительных мощностей	Преступные группы (криминальные структуры)	Внешний	Н2
	Системные администраторы и администраторы безопасности	Внутренний	Н2
У3: Утечка информации ограниченного доступа	Преступные группы (криминальные структуры)	Внешний	Н2
	Системные администраторы и администраторы безопасности	Внутренний	Н2

Для ОКИИ актуальными признаны виды нарушителей, обладающие базовыми возможностями (Н1), базовыми повышенными возможностями (Н2) и средними возможностями (Н3).

4.6 Способы реализации (возникновения) угроз безопасности информации в ОКИИ

С учетом предполагаемой архитектуры и условий функционирования ОКИИ проведена оценка возможности доступа нарушителей к следующим типам интерфейсов объектов воздействия:

– сетевые интерфейсы, обеспечивающие взаимодействие с смежными (взаимодействующими) системами и сетями (проводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

– внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами ОКИИ, имеющими внешние сетевые интерфейсы (проводные);

– интерфейсы для пользователей (проводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

– интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;

– интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов ОКИИ;

– возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам ОКИИ.

Результаты оценки возможных способов реализации угроз безопасности информации представлены в документе «Модель угроз и нарушителей безопасности информации объектов критической информационной инфраструктуры» (НКНХ.5273-ПД-ИБ-ИД1).

4.7 Актуальные угрозы безопасности информации в ОКИИ

В качестве исходных данных об угрозах безопасности информации и их характеристиках используется банк данных угроз безопасности информации, сформированный и поддерживаемый ФСТЭК России (http://bdu.fstec.ru/threat).

Экспертной группой были рассмотрены все угрозы безопасности информации, описанные в банке данных угроз, которые могут быть реализованы внешним и внутренним нарушителями с низким потенциалом (обладающими базовыми и базовыми повышенными возможностями), а также внутренним нарушителем со средним потенциалом, которые могут быть реализованы в отношении объектов воздействия, свойственных для ОКИИ, и которые могут быть реализованы в отношении ОКИИ с учетом ее структурно-функциональных характеристик и особенностей функционирования.

Актуальность угроз безопасности информации определяется в отношении угроз, для которых экспертным методом определено, что:

– возможности (потенциал) нарушителя достаточны для реализации угрозы безопасности информации;

– структурно-функциональные характеристики и особенности функционирования ОКИИ не исключают возможности применения техник и тактик, необходимых для реализации угрозы безопасности информации (существует сценарий реализации угрозы безопасности).

Рассмотренные сценарии реализации угрозы безопасности (комбинации возможных тактик и техник, которые могут применяться нарушителями для реализации угроз безопасности) и результаты оценки актуальности угроз безопасности информации для ОКИИ представлены в моделях угроз и нарушителей безопасности информации.

По результатам моделирования угроз безопасности информации при ее обработке в ОКИИ были выявлены следующие актуальные угрозы:

– УБИ.004 Угроза аппаратного сброса пароля BIOS.

– УБИ.006 Угроза внедрения кода или данных.

– УБИ.007 Угроза воздействия на программы с высокими привилегиями.

– УБИ.008 Угроза восстановления аутентификационной информации.

– УБИ.012 Угроза деструктивного изменения конфигурации/среды окружения программ.

– УБИ.013 Угроза деструктивного использования декларированного функционала BIOS.

– УБИ.014 Угроза длительного удержания вычислительных ресурсов пользователями.

– УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути.

– УБИ.018 Угроза загрузки нештатной операционной системы.

– УБИ.022 Угроза избыточного выделения оперативной памяти.

– УБИ.023 Угроза изменения компонентов системы.

– УБИ.025 Угроза изменения системных и глобальных переменных.

– УБИ.028 Угроза использования альтернативных путей доступа к ресурсам.

– УБИ.030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию.

– УБИ.031 Угроза использования механизмов авторизации для повышения привилегий.

– УБИ.033 Угроза использования слабостей кодирования входных данных.

– УБИ.034 Угроза использования слабостей протоколов сетевого/локального обмена данными.

– УБИ.036 Угроза исследования механизмов работы программы.

– УБИ.045 Угроза нарушения изоляции среды исполнения BIOS.

– УБИ.053 Угроза невозможности управления правами пользователей BIOS.

– УБИ.063 Угроза некорректного использования функционала программного и аппаратного обеспечения.

– УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией.

– УБИ.068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.

– УБИ.069 Угроза неправомерных действий в каналах связи.

– УБИ.072 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.

– УБИ.073 Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.

– УБИ.074 Угроза несанкционированного доступа к аутентификационной информации.

– УБИ.084 Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети.

– УБИ.086 Угроза несанкционированного изменения аутентификационной информации.

– УБИ.087 Угроза несанкционированного использования привилегированных функций BIOS.

– УБИ.088 Угроза несанкционированного копирования защищаемой информации.

– УБИ.089 Угроза несанкционированного редактирования реестра.

– УБИ.090 Угроза несанкционированного создания учетной записи пользователя.

– УБИ.091 Угроза несанкционированного удаления защищаемой информации.

– УБИ.093 Угроза несанкционированного управления буфером.

– УБИ.094 Угроза несанкционированного управления синхронизацией и состоянием.

– УБИ.095 Угроза несанкционированного управления указателями.

– УБИ.098 Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.

– УБИ.099 Угроза обнаружения хостов.

– УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации

– УБИ.102 Угроза опосредованного управления группой программ через совместно используемые данные.

– УБИ.103 Угроза определения типов объектов защиты.

– УБИ.104 Угроза определения топологии вычислительной сети.

– УБИ.109 Угроза перебора всех настроек и параметров приложения.

– УБИ.111 Угроза передачи данных по скрытым каналам.

– УБИ.114 Угроза переполнения целочисленных переменных.

– УБИ.115 Угроза перехвата вводимой и выводимой на периферийные устройства информации.

– УБИ.116 Угроза перехвата данных, передаваемых по вычислительной сети.

– УБИ.121 Угроза повреждения системного реестра.

– УБИ.122 Угроза повышения привилегий.

– УБИ.123 Угроза подбора пароля BIOS.

– УБИ.124 Угроза подделки записей журнала регистрации событий.

– УБИ.127 Угроза подмены действия пользователя путем обмана.

– УБИ.128 Угроза подмены доверенного пользователя.

– УБИ.129 Угроза подмены резервной копии программного обеспечения BIOS.

– УБИ.132 Угроза получения предварительной информации об объекте защиты.

– УБИ.139 Угроза преодоления физической защиты.

– УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании».

– УБИ.143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.

– УБИ.144 Угроза программного сброса пароля BIOS.

– УБИ.145 Угроза пропуска проверки целостности программного обеспечения.

– УБИ.149 Угроза сбоя обработки специальным образом измененных файлов.

– УБИ.152 Угроза удаления аутентификационной информации.

– УБИ.153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.

– УБИ.155 Угроза утраты вычислительных ресурсов.

– УБИ.156 Угроза утраты носителей информации.

– УБИ.157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.

– УБИ.160 Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.

– УБИ.163 Угроза перехвата исключения/сигнала из привилегированного блока функций.

– УБИ.166 Угроза внедрения системной избыточности.

– УБИ.170 Угроза неправомерного шифрования информации.

– УБИ.177 Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью.

– УБИ.178 Угроза несанкционированного использования системных и сетевых утилит.

– УБИ.179 Угроза несанкционированной модификации защищаемой информации.

– УБИ.182 Угроза физического устаревания аппаратных компонентов.

– УБИ.183 Угроза перехвата управления автоматизированной системой управления технологическими процессами.

– УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации.

– УБИ.187 Угроза несанкционированного воздействия на средство защиты информации.

– УБИ.189 Угроза маскирования действий вредоносного кода.

– УБИ.191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

– УБИ.192 Угроза использования уязвимых версий программного обеспечения.

– УБИ.198 Угроза скрытной регистрации вредоносной программой учетных записей администраторов.

– УБИ.204 Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров.

– УБИ.208 Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники.

– УБИ.214 Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации.

– УБИ.215 Угроза несанкционированного доступа к системе при помощи сторонних сервисов.

– УБИ.217 Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.

5 КЛАСС ЗАЩИЩЕННОСТИ / КАТЕГОРИЯ ЗНАЧИМОСТИ ОКИИ

5.1 Результаты категорирования ОКИИ

Отнесение объектов к ЗОКИИ и их категорирование проводится согласно Постановлению Правительства Российской Федерации от 08.02.2018 г. № 127 (ПП № 127) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Была проведена оценка применимости показатели критериев значимости с учетом специфики функционирования ОКИИ, автоматизированных процессов, процессов и характера деятельности субъекта КИИ и выделены применимые к ОКИИ показатели. Результаты оценки представлены в Таблица 5.1.

Таблица 5.1 – Перечень применимых для ОКИИ показателей критериев значимости в соответствии с ПП № 127

№	Показатель	Значение III категории	Значение II категории	Значение I категории
III. Экономическая значимость				
9	Возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)	более 0,0003, но менее или равно 0,0006	более 0,0006, но менее или равно 0,001	более 0,001

Вследствие реализации угроз информационной безопасности и компьютерных атак потенциальный ущерб от простоя или нарушения функционирования ОКИИ не приводит к снижению налоговых отчислений в размере, превышающем 0,0003%. Таким образом, ни по одному из показателей значимости ОКИИ АСУТП, АСПЗ, ЛСО, СПС, КИТСО не имеют признаков значимых ОКИИ.

В соответствии с Приказом ФСТЭК № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» оценивается степень возможного ущерба от нарушения целостности (неправомерные уничтожение или модифицирование), конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), доступности (неправомерное блокирование) информации, обрабатываемой в АСУ.

Для всех ОКИИ степень возможного ущерба от нарушения целостности, конфиденциальности, доступности низкая – в результате нарушения целостности

информации возможны незначительные негативные последствия локального характера. Уровень значимости информации, обрабатываемой в ОКИИ, – третий.

Защищаемые ОКИИ классифицируются как АСУ третьего класса защищенности.

6 ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

6.1 Общий состав групп мер по ИБ

Для обеспечения защиты информации создается СОИБ ОКИИ должна реализовать следующие группы мер (согласно Приказа ФСТЭК России от 14.03.2014 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»):

- Идентификация и аутентификация (ИАФ);
- Управление доступом (УПД);
- Защита машинных носителей информации (ЗНИ);
- Аудит безопасности (АУД);
- Антивирусная защита (АВЗ);
- Предотвращение вторжений (компьютерных атак) (СОВ);
- Обеспечение целостности (ОЦЛ);
- Обеспечение доступности (ОДТ);
- Защита технических средств и систем (ЗТС);
- Защита информационной системы и ее компонентов (ЗИС);
- Планирование мероприятий по обеспечению безопасности (ПЛН);
- Управление конфигурацией (УКФ);
- Управление обновлениями программного обеспечения (ОПО);
- Реагирование на компьютерные инциденты (ИНЦ);
- Обеспечение действий в нештатных ситуациях (ДНС);
- Информирование и обучение персонала (ИПО).

Состав организационно-технических мер защиты информации, необходимый для нейтрализации актуальных угроз, для защищаемых ЗОКИИ, АСУ представлен в Таблица 6.1.

Таблица 6.1 – Организационно-технические меры по защите ОКИИ

№ п/п	Идентификатор меры	Организационно-техническая мера по защите информации	Приказ ФСТЭК №31 (3 класс)
1	Идентификация и аутентификация (ИАФ)		
1.1	ИАФ.0	Разработка политики идентификации и аутентификации	+
1.2	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+

№ п/п	Идентификатор меры	Организационно-техническая мера по защите информации	Приказ ФСТЭК №31 (3 класс)
1.3	ИАФ.2	Идентификация и аутентификация устройств	+
1.4	ИАФ.3	Управление идентификаторами	+
1.5	ИАФ.4	Управление средствами аутентификации	+
1.6	ИАФ.5	Идентификация и аутентификация внешних пользователей	+
1.7	ИАФ.6	Двусторонняя аутентификация	-
1.8	ИАФ.7	Защита аутентификационной информации при передаче	+
2	Управление доступом (УПД)		
2.1	УПД.0	Разработка политики управления доступом	+
2.2	УПД.1	Управление учетными записями пользователей	+
2.3	УПД.2	Реализация политик управления доступом	+
2.4	УПД.4	Разделение полномочий (ролей) пользователей	+
2.5	УПД.5	Назначение минимально необходимых прав и привилегий	+
2.6	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+
2.7	УПД.9	Ограничение числа параллельных сеансов доступа	-
2.8	УПД.10	Блокирование сеанса доступа пользователя при неактивности	+
2.9	УПД.11	Управление действиями пользователей до идентификации и аутентификации	+
2.10	УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+
3	Защита машинных носителей информации (ЗНИ)		
3.1	ЗНИ.0	Разработка политики защиты машинных носителей информации	+
3.2	ЗНИ.1	Учет машинных носителей информации	+
3.3	ЗНИ.2	Управление физическим доступом к машинным носителям информации	+
3.4	ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	-
3.5	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+
3.6	ЗНИ.7	Контроль подключения машинных носителей информации	+
3.7	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+
4	Аудит безопасности (АУД)		
4.1	АУД.0	Разработка политики аудита безопасности	+
4.2	АУД.1	Инвентаризация информационных ресурсов	+
4.3	АУД.2	Анализ уязвимостей и их устранение	+
4.4	АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+
4.5	АУД.4	Регистрация событий безопасности	+
4.6	АУД.5	Контроль и анализ сетевого трафика	-
4.7	АУД.6	Защита информации о событиях безопасности	+
4.8	АУД.7	Мониторинг безопасности	+
4.9	АУД.8	Реагирование на сбои при регистрации событий безопасности	+
4.10	АУД.9	Анализ действий пользователей	-
4.11	АУД.10	Проведение внутренних аудитов	+

№ п/п	Идентификатор меры	Организационно-техническая мера по защите информации	Приказ ФСТЭК №31 (3 класс)
5	Антивирусная защита (АВЗ)		
5.1	АВЗ.0	Разработка политики антивирусной защиты	+
5.2	АВЗ.1	Реализация антивирусной защиты	+
5.3	АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+
5.4	АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	-
5.5	АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+
6	Предотвращение вторжений (компьютерных атак) (СОВ)		
6.1	СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)	-
6.2	СОВ.1	Обнаружение и предотвращение компьютерных атак	-
6.3	СОВ.2	Обновление базы решающих правил	-
7	Обеспечение целостности (ОЦЛ)		
7.1	ОЦЛ.0	Разработка политики обеспечения целостности	+
7.2	ОЦЛ.1	Контроль целостности программного обеспечения	+
7.3	ОЦЛ.2	Контроль целостности информации	-
8	Обеспечение доступности (ОДТ)		
8.1	ОДТ.0	Разработка политики обеспечения доступности	+
8.2	ОДТ.4	Резервное копирование информации	+
8.3	ОДТ.5	Обеспечение возможности восстановления информации	+
8.4	ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+
8.5	ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+
9	Защита технических средств и систем (ЗТС)		
9.1	ЗТС.0	Разработка политики защиты технических средств и систем	+
9.2	ЗТС.2	Организация контролируемой зоны	+
9.3	ЗТС.3	Управление физическим доступом	+
9.4	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+
9.5	ЗТС.5	Защита от внешних воздействий	+
10	Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)		
10.1	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+
10.2	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+
10.3	ЗИС.2	Защита периметра информационной (автоматизированной) системы	+
10.4	ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+
10.5	ЗИС.4	Сегментирование информационной (автоматизированной) системы	-
10.6	ЗИС.5	Организация демилитаризованной зоны	+
10.7	ЗИС.6	Управление сетевыми потоками	-

№ п/п	Идентификатор меры	Организационно-техническая мера по защите информации	Приказ ФСТЭК №31 (3 класс)
10.8	ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+
10.9	ЗИС.19	Защита информации при ее передаче по каналам связи	+
10.1	ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+
10.1	ЗИС.35	Управление сетевыми соединениями	-
10.1	ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+
11	Реагирование на компьютерные инциденты (ИНЦ)		
11.1	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+
11.2	ИНЦ.1	Выявление компьютерных инцидентов	+
11.3	ИНЦ.2	Информирование о компьютерных инцидентах	+
11.4	ИНЦ.3	Анализ компьютерных инцидентов	+
11.5	ИНЦ.4	Устранение последствий компьютерных инцидентов	+
11.6	ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+
11.7	ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	-
12	Управление конфигурацией (УКФ)		
12.1	УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	+
12.2	УКФ.2	Управление изменениями	+
12.3	УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+
13	Управление обновлениями программного обеспечения (ОПО)		
13.1	ОПО.0	Разработка политики управления обновлениями программного обеспечения	+
13.2	ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+
13.3	ОПО.2	Контроль целостности обновлений программного обеспечения	+
13.4	ОПО.3	Тестирование обновлений программного обеспечения	+
13.5	ОПО.4	Установка обновлений программного обеспечения	+
14	Планирование мероприятий по обеспечению безопасности (ПЛН)		
14.1	ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+
14.2	ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+
14.3	ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+
15	Обеспечение действий в нештатных ситуациях (ДНС)		
15.1	ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+
15.2	ДНС.1	Разработка плана действий в нештатных ситуациях	+
15.3	ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+
15.4	ДНС.4	Резервирование программного обеспечения, ТС, каналов связи на случай возникновения нештатных ситуаций	-
15.5	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения	+

№ п/п	Идентификатор меры	Организационно-техническая мера по защите информации	Приказ ФСТЭК №31 (3 класс)
		нештатных ситуаций	
15.6	ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+
16	Информирование и обучение персонала (ИПО)		
16.1	ИПО.0	Разработка политики информирования и обучения персонала	+
16.2	ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+
16.3	ИПО.2	Обучение персонала правилам безопасной работы	+
16.4	ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+

В Таблица 6.2 приведено обоснование исключения части базовых мер защиты, требуемых для защиты 3 категории значимости ОКИИ, 3 класса защищенности АСУ.

Таблица 6.2 – Обоснование исключения мер из набора

Мера защиты	Обоснование исключения
ИАФ.5 Идентификация и аутентификация внешних пользователей	Удаленный доступ не используется (запрещен)
УПД.13 Реализация защищенного удаленного доступа	
УПД.14 Контроль доступа из внешних информационных (автоматизированных) систем	
АВЗ.2 Антивирусная защита электронной почты и иных сервисов	Сервисы электронной почты не используются
ОДТ.8 Контроль предоставляемых вычислительных ресурсов и каналов связи	Услуги поставщиков вычислительных ресурсов и каналов связи не используются
ЗИС.21 Запрет несанкционированной удаленной активации периферийных устройств	Периферийные устройства с возможностью удаленной активации не применяются
ЗИС.32 Защита беспроводных соединений	Беспроводные соединения не используются
ЗИС.38 Защита информации при использовании мобильных устройств	Мобильные устройства не используются
ЗИС.39 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Средства виртуализации на объекте Заказчика не используются

Перечень наложенных средств защиты, обеспечивающих реализацию указанных организационно-технических мер, представлен в Таблица 6.3.

Таблица 6.3 – Организационно-технические меры по защите ОКИИ

Актуальная угроза	Идентификаторы мер по митигации риска	Классы средств защиты информации, реализующие указанные меры
Угроза аппаратного сброса пароля BIOS (УБИ.004)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза внедрения кода или данных (УБИ.006)	ИАФ.1, ИАФ.6, УПД.4, УПД.5, АВЗ.1, АВЗ.2, АВЗ.3, АВЗ.4 ЗНИ.2, ЗНИ.5, ЗНИ.7	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности

Актуальная угроза	Идентификаторы мер по митигации риска	Классы средств защиты информации, реализующие указанные меры
Угроза воздействия на программы с высокими привилегиями (УБИ.007)	УПД.4, УПД.5, ИАФ.1, ИАФ.3 ИАФ.4, ИАФ.5	Средство защиты конечных точек; Средство защиты от НСД;
Угроза восстановления аутентификационной информации (УБИ.008)	ИАФ.0, ИАФ.4, УПД.6, АУД.4	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности
Угроза деструктивного изменения конфигурации/среды окружения программ (УБИ.012)	ИАФ.1, УПД.4, УПД.5, АУД.4; АУД.7; ОЦЛ.1; ОЦЛ.2	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности; Средство контроля конфигураций; Средство регистрации и обработки событий безопасности
Угроза деструктивного использования декларированного функционала BIOS (УБИ.013)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза длительного удержания вычислительных ресурсов пользователями (УБИ.014)	ИАФ.1, УПД.4, УПД.5, ОДТ.8	Средство защиты конечных точек; Средство регистрации и обработки событий безопасности
Угроза доступа к защищаемым файлам с использованием обходного пути (УБИ.015)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5	Межсетевой экран
Угроза загрузки нештатной операционной системы (УБИ.018)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5, ЗТС.2, ЗТС.3	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности
Угроза избыточного выделения оперативной памяти (УБИ.022)	АВЗ.1, АВЗ.4	Средство защиты конечных точек
Угроза изменения компонентов информационной (автоматизированной) системы (УБИ.023)	УПД.4, АУД.4, ЗНИ.5, ЗНИ.7, УКФ.0, УКФ.1, УКФ.2, УКФ.3	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности; Средство регистрации и обработки событий безопасности; Средство контроля конфигураций
Угроза изменения системных и глобальных переменных (УБИ.025)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5, ОЦЛ.1	Средство защиты конечных точек; Средство защиты от НСД; Средство регистрации и обработки событий безопасности; Средство контроля конфигураций
Угроза использования альтернативных путей доступа к ресурсам (УБИ.028)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5	Межсетевой экран
Угроза использования информации идентификации / аутентификации, заданной по умолчанию (УБИ.030)	ИАФ.0, ЗИС.8, АУД.2, АУД.10	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности; Средство регистрации и обработки событий безопасности
Угроза использования механизмов авторизации для повышения привилегий (УБИ.031)	УПД.4, УПД.5, ИАФ.1, ИАФ.3 ИАФ.4, ИАФ.5	Средство защиты конечных точек; Средство анализа защищенности
Угроза использования слабостей кодирования входных данных (УБИ.033)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.6, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11	Средство защиты конечных точек

Актуальная угроза	Идентификаторы мер по митигации риска	Классы средств защиты информации, реализующие указанные меры
Угроза использования слабостей протоколов сетевого / локального обмена данными (УБИ.034)	ОЦЛ.4	Средство защиты конечных точек; Средство анализа защищенности
Угроза исследования механизмов работы программы (УБИ.036)	ИАФ.1, УПД.5, УКФ.3, УПД.5	Средство защиты конечных точек; Межсетевой экран
Угроза нарушения изоляции среды исполнения BIOS (УБИ.045)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза невозможности управления правами пользователей BIOS (УБИ.053)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза некорректного использования функционала программного и аппаратного обеспечения (УБИ.063)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5, ОЦЛ.5	Средство защиты конечных точек; Средство защиты от НСД
Угроза неправомерного ознакомления с защищаемой информацией (УБИ.067)	ЗТС.0, ЗТС.4	Средство защиты конечных точек; Межсетевой экран; Средство криптографической защиты информации; Средство регистрации и обработки событий безопасности
Угроза неправомерного / некорректного использования интерфейса взаимодействия с приложением (УБИ.068)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5, АУД.2	Средство защиты конечных точек; Межсетевой экран; Средство регистрации и обработки событий безопасности
Угроза неправомерных действий в каналах связи (УБИ.069)	СОВ.1, СОВ.2, АУД.2, ЗИС.19, ЗИС.27	Межсетевой экран; Средство криптографической защиты информации
Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS (УБИ.072)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза несанкционированного доступа к аутентификационной информации (УБИ.074)	ИАФ.1, ИАФ.3, ИАФ.4, УПД.4, УПД.5, ЗНИ.5, ЗНИ.7, АВЗ.1	Средство защиты конечных точек; Межсетевой экран; Средство анализа защищенности
Угроза несанкционированного изменения аутентификационной информации (УБИ.086)	ИАФ.3, ИАФ.4, ИАФ.7, АВЗ.1	Средство защиты конечных точек; Средство анализа защищенности; Средство регистрации и обработки событий безопасности; Средство контроля конфигураций
Угроза несанкционированного использования привилегированных функций BIOS (УБИ.087)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза несанкционированного копирования защищаемой информации (УБИ.088)	ИАФ.1, ИАФ.3, ИАФ.4, УПД.5, ЗТС.2, ЗТС.3, ЗНИ.3	Средство защиты конечных точек; Межсетевой экран; Средство регистрации и обработки событий безопасности
Угроза несанкционированного редактирования реестра (УБИ.089)	ИАФ.1, ИАФ.3, ИАФ.4, УПД.4, УПД.5, ЗНИ.5, ЗНИ.7, АВЗ.1	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности; Средство контроля конфигураций

Актуальная угроза	Идентификаторы мер по митигации риска	Классы средств защиты информации, реализующие указанные меры
Угроза несанкционированного создания учетной записи пользователя (УБИ.090)	ИАФ.1, ИАФ.3, ИАФ.4, УПД.4. УПД.5, УКФ.3, АВЗ.1, АВЗ.4	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности; Средство регистрации и обработки событий безопасности; Средство контроля конфигураций
Угроза несанкционированного удаления защищаемой информации (УБИ.091)	ОЦЛ.1, ОЦЛ.2, ОДТ.4, ОДТ.5, ОДТ.6	Средство защиты конечных точек; Средство анализа защищенности; Средство резервного копирования; Средство контроля конфигураций
Угроза несанкционированного управления буфером (УБИ.093)	ИАФ.1, ИАФ.3, ИАФ.4, УПД.4. УПД.5, УКФ.3, АВЗ.1, АВЗ.4	Средство защиты конечных точек; Средство защиты от НСД
Угроза несанкционированного управления синхронизацией и состоянием (УБИ.094)	УПД.0, УПД.5, АУД.0, АУД.3	Средство защиты конечных точек; Средство анализа защищенности
Угроза несанкционированного управления указателями (УБИ.095)	ИАФ.1, ИАФ.4, УПД.4, УПД.5, ЗНИ.5, ЗНИ.7, АВЗ.1	Средство защиты конечных точек; Средство анализа защищенности
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб (УБИ.098)	СОВ.1, СОВ.2, ЗИС.2, АУД.2	Межсетевой экран; Средство анализа защищенности; Средство защиты от НСД
Угроза обнаружения хостов (УБИ.099)	ЗИС.2, ЗИС.4, СОВ.1, СОВ.2, АУД.2	Межсетевой экран; Средство анализа защищенности
Угроза обхода некорректно настроенных механизмов аутентификации (УБИ.100)	ИАФ.1, ИАФ.3, ИАФ.4, ОЦЛ.3, ОЦЛ.4	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности
Угроза опосредованного управления группой программ через совместно используемые данные (УБИ.102)	УПД.2, УПД.4, УПД.5, ОЦЛ.1	Средство защиты конечных точек; Средство защиты от НСД
Угроза определения типов объектов защиты (УБИ.103)	СОВ.1, СОВ.2, ЗИС.2, АУД.2	Средство защиты конечных точек; Межсетевой экран
Угроза определения топологии вычислительной сети (УБИ.104)	СОВ.1, СОВ.2, ЗИС.2, АУД.2	Межсетевой экран; Средство анализа защищенности
Угроза перебора всех настроек и параметров приложения (УБИ.109)	УКФ.0, УКФ.2, УКФ.3	Средство защиты конечных точек; Средство анализа защищенности
Угроза передачи данных по скрытым каналам (УБИ.111)	СОВ.1, СОВ.2, ЗИС.2, ЗИС.31	Средство защиты конечных точек; Межсетевой экран; Средство криптографической защиты информации
Угроза переполнения целочисленных переменных (УБИ.114)	УПД.4, УПД.5, АВЗ.1, АВЗ.4	Средство защиты конечных точек
Угроза перехвата вводимой и выводимой на периферийные устройства информации (УБИ.115)	УПД.4, УПД.5, АВЗ.1, АВЗ.4	Средство защиты конечных точек
Угроза перехвата данных, передаваемых по вычислительной сети (УБИ.116)	ЗТС.3, ЗИС.4, ЗИС.19	Средство криптографической защиты информации

Актуальная угроза	Идентификаторы мер по митигации риска	Классы средств защиты информации, реализующие указанные меры
Угроза повреждения системного реестра (УБИ.121)	ИАФ.1, ИАФ.3, ИАФ.4, УПД.4, УПД.5, ЗНИ.5, ЗНИ.7, АВЗ.1	Средство защиты конечных точек; Средство анализа защищенности; Средство контроля конфигураций
Угроза повышения привилегий (УБИ.122)	АВЗ.1, АВЗ.4, АУД.2, АУД.7, УПД.4, УПД.5	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности; Средство регистрации и обработки событий безопасности
Угроза подбора пароля BIOS (УБИ.123)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза подделки записей журнала регистрации событий (УБИ.124)	УПД.4, УПД.5, АУД.4, АУД.6, АУД.7, АУД.8, УКФ.3	Средство защиты конечных точек; Средство регистрации и обработки событий безопасности
Угроза подмены действия пользователя путем обмана (УБИ.127)	ИПО.0, ИПО.1, ИПО.2, ИПО.4	Средство защиты конечных точек; Средство защиты от НСД; Средство регистрации и обработки событий безопасности
Угроза подмены доверенного пользователя (УБИ.128)	СОВ.1, СОВ.2, ЗИС.27	Средство защиты конечных точек; Средство регистрации и обработки событий безопасности
Угроза подмены резервной копии программного обеспечения BIOS (УБИ.129)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза получения предварительной информации об объекте защиты (УБИ.132)	СОВ.1, СОВ.2, ЗИС.2	Средство защиты конечных точек; Межсетевой экран; Средство криптографической защиты информации; Средство анализа защищенности
Угроза преодоления физической защиты (УБИ.139)	ЗТС.2, ЗТС.3	Средство регистрации и обработки событий безопасности
Угроза приведения системы в состояние «отказ в обслуживании» (УБИ.140)	УПД.2, УПД.9, УПД.10, СОВ.1	Средство защиты конечных точек; Средство защиты от НСД; Межсетевой экран
Угроза программного выведения из строя средств хранения, обработки и (или) ввода / вывода / передачи информации (УБИ.143)	АВЗ.1, АВЗ.3	Средство защиты конечных точек; Средство защиты от НСД
Угроза программного сброса пароля BIOS (УБИ.144)	УПД.0, ЗНИ.0, ЗТС.0, ЗТС.2, ЗТС.3,	Организационные меры, управление доступом к оборудованию
Угроза пропуска проверки целостности программного обеспечения (УБИ.145)	УПД.2, УПД.5, АВЗ.1, АВЗ.2, ОЦЛ.4	Средство защиты конечных точек; Средство защиты от НСД; Средство анализа защищенности
Угроза сбоя обработки специальным образом измененных файлов (УБИ.149)	ОЦЛ.0, ОЦЛ.1, ЗИС.0, ЗИС.8	Средство защиты конечных точек; Средство защиты от НСД;
Угроза удаления аутентификационной информации (УБИ.152)	АВЗ.1, АВЗ.2, АВЗ.3	Средство защиты конечных точек; Средство контроля конфигураций
Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов (УБИ.153)	СОВ.1, СОВ.2, ЗИС.2, ЗИС.4, ЗИС.34	Средство защиты конечных точек; Средство защиты от НСД; Межсетевой экран

Актуальная угроза	Идентификаторы мер по митигации риска	Классы средств защиты информации, реализующие указанные меры
Угроза утраты вычислительных ресурсов (УБИ.155)	ЗИС.2, ЗИС.4	Средство защиты конечных точек; Средство защиты от НСД; Средство регистрации и обработки событий безопасности
Угроза утраты носителей информации (УБИ.156)	ЗНИ.1, ЗНИ.2, ОДТ.4, ОДТ.5	Средство защиты конечных точек; Средство защиты от НСД; Средство регистрации и обработки событий безопасности; Средство резервного копирования
Угроза физического выведения из строя средств хранения, обработки и (или) ввода / вывода / передачи информации (УБИ.157)	ЗТС.2, ЗТС.3, ОДТ.1, ОДТ.2, ОДТ.3, ОДТ.4, ОДТ.5, ОДТ.6	Средство регистрации и обработки событий безопасности; Средство резервного копирования
Угроза хищения средств хранения, обработки и (или) ввода / вывода / передачи информации (УБИ.160)	ЗНИ.1, ЗНИ.2, ЗНИ.3, ЗТС.2, ЗТС.3	Средство защиты конечных точек
Угроза перехвата исключения / сигнала из привилегированного блока функций (УБИ.163)	СОВ.1, ЗТС.2, ЗТС.5, ЗИС.6, ЗИС.19	Средство защиты конечных точек
Угроза внедрения системной избыточности (УБИ.166)	УКФ.3, АУД.10, ПЛН.2	Средство защиты конечных точек; Средство защиты от НСД; Средство регистрации и обработки событий безопасности
Угроза неправомерного шифрования информации (УБИ.170)	АВЗ.1, АВЗ.4, ОДТ.4, ОДТ.5, ОДТ.6	Средство защиты конечных точек; Средство резервного копирования
Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью (УБИ.177)	ИПО.0, ИПО.1, ИПО.2, ИПО.4	Средство регистрации и обработки событий безопасности
Угроза несанкционированного использования системных и сетевых утилит (УБИ.178)	УПД.4, УПД.5, УКФ.3	Межсетевой экран; Средство криптографической защиты информации; Средство анализа защищенности
Угроза несанкционированной модификации защищаемой информации (УБИ.179)	УПД.4, УПД.5, ЗТС.2, ЗТС.3, ЗНИ.2, ОЦЛ.1, ОЦЛ.2, ОДТ.4, ОДТ.5, ОДТ.6	Средство защиты конечных точек; Средство защиты от НСД; Средство резервного копирования; Средство контроля конфигураций
Угроза физического устаревания аппаратных компонентов (УБИ.182)	ЗТС.5	Средство регистрации и обработки событий безопасности
Угроза перехвата управления автоматизированной системой управления технологическими процессами (УБИ.183)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5, АУД.2, АУД.7, СОВ.1, СОВ.2, АВЗ.1, АВЗ.2, АВЗ.4	Средство защиты конечных точек; Средство защиты от НСД
Угроза несанкционированного изменения параметров настройки средств защиты информации (УБИ.185)	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.4, УПД.5	Средство регистрации и обработки событий безопасности; Средство контроля конфигураций

Актуальная угроза	Идентификаторы мер по митигации риска	Классы средств защиты информации, реализующие указанные меры
Угроза несанкционированного воздействия на средство защиты информации (УБИ.187)	УПД.4, УПД.5, ЗИС.1	Средство анализа защищенности; Средство регистрации и обработки событий безопасности
Угроза маскирования действий вредоносного кода (УБИ.189)	АУД.1, АУД.2, ОПО.3, ОПО.4, АВЗ.1, АВЗ.3, АВЗ.4	Средство защиты конечных точек; Средство регистрации и обработки событий безопасности
Угроза внедрения вредоносного кода в дистрибутив программного обеспечения (УБИ.191)	АВЗ.1, АВЗ.4, УКФ.3	Средство защиты конечных точек; Средство анализа защищенности; Средство регистрации и обработки событий безопасности
Угроза использования уязвимых версий программного обеспечения (УБИ.192)	АУД.1, АУД.2, ОПО.3, ОПО.4	Средство защиты конечных точек; Средство анализа защищенности
Угроза скрытной регистрации вредоносной программой учетных записей администраторов (УБИ.198)	УПД.4, УПД.5, АВЗ.1, АВЗ.4	Средство защиты конечных точек; Средство анализа защищенности; Средство регистрации и обработки событий безопасности
Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров (УБИ.204)	АВЗ.1, АВЗ.2, СОВ.1, СОВ.2	Средство защиты конечных точек
Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники (УБИ.208)	АВЗ.1, АВЗ.4, УКФ.3	Средство защиты конечных точек; Средство защиты от НСД; Средство регистрации и обработки событий безопасности
Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации (УБИ.214)	АУД.1, АУД.2, АУД.3, АУД.4	Средство регистрации и обработки событий безопасности
Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения (УБИ.217)	АВЗ.1, АВЗ.4, ОПО.0, ОПО.2, ОПО.3	Средство регистрации и обработки событий безопасности

6.2 Требования к структуре и функционированию СОИБ ОКИИ

Программно-технические СрЗИ применяются в соответствии с принципами необходимости и достаточности для митигации актуальных угроз с учетом компонентного состава ОКИИ, наличии взаимодействия технологической сети с внешними ОКИИ и в соответствии с классом СрЗИ, требуемым действующими нормативными документами Российской Федерации для ЗОКИИ III категории. Средства защиты, требуемые для использования в рамках защищаемых ОКИИ, с указанием требуемого класса СрЗИ, указаны в Таблица 6.4.

Таблица 6.4 – Перечень средств защиты для реализации СОИБ ОКИИ

Средства защиты	Требуемый класс СрЗИ
Средство защиты от НСД	6 уровень доверия НДВ +
Средство защиты конечных точек	6 класс защиты +Тип А / Б / В 6 уровень доверия НДВ +
Средство контроля конфигураций	6 уровень доверия НДВ +
МЭ с функцией обнаружения вторжений	6 класс защиты +Тип Б 6 уровень доверия НДВ +
Средство криптографической защиты информации	6 класс защиты +Тип А 6 уровень доверия НДВ +
Средство анализа защищенности	6 уровень доверия НДВ +
Средство регистрации и обработки событий безопасности	6 уровень доверия НДВ +
Средство резервного копирования и восстановления данных	6 уровень доверия НДВ +

Средство защиты от НСД обеспечивает защиту хостов (АРМ, Серверов) на базе ОС семейства Windows.

Средство защиты конечных точек обеспечивает обнаружение вредоносных компьютерных программ и иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации СрЗИ, а также реагирования на обнаружение этих программ и информации на серверах и рабочих местах ОКИИ. Применяется специализированный программный комплекс для противодействия вредоносному ПО в технологических сетях.

Средство контроля конфигураций обеспечивает контроль конфигураций и топологии сети, контроль целостности и проверки соответствия хостов и конечных точек.

МЭ обеспечивают контроль и управление сетевыми потоками между различными сегментами технологической сети, включая функцию обнаружения вторжений со специфичными для технологических сетей сигнатурами на внешнем интерфейсе периметрового МЭ технологической сети / сегмента сети.

Средство криптографической защиты информации обеспечивает защиту каналов связи при передаче данных по вычислительной сети между объектами ПАО «Нижнекамскнефтехим».

Средство анализа защищенности обеспечивает проведение систематических мероприятий по анализу защищенности компонентов ОКИИ верхнего уровня (серверов, рабочих мест), компонентов обеспечивающей ИТ-инфраструктуры, в том числе серверов управления СрЗИ в составе СОИБ ОКИИ.

Средство регистрации и обработки событий безопасности обеспечивает сбор и корреляцию событий безопасности, поступающих как от СрЗИ в составе СОИБ ОКИИ, так и от компонентов ОКИИ верхнего уровня (при наличии технической возможности).

Средство резервного копирования и восстановления данных предназначено для создания образов операционных систем и прикладного ПО на АРМ и серверах защищаемых ОКИИ.

Требования к функционалу средств защиты информации представлены в документе НКНХ.5273-ПД-ИБ-ИД2 «Частное техническое задание на создание системы обеспечения информационной безопасности объектов критической информационной инфраструктуры ПАО «Нижнекамскнефтехим».

Взаимодействие между компонентами СОИБ ОКИИ и со смежными системами организуется с использованием имеющейся информационной инфраструктуры.

6.2.1 Требования к ТС, ПО и СрЗИ

Специальные требования к поставляемым ТС и ПО не предъявляются.

СрЗИ, применяемые для реализации технических мер защиты информации, должны выбираться из СрЗИ, прошедших оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки с учетом требований к классам средств защиты.

7 ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИБ

7.1 Состав подсистем СОИБ для реализации групп мер по ИБ

Перечень функциональных подсистем, посредством которых осуществляется реализация требований по защите информации, представлен в Таблица 7.1.

Таблица 7.1 – Перечень функциональных подсистем СОИБ ОКИИ

Наименование подсистемы СОИБ ОКИИ	СрЗИ СОИБ ОКИИ	Назначение подсистемы СОИБ ОКИИ	Реализуемые меры защиты
Подсистема защиты от НСД	Встроенные механизмы системного ПО. Средства защиты конечных точек, устанавливаемое на АРМ и серверы ОКИИ. Средства защиты от НСД.	Идентификация и аутентификация пользователей в ОС, защиты серверов, АРМ от НСД	ИАФ, УПД
Подсистема межсетевого экранирования и обнаружения вторжений	Средства межсетевого экранирования	Контроль и управление сетевыми потоками между различными сегментами ТСПД, различными АСУ	УПД, ЗИС, СОВ
Подсистема криптографической защиты	Средства криптографической защиты	Защита информации, передаваемой по каналам связи между объектами ПАО «Нижнекамскнефтехим»	УПД, ЗИС
Подсистема АВЗ	Средства защиты конечных точек, устанавливаемое на АРМ и серверы ОКИИ	Обнаружение компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации СЗИ, а также реагирование на обнаружение этих программ и информации	ЗНИ, АВЗ
Подсистема анализа защищенности	Средства анализа защищенности	Проведение систематических мероприятий по анализу защищенности ИС и тестированию работоспособности системы защиты информации	АУД, ПЛН
Подсистема регистрации и обработки событий безопасности	Средства регистрации и обработки событий безопасности, осуществляющее дистанционный сбор событий безопасности с АРМ и серверов ОКИИ	Подсистема предназначена для сбора и корреляции событий безопасности, поступающих от различных источников	УПД, ИНЦ, ПЛН

Наименование подсистемы СОИБ ОКИИ	СрЗИ СОИБ ОКИИ	Назначение подсистемы СОИБ ОКИИ	Реализуемые меры защиты
Подсистема резервного копирования	Средство резервного копирования и восстановления данных	Создание образов операционных систем и прикладного ПО на АРМ и серверах защищаемых ОКИИ, восстановление данных в случае потери	ОДТ, ДНС

Обеспечение защиты компонентов ОКИИ обеспечивается периметровым межсетевым экраном, а также клиентскими компонентами, разворачиваемыми на компонентах (АРМ, серверы). Управление клиентскими компонентами осуществляется из СОИБ ОКИИ.

7.2 Реализация мер по обеспечению требований безопасности ОКИИ

7.2.1 Идентификация и аутентификация (ИАФ)

Учетные данные, используемые в ОКИИ, должны создаваться в соответствии с требованиями к парольной политике учетных записей и обладать следующими функциональными характеристиками:

– длина пароля должна быть не менее 8 символов и состоять из цифр, букв и специальных символов;

– срок действия пароля должен быть ограничен 3 месяцами;

– повторное использование пароля должно быть запрещено;

– уведомление пользователя ОКИИ о необходимости смены пароля;

– блокировка УЗ после 5 неуспешных попыток доступа с вводом некорректного пароля;

– при смене пароля:

а) двойное подтверждение при самостоятельной смене пароля;

б) автоматический сброс поля ввода после каждой проверки введенного пароля;

– парольный ввод в ОКИИ должен осуществляться:

а) без отображения истинных символов в поле ввода;

б) с двойным подтверждением при самостоятельной смене;

в) со сбросом поля ввода после каждой проверки введенного пароля;

– пароли, создаваемые по умолчанию, в том числе к системным и служебным учетным записям, а также служебные коды доступа к контроллерам и оборудованию КИПиА должны быть изменены после инсталляции и настройки ОКИИ и/или монтажа оборудования перед запуском ОКИИ в эксплуатацию.

Для обеспечения мер безопасности ОКИИ должны выполняться:

– регламентация правил и процедур идентификации и аутентификации (ИАФ.0);

– идентификация и аутентификация пользователей и инициируемых ими процессов (ИАФ.1);

– идентификация и аутентификация устройств (ИАФ.2);

– управление идентификаторами (ИАФ.3);

– управление средствами аутентификации (ИАФ.4);

– идентификация и аутентификация внешних пользователей (ИАФ.5);

– двусторонняя аутентификация (ИАФ.6)

– защита аутентификационной информации при передаче (ИАФ.7).

7.2.2 Управление доступом (УПД)

Для управления доступом ОКИИ должны выполнять:

– регламентация правил и процедур управления доступом (УПД.0)

– управление учетными записями пользователей (УПД.1);

– реализацию политик управления доступом (УПД.2);

– разделение полномочий (ролей) пользователей (УПД.4);

– назначение минимально необходимых прав и привилегий (УПД.5);

– ограничение неуспешных попыток доступа к автоматизированной системе (УПД.6);

– ограничение числа параллельных сеансов доступа (УПД.9);

– блокирование сеанса доступа пользователя при неактивности (УПД.10);

– управление действиями пользователей до ИАФ (УПД.11);

– контроль доступа из внешних информационных (автоматизированных) систем (УПД.14).

Управление доступом, настройка минимально необходимых полномочий пользователей и сервисов (служб) для выполнения производственных задач осуществляется на уровнях доступа:

– уровень системного ПО ОКИИ (операционная система АРМ, серверов);

– уровень прикладного ПО (прикладное ПО SCADA).

Данные меры должны быть реализованы за счет использования встроенных в ОС, ППО механизмов защиты информации, а также средств защиты конечных точек/АВЗ, средств межсетевого экранирования.

При реализации доступа работников к компонентам ОКИИ необходимо наличие:

– возможности настройки минимально необходимых полномочий для решения производственных задач;

– возможности отключения всех дополнительных прав работников и функционала систем;

– возможности настройки права доступа на уровне модулей ППО ОКИИ;

– возможности настройки права доступа на уровне баз данных ОКИИ, при этом доступ работников к базам данных, используемых в ОКИИ, должен быть ограничен. Доступ к базам данных должен быть разрешен только администраторам ОКИИ и только при условии регистрации всех событий и действий работника в базе данных. Все действия, совершаемые работниками в базах данных, должны регистрироваться в журналах базах данных либо в специальных системах контроля действий пользователей баз данных;

– возможности настройки права доступа на уровне ОС серверов управления и АРМ;

– возможности настройки права доступа на уровне контроллеров и оборудования нижнего уровня ОКИИ (уровня КИПиА);

При предоставлении прав и привилегий по доступу к компонентам ОКИИ:

– возможность разделять права таким образом, чтобы у одного лица не было полного контроля над всеми компонентами ОКИИ;

– возможность разделения прав администрирования по компонентам АСУ– РСУ, противоаварийная защита, КИПиА;

– исключение неконтролируемого совершения операций в ОКИИ другими лицами;

– в случае необходимости предоставления доступа сотруднику сторонней организации (например, технической поддержке вендора) предоставить временный контролируемый доступ через защищенные каналы связи. По завершению работ, удаленный доступ должен быть отключен;

– обеспечить разделение ролей администратора и оператора АСУ:

○ администратор АСУ, имеющий возможность изменять конфигурацию АСУ, устанавливать и инициализировать модули ПО, создавать учетные записи работников и управлять правами доступа;

○ оператор АСУ, имеющий возможность контролировать и управлять технологическим процессом, без возможностей внесения изменений в состав и конфигурацию компонентов АСУ;

– возможность управления доступом на уровне ролей. При этом минимальный набор ролей на уровне ППО ОКИИ должен включать:

○ роль, реализующую функции администратора ОКИИ, включающие внесение изменений в состав и конфигурацию ОКИИ, установку и инициализацию модулей ПО, создание учетных записей работников и управление правами доступа;

- роль, реализующую функции оператора ОКИИ, включающие осуществление задач по контролю и управлению технологическим процессом, без возможностей внесения изменений в состав и конфигурацию компонентов ОКИИ.

– контроль средствами защиты конечных точек за применением мобильных ТС (флэш-накопители, внешние накопители на жестких дисках, ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства);

– все действия по созданию учетных записей (идентификаторов), присвоению и изменению прав доступа к компонентам ОКИИ должны регистрироваться в журналах ОКИИ.

7.2.3 Защита машинных носителей информации (ЗНИ)

Защита машинных носителей информации обеспечивается средствами СОИБ ОКИИ – подсистемой антивирусной защиты (средствами защиты конечных точек). СОИБ ОКИИ обеспечивает:

– регламентация правил и процедур защиты машинных носителей информации (ЗНИ.0);

– учет машинных носителей информации (ЗНИ.1);

– управление физическим доступом к машинным носителям информации (ЗНИ.2);

– контроль перемещения машинных носителей информации за пределы контролируемой зоны (ЗНИ.3);

– контроль использования интерфейсов ввода (вывода) информации на машинные носители информации (ЗНИ.5);

– контроль подключения машинных носителей информации (ЗНИ.7);

– Уничтожение (стирание) информации на машинных носителях информации (ЗНИ.8).

В BIOS АРМ операторов и инженерных станций ОКИИ, серверов управления СОИБ ОКИИ должна быть запрещена загрузка ОС с иных носителей, кроме жесткого диска компьютеров и серверов.

При отсутствии производственной необходимости, все интерфейсы и устройства ввода-вывода на съемные носители, включая порты USB, IEEE 1394, порты карт памяти, устройства чтения и записи на оптические и магнитные диски отключаются, возможность чтения/записи с/на съемные носители блокируется средством защиты конечных точек. Должна быть предусмотрена возможность физического ограничения доступа к машинным носителям информации устройств (АРМ, серверы, ПЛК, КИПиА) посредством опломбирования корпусов и интерфейсов (пломбировочные материалы должны быть включены в состав поставки АСУ).

Все факты использования съемных носителей информации, с указанием совершенных операций (чтения/записи с/на носитель) регистрируются в соответствующих системных журналах средства защиты конечных точек с указанием

времени регистрации события, совершенной операции, имени активного пользователя в ОС компонента АСУ.

7.2.4 Аудит безопасности (АУД)

Аудит событий безопасности обеспечивается средствами АСУ (встроенные в ОС, ППО, АСО механизмы регистрации событий безопасности), средствами подсистемы централизованного сбора и обработки событий безопасности в составе СОИБ ОКИИ. Комплекс мер обеспечивает:

– регламентация правил и процедур аудита безопасности (АУД.0);

– инвентаризацию информационных ресурсов (АУД.1);

– анализ уязвимостей и их устранение (АУД.2);

– генерирование временных меток и (или) синхронизация системного времени (АУД.3);

– регистрацию событий безопасности (АУД.4);

– контроль и анализ сетевого трафика (АУД.5);

– защиту информации о событиях безопасности (АУД.6);

– мониторинг безопасности (АУД.7);

– реагирование на сбои при регистрации событий безопасности (АУД.8);

– анализ действий пользователей (АУД.9);

– проведение внутренних аудитов (АУД.10).

В ОС и ППО АСУ должна осуществляться регистрация:

– событий безопасности;

– вход/выход пользователей, включая неуспешные попытки доступа, с указанием идентификатора пользователя, даты и времени события;

– создание, удаление, изменение привилегий пользователей;

– действия операторов, администраторов АСУ, по внесению изменений в конфигурацию и настройки АСУ, формирование команд и операций в АСУ, операции с журналами регистрации;

– совершаемые технологические операции, транзакции в АСУ и параметры операций, включая дату и время совершения операции, и иные параметры;

– системные ошибки;

– изменение параметров конфигурации ПО, состава компонентов АСУ, установка/удаление программ и обновлений;

– старт/стоп событий и процессов, запуск/останов особых режимов работы ПО и оборудования АСУ;

– доступ к объектам системы – файлам конфигурации, файлам данных, файлам журналов регистрации.

Средства защиты конечных точек, средства защиты от НСД регистрируют следующие виды событий:

– аутентификация пользователей в систему управления;

– факт отключения защиты на агентском ПО;

– обнаружение вирусов и дальнейшие действия с объектом;

– изменение состояния антивирусных средств;

– установку и распространение обновлений.

Средства анализа защищенности регистрируют следующие виды событий:

– аутентификация пользователей в систему;

– запуск и останов задач сканирования области инфраструктуры;

– выявленные известные уязвимости по сканируемым хостам;

– метаданные о задачах сканирования (время запуска, пользователь, время завершения задачи).

Средства межсетевого экранирования, средства криптографической защиты регистрируют следующие виды событий:

– аутентификация пользователей в систему;

– изменение политики межсетевого экранирования;

– изменение настроек сетевых интерфейсов МЭ;

– факт сработки запрещающих правил сетевого взаимодействия;

– сработки правил обнаружения вторжений на внешнем интерфейсе МЭ.

7.2.5 Антивирусная защита (АВЗ)

Антивирусная защита обеспечивается средств защиты конечных точек (АВЗ). Выполняются следующие меры:

– регламентация правил и процедур антивирусной защиты (АВЗ.0);

– реализация антивирусной защиты (АВЗ.1);

– антивирусная защита электронной почты и иных сервисов (АВЗ.2);

– контроль использования архивных, исполняемых и зашифрованных файлов (АВЗ.3)

– обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.4).

Средства АВЗ обеспечивают:

– отключение автоматического обновления и сканирования;

– отключение дополнительных функций АВЗ, за исключением файлового антивируса;

– обновление компонентов ПО и сигнатур вирусов только в «ручном» режиме;

– выполнение сканирования файловой системы только в «ручном» режиме;

– отключение автоматических действий с файлами (таких как их удаление, блокирование или перемещение). При обнаружении вредоносного ПО допускается только соответствующее оповещение на экран АРМ или сервера АСУ со звуковым оповещением;

– анализ архивных, исполняемых файлов;

– запрет доступа к административным функциям АВЗ под любыми учетными записями, за исключением привилегированных. Доступ к настройкам АВЗ для учетных записей администраторов должен предоставляться только после ввода пароля доступа;

– возможность исключения конкретных папок и файлов из области проверки средствами АВЗ, для исключения негативного влияния на работоспособность компонентов АСУ.

Для всех применяемых на АРМ и серверах АСУ (коммутационные серверы, SCADA-системы, серверы приложений и баз данных) антивирусных средств обязательно официальное подтверждение поставщиком АСУ и/или организацией, осуществляющей внедрение, техническую поддержку и/или сопровождение АСУ, программной совместимости с ППО АСУ для каждого типового АРМ и сервера и по результатам тестирования совместимости.

7.2.6 Предотвращение вторжений (компьютерных атак) (СОВ)

Для СОВ компонентов ОКИИ должны выполнять:

– Разработка политики предотвращения вторжений (компьютерных атак) (СОВ.0);

– Обнаружение и предотвращение компьютерных атак (СОВ.1);

– Обновление базы решающих правил (СОВ.2).

Данные меры должны быть реализованы за счет использования модуля обнаружения вторжений на периметровых МЭ, обеспечивающего анализ содержания потоков данных с проверкой на наличие признаков сетевых вторжений, в том числе с анализом протоколов, используемых SCADA.

7.2.7 Обеспечение целостности (ОЦЛ)

Для ОЦЛ компонентов ОКИИ должны выполнять:

– регламентация правил и процедур обеспечения целостности (ОЦЛ.0);

– контроль целостности ПО (ОЦЛ.1);

– контроль целостности информации (ОЦЛ.2).

Данные меры должны быть реализованы за счет использования встроенных в ППО и ОС механизмов защиты информации.

В АСУ должна быть реализована возможность контроля целостности ПО, включая их обновления, с использованием контрольных сумм, хэш-функции или электронной подписи в процессе загрузки или динамически в процессе работы АСУ.

Использование автоматизированных средств контроля состава и целостности ПО, при их наличии, не должно каким-либо образом влиять на работу ПО (блокировать или останавливать работу программ, удалять файлы), только регистрировать факт нарушения с указанием названия измененного программного модуля или не вошедшего в перечень разрешенного ПО.

7.2.8 Обеспечение доступности (ОДТ)

Для ОДТ компонентов ОКИИ должно выполняться:

– регламентация правил и процедур обеспечения доступности (ОДТ.0);

– резервное копирование информации (ОДТ.4);

– обеспечение возможности восстановления информации (ОДТ.5);

– обеспечение возможности восстановления программного обеспечения при нештатных ситуациях (ОДТ.6);

– контроль предоставляемых вычислительных ресурсов и каналов связи (ОДТ.8).

Данные меры должны быть реализованы за счет использования встроенных в ОС, ППО механизмов защиты информации, средств резервного копирования.

Компоненты АСУ (прикладное ПО АРМ, серверов) должны обладать функциональной возможностью выполнения резервного копирования конфигураций с сохранением резервных копий на машинные носители информации и сетевые ресурсы (систему резервного копирования, развернутую в технологической сети).

Резервному копированию подлежат:

– конфигурационные файлы и базы данных АСУ – не реже одного раза в неделю;

– электронные журналы регистрации событий АСУ – не реже одного раза в неделю;

– конфигурационные файлы компонентов АСУ – при каждом внесении изменений в конфигурационные настройки АСУ и ее средств защиты, но не реже одного раза в месяц;

– образы системных жестких дисков АРМ, серверов АСУ - не реже одного раза в месяц (неделя, в случае использования виртуальной инфраструктуры).

7.2.9 Защита технических средств и систем (ЗТС)

Для обеспечения ЗТС ОКИИ необходимы:

– регламентация правил и процедур защиты технических средств и систем (ЗТС.0);

– организация контролируемой зоны (ЗТС.2);

– управление физическим доступом (ЗТС.3);

– размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4);

– защита от внешних воздействий (ЗТС.5).

Данные меры защиты должны быть реализованы за счет применения организационных и технических мер.

Оборудование АСУ (АРМ, сервера, активное сетевое оборудование, ПЛК, КИПиА) должно размещаться в запираемых шкафах, либо должно быть обеспечено пломбирование корпусов оборудования. В случае размещения в запираемых шкафах, в АСУ должен быть реализован контроль доступа и оповещение оперативного персонала о вскрытии шкафа, с последующей регистрацией события в ПО верхнего уровня, а также, при наличии технической возможности, с передачей в системы охранной сигнализации.

7.2.10 Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)

Защита АСУ обеспечивается за счет использования встроенных в ППО и ОС механизмов защиты информации, средством защиты конечных точек и МЭ. Реализуется:

– регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов (ЗИС.0)

– разделение функций по управлению (администрированию) автоматизированной системой с иными функциями (ЗИС.1);

– защиту периметра автоматизированной системы (ЗИС.2);

– эшелонированная защита информационной (автоматизированной) системы (ЗИС.3);

– сегментирование информационной (автоматизированной) системы (ЗИС.4);

– организация демилитаризованной зоны (ЗИС.5);

– управление сетевыми потоками (ЗИС.6);

– сокрытие архитектуры и конфигурации автоматизированной системы (ЗИС.8);

– защиту информации при ее передаче по каналам связи (ЗИС.19);

– защита от угроз отказа в обслуживании (DOS, DDOS-атак) (ЗИС.34);

– управление сетевыми соединениями (ЗИС.35).

В ОКИИ должна быть реализована возможность локального, либо с использованием защищенных протоколов сетевого взаимодействия администрирования и конфигурирования компонентов сетевой инфраструктуры ОКИИ. Административный доступ средствами МЭ открывается только для сетевых адресов, специально выделенных для административных консолей (АРМ Администраторов СОИБ ОКИИ).

Управление закрытием сетевых подключений для взаимодействий внутри сегмента технологической подсети осуществляется ОС посредством использования функционала стека IP-протоколов. При использовании для осуществления информационного обмена TCP-протокола (протокол с установлением соединения), закрытие сетевого подключения происходит либо при отправке пакета завершения соединения, либо по определенному в настройках стека IP-протоколов временному интервалу. При использовании для осуществления информационного обмена UDP-протокола (протокола без установления соединения), закрытие сетевого подключения происходит по завершении передачи пакета. Сетевые подключения, осуществляемые из смежных технологических подсетей, разграничиваются средствами МЭ.

Информационное взаимодействие АСУ со смежными системами эксплуатирующей организации осуществляется через выделенные компоненты систем управления, что определяется их архитектурой и параметрами конфигурации. Для контроля информационных потоков между АСУ и смежными системами управления используется МЭ. Правило, предназначенное для контроля информационных потоков, должно разрешать информационное взаимодействие только между выделенными компонентами.

Блокирование сеанса пользователя осуществляется ОС Windows посредством ввода команды с клавиатуры. Для разблокирования сеанса пользователь должен выполнить процедуру повторной идентификации/аутентификации. Технологией обработки информации на конкретном рабочем месте блокировка сеанса пользователя может быть не предусмотрена.

Должна обеспечиваться при возможности отключение неиспользуемых интерфейсов на устройствах для исключения подключения отчуждаемых устройств.

При осуществлении информационного взаимодействия по региональной СПД между территориально обособленными площадками и между смежными системами в пределах площадок для фильтрации информационных потоков используется МЭ.

МЭ обеспечивает фильтрацию информационных потоков на основе критериев, задаваемых в правилах межсетевого экранирования.

Правила межсетевого экранирования определяются на основе информации о распределении IP-адресов и маршрутизации пакетов, предоставляемой эксплуатирующей организацией на этапе пусконаладочных работ.

Правила межсетевого экранирования должны явным образом запрещать информационное взаимодействие между АСУ и СПД общего пользования, а также внешними технологическими сетями.

В целях обеспечения непрерывности функционирования МЭ его электропитание осуществляется от источник бесперебойного питания для оборудования сетей связи, МЭ устанавливается в отказоустойчивом исполнении (кластере из двух программно-аппаратных комплексов).

Технологическая сеть и сеть общего назначения должны быть разделены. При этом:

– взаимодействие технологической и корпоративной СПД осуществляется через МЭ;

– количество точек взаимодействия между технологической и корпоративной сетями должно быть сведено к минимуму;

– технологическая сеть не должна иметь соединений с внешней сетью Интернет.

7.2.11 Реагирование на компьютерные инциденты (ИНЦ)

Реагирование на компьютерные инциденты осуществляется средствами СОИБ ОКИИ: подсистемой централизованного сбора и обработки событий безопасности. Обеспечивается:

– регламентация правил и процедур реагирования на компьютерные инциденты (ИНЦ.0)

– выявление компьютерных инцидентов (ИНЦ.1);

– информирование о компьютерных инцидентах (ИНЦ.2);

– анализ компьютерных инцидентов (ИНЦ.3);

– устранение последствий компьютерных инцидентов (ИНЦ.4);

– принятие мер по предотвращению повторного возникновения компьютерных инцидентов (ИНЦ.5);

– хранение и защита информации о компьютерных инцидентах (ИНЦ.6).

СрЗИ в составе СОИБ ОКИИ обеспечивают регистрацию событий безопасности, отправку по стандартным протоколам (Syslog) в подсистему централизованного сбора и обработки событий безопасности.

Отправляются события об отказах в обслуживании, сбоях (перезагрузках) в работе ТС, ПО и СрЗИ, нарушениях правил разграничения доступа, неправомерных действиях по сбору информации, внедрениях вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов ИБ.

7.2.12 Управление конфигурацией (УКФ)

Меры по управлению конфигурацией обеспечиваются встроенными в ОС, ППО механизмами защиты информации, средствами защиты конечных точек и МЭ:

– регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы (УКФ.0).

– управление изменениями (УКФ.2);

– установку (инсталляцию) только разрешенного к использованию программного обеспечения (УКФ.3).

Встроенные механизмы защиты СПО, ОС, АВЗ и МЭ должны обеспечивать: регистрацию действий по внесению изменений в конфигурацию системы.

Все действия по внесению изменений в конфигурации АСУ (изменения состава и параметров тегов, добавление/удаление оборудования, изменения в калибровочных таблицах, изменения алгоритмов работы АСУ, изменения в параметрах защиты –

изменение ролей и состава пользователей, параметров аутентификации и пр.) должны регистрироваться в журналах регистрации АСУ с указанием:

– даты и времени изменения;

– учетной записи пользователя;

– названия и значения изменяемого параметра.

Для программных прошивок контроллеров и микроконтроллеров должен поддерживаться архив версий встроенного ПО, с указанием истории вносимых изменений.

7.2.13 Управление обновлениями программного обеспечения (ОПО)

Для управления ОПО компонентов в АСУ должно выполняться:

– регламентация правил и процедур управления обновлениями программного обеспечения (ОПО.0);

– поиск, получение обновлений программного обеспечения от доверенного источника (ОПО.1);

– контроль целостности обновлений программного обеспечения (ОПО.2);

– тестирование обновлений программного обеспечения (ОПО.3);

– установка обновлений программного обеспечения (ОПО.4).

Данные меры должны быть реализованы за счет организационных мер, в комплект поставки АСУ должны входить инструкции по обновлению ОС, СПО, СрЗИ в составе СОИБ ОКИИ, а также регламенты (инструкции) по установке обновлений ОС и ППО от разработчика АСУ.

7.2.14 Планирование мероприятий по обеспечению безопасности (ПЛН)

В рамках мероприятий по планированию мероприятий по обеспечению безопасности должно быть обеспечено:

– регламентация правил и процедур планирования мероприятий по обеспечению защиты информации (ПЛН.0);

– Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации (ПЛН.1);

– контроль выполнения мероприятий по обеспечению защиты информации (ПЛН.2).

7.2.15 Обеспечение действий в нештатных ситуациях (ДНС)

Для обеспечения ДНС в АСУ должно быть обеспечено:

– регламентация правил и процедур обеспечения действий в нештатных ситуациях (ДНС.0);

– разработка плана действий в нештатных ситуациях (ДНС.1);

– обучение и отработка действий персонала в нештатных ситуациях (ДНС.2);

– резервирование программного обеспечения, ТС, каналов связи на случай возникновения нештатных ситуаций (ДНС.4);

– обеспечение возможности восстановления объекта автоматизации в случае возникновения нештатных ситуаций (ДНС.5);

– анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения (ДНС.6).

Данные меры должны быть реализованы за счет использования системы резервного копирования, организационных мер по восстановлению компонентов ОКИИ (при использовании резервных компонентов) в случае выхода из строя основных компонентов.

Организационные решения описаны в Документе Проект политики обеспечения непрерывности.

7.2.16 Информирование и обучение персонала (ИПО)

В рамках мероприятий по информированию и обучению персонала должно быть обеспечено:

– регламентация правил и процедур информирования и обучения персонала (ИПО.0);

– информирование персонала об угрозах безопасности информации и о правилах безопасной работы (ИПО.1);

– обучение персонала правилам безопасной работы (ИПО.2);

– контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы (ИПО.4).

7.2.17 Дополнительные требования к техническим мерам защиты информации КИПиА и средств измерений (контрольно-измерительных приборов)

Программируемые компоненты КИПиА и средств измерений должны иметь парольную защиту от НСД к просмотру и изменению настроек и конфигурации, а также изменению технологических параметров средства измерения.

Команды и данные, введенные через интерфейс пользователя оборудования КИПиА, не должны оказывать недопустимое влияние на метрологически значимое ПО и данные. Должно быть предусмотрено однозначное назначение каждой команды для инициирования функции или изменения данных в соответствии с сопроводительной технической документацией.

Конструкция оборудования КИПиА должна обеспечивать ограничение доступа к определенным частям средства измерения (включая ПО), в целях предотвращения несанкционированных настройки и вмешательства, которые могут привести к искажениям результатов измерений.

Защиту ПО и данных в оборудовании КИПиА обеспечить в соответствии с ГОСТ Р 8.654-2015.

В эксплуатационной документации на оборудование КИПиА должны быть описаны:

– все интерфейсы, посредством которых возможно изменение метрологически значимых параметров средства измерения, а также средства контроля доступа к указанным интерфейсам (в том числе фактов использования конфигурационного ПО);

– возможности независимой, т.е. выполняемой сторонним ПО, проверки идентификационных данных (контрольной суммы CRC32, md5, SHA1 или специально разработанный алгоритм с указанием способа их вычисления) микропрограммного обеспечения средства измерения, а также метрологически значимой части ПО для подтверждения подлинности ПО.

8 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

8.1 Структура СОИБ ОКИИ

СОИБ ОКИИ включает следующие функциональные подсистемы:

- Подсистема защиты от НСД;
- Подсистема межсетевого экранирования и обнаружения вторжений;
- Подсистема криптографической защиты;
- Подсистема антивирусной защиты;
- Подсистема анализа защищенности;
- Подсистема регистрации и обработки событий безопасности;
- Подсистема резервного копирования.

Структурная схема СОИБ ОКИИ представлена в документе НКНХ.5273-ПД-ИБ2-С1 «Структурная схема технических средств СОИБ ОКИИ».

8.2 Подсистема защиты от НСД

8.2.1 Общие положения

Подсистема защиты от НСД предназначена для выполнения следующих задач:

– исключение неправомерного и нелегитимного доступа к АРМ, серверам, SCADA, ПЛК, компонентам уровня КИПиА;

– разграничение доступа пользователям и сервисам к информационным ресурсам защищаемых ОКИИ;

- журналирование доступа пользователей к АРМ и серверам;
- контроль подключения отчуждаемых устройств к АРМ и серверам;
- контроль запущенных программ, процессов на АРМ и серверах.

Подсистема защиты от НСД обеспечивается как встроенными механизмами безопасности системного ПО ПЛК, сетевых устройств, АРМ и серверов на базе ОС семейства Linux, так и наложенными средствами защиты:

8.2.2 Функциональные возможности подсистемы

Подсистема защиты от НСД обеспечивает выполнение функций, требуемых для реализации следующих мер обеспечения безопасности объекта КИИ:

– ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов;

- ИАФ.2 Идентификация и аутентификация устройств;
- ИАФ.3 Управление идентификаторами;
- ИАФ.4 Управление средствами аутентификации;

– ИАФ.7 Защита аутентификационной информации при передаче;

– УПД.1 Управление учетными записями пользователей;

– УПД.2 Реализация модели управления доступом;

– УПД.4 Разделение полномочий (ролей) пользователей;

– УПД.5 Назначение минимально необходимых прав и привилегий;

– УПД.6 Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему;

– УПД.10 Блокирование сеанса доступа пользователя при неактивности;

– УПД.11 Управление действиями пользователей до идентификации и аутентификации;

– АУД.3 Генерирование временных меток и (или) синхронизация системного времени;

– АУД.4 Регистрация событий безопасности;

– АУД.6 Защита информации о событиях безопасности;

– ЗИС.1 Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями;

– ЗИС.3 Эшелонированная защита информационной (автоматизированной) системы;

– УКФ.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения.

8.2.3 Структура подсистемы

Подсистема защиты от НСД реализуется встроенными механизмами безопасности, наложенными средствами защиты:

– встроенные механизмы защиты ОС АРМ/серверов АСУТП;

– встроенные механизмы защиты прикладного ПО АСУТП;

– встроенные механизмы защиты активного сетевого оборудования;

– встроенные механизмы защиты ПЛК;

– встроенные механизмы безопасности BIOS;

– средство защиты от НСД – агент Secret Net Studio, устанавливаемый на АРМ под управлением ОС семейства Windows;

– средство защиты конечных точек – агент KICS for Nodes, устанавливаемый на АРМ и серверы под управлением ОС семейства Windows, семейства Linux.

8.2.3.1 Требования к параметрам настройки встроенных механизмов защиты ОС

В ОС АРМ / серверов АСУТП используются встроенные механизмы идентификации и аутентификации пользователей, управления правами доступа, а также регистрации событий безопасности.

Детальное описание и порядок настройки для применяемых в АСУТП ОС должны быть разработаны на этапе внедрения.

Применяемые учетные записи в ОС делятся на следующие типы:

– административные – персональные учетные записи для каждого администратора (инженера) АСУТП,

– технические – учетные записи, используемые для запуска ПО АСУТП, настройки отдельных компонентов АСУТП и СОИБ ОКИИ;

– операторские – персональные или групповые учетные записи, используемые операторами АСУТП для доступа в ОС.

Все субъекты доступа уникально идентифицируются и аутентифицируются при входе в ОС с помощью ввода идентификатора и пароля. Идентификация и аутентификация осуществляются до выполнения пользователем каких-либо действий.

При этом допускается автоматическая загрузка ОС на АРМ оператора с ограниченным доступом только к интерфейсу прикладного ПО АСУТП (режим «киоска»);

Для операторских учетных записей запрещается назначения прав доступа, соответствующих группе «Локальные администраторы».

Для операторских УЗ отключено блокирование сеанса доступа пользователя при неактивности (применимо только для административных и технических УЗ).

В ОС задаются параметры политики паролей и блокировки УЗ:

– для административных, технических и операторских учетных записей пароли задаются вручную.

– длина пароля должна быть не менее 8 символов и состоять из цифр, букв и специальных символов;

– срок действия пароля должен быть не ограничен;

– повторное использование пароля должно быть запрещено.

– отключена блокировка УЗ.

Назначение прав доступа и настройка политик безопасности в ОС выполняется на каждом АРМ / сервере отдельно.

Для регистрации событий безопасности ОС настраиваются политики аудита.

Долговременное хранение событий безопасности обеспечивается Подсистема регистрации и обработки событий безопасности (Раздел 0).

При взаимодействии с компонентами ОКИИ применяются защищенные протоколов, отключаются небезопасные протоколы.

Защита журналов учета событий ОС от переполнения, несанкционированного просмотра и изменения обеспечивается встроенными механизмами защиты ОС. Возможность управления журналами событий безопасности ОС предоставляется только администраторам АСУТП.

На АРМ и серверах настраивается синхронизация времени с единого источника – сервера точного времени.

8.2.3.2 Требования к параметрам настройки встроенных механизмов защиты прикладного ПО АСУТП

Встроенными механизмами безопасности прикладного ПО АСУТП обеспечивается:

– идентификация и аутентификация пользователей с помощью учетной записи и пароля (централизованное управление с сервера АСУТП);

– настройка ролевой модели разграничения доступа (Администратор и Оператор);

– регистрация событий безопасности;

– настройка защищенных протоколов сетевого взаимодействия;

– смена паролей учетных записей, установленных производителем по умолчанию при развертывании ПО.

8.2.3.3 Требования к параметрам настройки встроенных механизмов защиты активного сетевого оборудования

На управляемом активном сетевом оборудовании выполняются следующие настройки:

– идентификация и аутентификация администраторов осуществляются по имени пользователя и паролю и обеспечиваются встроенными механизмами сетевого оборудования.

– применяются локальные УЗ.

– устанавливается уровень журналирования (severity level) в режим informational (6 level).

– настроена синхронизация с единого источника времени.

Все применяемое активное сетевое оборудование должно устанавливаться в запираемых шкафах и / или помещениях.

Встроенными механизмами безопасности активного сетевого оборудования обеспечивается (при наличии технической возможности):

– настройка персонифицированных учетных записей для доступа к функциям администрирования;

– смена паролей для штатных учетных записей на пароли, соответствующие требованиям безопасности;

– установка параметров парольных политик локальных учетных записей;

– настройка протоколов защищенного взаимодействия, отключение небезопасных протоколов;

– настройка механизма Port Security;

– настройка «белых» списков доступа (ACL).

8.2.3.4 Требования к параметрам настройки встроенных механизмов защиты ПЛК

В ПЛК используются встроенные механизмы идентификации и аутентификации, выполняется проверка выполнения приведенных ниже рекомендаций (без выполнения дополнительных настроек).

На ПЛК должны применяться только технические учетные записи. При наличии технической возможности на ПЛК должен быть настроен контроль подключения к ПЛК с помощью списка контроля доступа (access list) с возможностью удаленного подключения только с определенных сетевых узлов.

8.2.3.5 Требования к параметрам настройки встроенных механизмов безопасности BIOS.

Встроенными механизмами безопасности BIOS реализуются следующие функции СОИБ:

– управление действиями пользователей до идентификации и аутентификации;

– контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации.

Встроенными средствами BIOS осуществляются следующие настройки:

– установка пароля на доступ к BIOS;

– отключение функции загрузки системы с внешних носителей информации и загрузки по сети;

– отключение неиспользуемых периферийных устройств (CD/DVD-приводы и интерфейсы SATA).

До момента успешного прохождения идентификации и аутентификации администратора любые действия в среде BIOS запрещены.

8.2.3.6 Secret Net Studio

Клиентское ПО Secret Net Studio реализует следующие функции:

– усиленная идентификация и аутентификация пользователей при доступе к защищаемым АРМ, серверам по логину и паролю условно-постоянного действия, персональному идентификатору с использованием механизмов Secret Net Studio;

– управление и разграничение доступа к ресурсам, защищаемым на уровне ОС, контроль их изменения;

– регистрация событий безопасности локально на защищаемых АРМ, серверах;

– контроль подключения и разграничение доступа к подключаемым устройствам – запрет подключения внешних устройств, ведение электронного реестра разрешенных устройств, разрешенных в клиенте Secret Net Studio;

– регистрация всех событий печати на защищаемых серверах и АРМ, контроль вывода информации на печать;

– затирание информации при удалении на локальных и внешних (съемных) носителях;

– аудит изменения ролей пользователей и их прав доступа.

Идентификация и аутентификация пользователей на защищаемых АРМ и серверах осуществляется путем ввода учетных данных (логин и пароль, на который распространяется парольная политика). В качестве дополнительного фактора аутентификации возможно использование персонального идентификатора, зарегистрированного в системе Secret Net Studio.

Управление клиентским ПО Secret Net Studio осуществляется локально Администратором СОИБ ОКИИ.

8.2.3.7 KICS for Nodes

Решения по применению ПО KICS for Nodes описано в разделе 0 настоящего документа.

8.2.3.8 Резервное копирование

Восстановление образов АРМ / серверов, конфигурация активного сетевого оборудования и ПЛК осуществляется с помощью встроенных механизмов резервирования для ПЛК, а также с помощью подсистемы резервного копирования СОИБ ОКИИ для АРМ и серверов ОКИИ.

8.2.3.9 Обновление компонентов

Установка обновлений ОС, ППО и прошивок активного сетевого оборудования после проведения их тестирования. В объектах защиты автоматическая установка обновлений без проведения их тестирования не допускается. Обновление осуществляется в ручном режиме на основе предварительно скаченных с официальных сайтов производителей дистрибутивов. Тестирование обновлений проводится на отдельных компонентах в выделенном сегменте.

Все обновления безопасности устанавливаются на основе наличия информации о критической уязвимости в применяемом на объекте защиты оборудовании и ПО, а также письменного указания/распоряжения по Предприятию и только в момент технологического останова/вывода оборудование в ремонт.

Перед обновлением компонентов контролируется наличие актуальной резервной копии данных и конфигурации.

8.2.4 Описание комплекса ТС подсистемы

Клиентское ПО Secret Net Studio устанавливается на АРМ под управлением ОС семейства Windows. Системные требования представлены в Таблица 8.1.

Таблица 8.1 – Системные требования для установки ПО Secret Net Studio

Параметр	Описание
Операционная система	Windows 11; Windows 10; Windows 8.1 Rollup Update; Windows 7 SP1 KB3033929; Windows Server 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2 Rollup Update; Windows Server 2008 R2 SP1 KB3033929
Процессор	В соответствии с требованиями ОС, установленной на компьютер
Интерфейсы, необходимые для установки программного обеспечения	Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры
Оперативная память	Минимально – 2 ГБ; Рекомендуется – 4 ГБ
Жесткий диск (свободное пространство)	4 ГБ
Дополнительное ПО	Internet Explorer 8 или выше
Поддерживаемое прикладное ПО	ПАК Соболь (версии 3.0.9, 3.1, 4.2, 4.3) Kaspersky Endpoint Security (версии 10.03, 11) Microsoft Office (версии 2010 – 2019)

Клиентское ПО KICS for Nodes устанавливается на АРМ и серверы под управлением ОС семейства Windows, Linux. Системные требования для KICS for Linux Nodes представлены в Таблица 8.2. Системные требования для KICS for Windows Nodes представлены в Таблица 8.3.

Таблица 8.2 – Системные требования для установки KICS for Linux Nodes

Параметр	Описание
Операционная система	AlmaLinux OS 8 и выше; AlmaLinux OS 9 и выше; AlterOS 7.5 и выше; Amazon Linux 2; Astra Linux Common Edition (очередное обновление 2.12); Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5); Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6); Astra Linux Special Edition РУСБ.10015-16 (исп-е 1) (обновление 1.6); CentOS 6.7 и выше; CentOS 7.2 и выше; CentOS 8.0 и выше; Debian GNU / Linux 9.4 и выше; Debian GNU / Linux 10.1 и выше; Linux Mint 19 и выше; Linux Mint 20.1 и выше;

Параметр	Описание
	openSUSE Leap 15.0 и выше; Oracle Linux 7.3 и выше; Oracle Linux 8.0 и выше; Red Hat Enterprise Linux 6.7 и выше; Red Hat Enterprise Linux 7.2 и выше; Red Hat Enterprise Linux 8.0 и выше; SUSE Linux Enterprise Server 15 и выше; Ubuntu 18.04 LTS и выше; Ubuntu 20.04 LTS; Альт Рабочая Станция 10; Альт Сервер 10; Гослинукс 7.2; РЕД ОС 7.3; РЕД ОС 8.0; РОСА Enterprise Linux Server 7.9; РОСА Enterprise Linux Desktop 7.9; РОСА "Кобальт" 7.9; РОСА "Хром" 12; СинтезМ-Клиент 8.6; СинтезМ-Сервер 8.6.
Процессор	Процессор Core 2 Duo 1.86 ГГц или выше
Оперативная память	2 ГБ
Жесткий диск	4 ГБ свободного места
Дополнительное ПО	Интерпретатор языка Perl версии 5.10 или выше; Установленные пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make, ld) на операционных системах, не поддерживающих технологию fanotify; Заголовочные файлы ядра операционной системы для компиляции модулей Kaspersky Industrial CyberSecurity for Linux Nodes на операционных системах, не поддерживающих технологию fanotify

Таблица 8.3 – Системные требования для установки KICS for Nodes (Windows)

Параметр	Описание
Операционная система	Windows XP Professional SP2 32-разрядная / 64-разрядная; Windows XP Professional SP3 32-разрядная; Windows Vista SP2 32-разрядная / 64-разрядная; Windows 7 SP1 Professional / Enterprise / Ultimate 32-разрядная / 64-разрядная; Windows 8 Professional / Enterprise 32-разрядная/ 64-разрядная; Windows 8.1 Professional / Enterprise 32-разрядная / 64-разрядная; Windows 10 LTSC 2015 версии 1507 32-разрядная / 64-разрядная; Windows 10 LTSC 2016 версии 1607 32-разрядная / 64-разрядная; Windows 10 RS4 версии 1803 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 RS5 версии 1809 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 LTSC 2019 версии 1809 32-разрядная / 64-разрядная;

Параметр	Описание
	Windows 10 19H1 версии 1903 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 20H1 версии 2004 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 20H2 версии 2009 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 21H1 версии 21H1 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 21H2 версии 21H2 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 22H2 версии 22H2 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная; Windows 10 LTSC 2021 версии 21H2 32-разрядная / 64-разрядная; Windows 11 21H2 версии 21H2 Home / Pro / Education / Enterprise 64-разрядная; Windows 11 22H2 версии 22H2 Home / Pro / Education / Enterprise 64-разрядная.
Процессор	2.4 ГГц четырехъядерный или выше
Оперативная память	2 ГБ
Жесткий диск	4 ГБ свободного места
Поддерживаемые ПЛК	SIMATIC S7-300 (Siemens); SIMATIC S7-400 (Siemens); SIMATIC S7-400H в режиме работы с резервированием (Siemens); Schneider Electric Modicon M340; Schneider Electric Modicon M580; устройства на базе CODESYS V3; ОВЕН ПЛК210; Fastwel CPM723-01; Прософт-Системы Regul R500; Siemens SIMATIC S7-1500; Siemens SIMATIC S7-1200; Siemens серии SIPROTEC 4

8.2.5 Сведения о сертификатах

ПО Secret Net Studio имеет сертификат ФСТЭК России №3745 от 16.05.2017 действителен до 16.05.2025 на соответствие требованиям руководящих документов по 4 уровню доверия, 5 классу защищенности СВТ, 4 классу защиты СКН (ИТ.СКН.П4.ПЗ), 4 классу защиты САВЗ (ИТ.САВЗ.А4.ПЗ, ИТ.САВЗ.Б4.ПЗ, ИТ.САВЗ.В4.ПЗ, ИТ.САВЗ.Г4.ПЗ), 4 классу защиты МЭ тип "В" (ИТ.МЭ.В4.ПЗ), 4 классу защиты СОВ (ИТ.СОВ.У4.ПЗ).

Kaspersky Industrial CyberSecurity for Nodes имеет сертификат ФСТЭК №3907 от 03.04.2018, действительный по 03.04.2026 на соответствие требованиям: Требования доверия (2), Требования к САВЗ, Профиль защиты САВЗ (В второго класса защиты. ИТ.САВЗ.В2.ПЗ), Требования к СКН, Профиль защиты СКН(контроля подключения съемных машинных носителей информации второго класса защиты. ИТ.СКН.П2.ПЗ), ЗБ.

8.2.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в следующей Таблица 8.4.

Таблица 8.4 – Используемые для взаимодействия сетевые порты

Название сервиса/ номер порта	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
TCP/123 (NTP), UDP/123 (NTP)	Синхронизация времени с NTP-сервером	Компонент ОКИИ	NTP сервер

8.3 Подсистема криптографической защиты информации

8.3.1 Общие положения

Подсистема криптографической защиты информации в составе СОИБ ОКИИ предназначена для обеспечения защищенного канала связи (VPN) между объектами ПАО «Нижнекамскнефтехим»: МДП Нижнекамск (титул 2012), МДП Казань (титул 1012), всех БКТМ (титулы 208-227, всего 20 объектов).

Защищенные каналы связи используются для взаимодействия серверных компонентов защищаемых ОКИИ, расположенных в МДП Нижнекамск, с компонентами нижнего уровня на площадках БКТМ (20 объектов), МДП Казань.

Также криптошлюзы являются сертифицированными межсетевыми экранами и обеспечивают разграничение (запрет) сетевого доступа различных ОКИИ друг с другом на уровне БКТМ, маршрутизацию подсетей ОКИИ БКТМ в подсети МДП Нижнекамск.

8.3.2 Функциональные возможности подсистемы

Подсистема криптографической защиты информации обеспечивает реализацию следующих мер обеспечения безопасности объекта КИИ:

– ИАФ.6 Двусторонняя аутентфиикация;

– ИАФ.7 Защита аутентификационной информации при передаче (Защита обратной связи при вводе аутентификационной информации);

– АУД.4 Регистрация событий безопасности;

– ЗИС.2 Защита периметра информационной (автоматизированной) системы;

– ЗИС.3 Эшелонированная защита информационной (автоматизированной) системы;

– ЗИС.4 Сегментирование информационной (автоматизированной) системы (Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы);

– ЗИС.5 Организация демилитаризованной зоны;

– ЗИС.6 Управление сетевыми потоками;

– ЗИС.8 Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы;

– ЗИС.19 Защита информации при ее передаче по каналам связи;

– ЗИС.20 Обеспечение доверенных канала, маршрута;

– ЗИС.34 Защита от угроз отказа в обслуживании (DOS, DDOS-атак);

– ЗИС.35 Управление сетевыми соединениями.

В части защиты каналов связи криптошлюзы подсистемы обеспечивают выполнение следующих функций:

– организация защищенных VPN-туннелей типа «точка-точка» (Site-to-Site);

– двусторонняя криптографическая аутентификация криптошлюзов средств криптографической защиты информации (СКЗИ) при установлении соединения с применением сертификатов ключей проверки электронной подписи;

– контроль целостности пакетов с использованием хэш-функции для защиты передаваемых данных от искажения;

– обеспечение КЗ данных, передаваемых по VPN-туннелям, за счет применения алгоритмов шифрования и имитозащиты;

– приоритезация сетевого трафика (QoS);

– фильтрация пакетов в соответствии с настроенной политикой межсетевого экранирования на криптошлюзах.

В части межсетевого экранирования криптошлюзы подсистемы обеспечивают выполнение следующих функций:

– экранирование сегментов технологических сетей ТМ и СОУ, СМПО, АСДУЭ в БКТМ посредством фильтрации сетевых пакетов при межсегментном взаимодействии на основе данных канального, сетевого, транспортного и прикладного уровней сетевой модели стека сетевых протоколов OSI/ISO в соответствии с заданными правилами;

– маршрутизация сетевых сегментов ТМ и СОУ, СМПО, АСДУЭ БКТМ в соответствующие сегменты МДП Нижнекамск для дальнейшей терминации подсетей ТМ и СОУ, СМПО, АСДУЭ на ПАК МЭ Infowatch АРМА Стена К1000;

– трансляция сетевых адресов (технология NAT);

– регистрация и учет фильтруемых пакетов с указанием адреса, времени и результата фильтрации, аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети;

– отправка зарегистрированных событий безопасности в систему централизованного сбора и обработки событий безопасности (SIEM).

8.3.3 Структура подсистемы

Подсистема криптографической защиты информации реализуется на базе программно-аппаратного комплекса С-терра и состоит из следующих компонентов:

– ПО Система управления С-терра КП, устанавливаемое на выделенный сервер МДП Нижнекамск в проектируемый сегмент СОИБ ОКИИ – НКНХ.5273-0000-С-SRV-024А;

– кластер ПАК С-терра Шлюз 1000, устанавливаемый в МДП Нижнекамск, обеспечивающий защиту каналов связи со всеми удаленными объектами;

– кластер ПАК С-терра Шлюз 1000, устанавливаемый в МДП Казань, обеспечивающий защиту каналов связи с МДП Нижнекамск;

– кластеры ПАК С-терра Шлюз 1000 (20 кластеров), устанавливаемый в БКТМ (титул 208 – титул 227), обеспечивающие защиту каналов связи с МДП Нижнекамск;

– ПО управления С-Терра КП, устанавливаемое на АРМ Администратора СОИБ ОКИИ, предназначенное для управления VPN-сетями, организованными на криптошлюзах С-терра.

8.3.3.1 Криптошлюзы МДП Нижнекамск

Кластер С-терра Шлюз 1000 включает следующие шлюзы:

– первый узел кластера С-терра Шлюз 1000 НКНХ.5273-0000-Т-FW-021А;

– первый узел кластера С-терра Шлюз 1000 НКНХ.5273-0000-Т-FW-022А.

Кластер С-терра Шлюз 1000 МДП Нижнекамск включается в следующие сегменты технологической сети:

– внешние интерфейсы – в транзитный сегмент между удаленными объектами, в рамках которого будут построены VPN каналы;

– внутренние интерфейсы – в подсети ТМ и СОУ, СМПО, АСДУЭ для маршрутизации трафика на интерфейсы МЭ Infowatch АРМА Стена К1000;

– управляющий интерфейс – в сегмент СОИБ ОКИИ для управления шлюзами, VPN-каналами, сбора событий безопасности по протоколу syslog.

Шлюзы С-терра 1000 включаются в сеть следующим образом:

– внешние (outside) интерфейсы подключаются к стеку внешних коммутаторов СОИБ ОКИИ, которые в свою очередь подключаются к основной и резервной линии связи между объектами ПАО «Нижнекамскнефтехим»;

– внутренние интерфейсы подключаются к стеку внутренних коммутаторов СОИБ ОКИИ, которые в свою очередь подключаются к сетевому оборудованию технологических сетей МДП Нижнекамск.

Управление шлюзами осуществляется централизованно ПО «Система управления С-терра КП», устанавливаемом на выделенный сервер в проектируемый сегмент СОИБ ОКИИ (МДП Нижнекамск) – НКНХ.5273-0000-С-SRV-024А.

Формирование правил сетевого разграничения доступа, маршрутизации осуществляется на этапе внедрения шлюзов на основе матрицы взаимодействия компонентов защищаемых ОКИИ с другими ОКИИ.

8.3.3.2 Криптошлюзы МДП Казань

Кластер С-терра Шлюз 1000 включает следующие шлюзы:

– первый узел кластера С-терра Шлюз 1000 НКНХ.5273-0000-Т-FW-031А;

– первый узел кластера С-терра Шлюз 1000 НКНХ.5273-0000-Т-FW-032А.

Кластер С-терра Шлюз 1000 МДП Казань включается в следующие сегменты технологической сети:

– внешние интерфейсы – в транзитный сегмент между удаленными объектами, в рамках которого будут построены VPN каналы;

– внутренние интерфейсы – в подсети ТМ и СОУ, СМПО для маршрутизации трафика на интерфейсы МЭ Infowatch АРМА Стена К1000 в МДП Нижнекамск;

– управляющий интерфейс – в транзитный сегмент между удаленными объектами, в рамках которого будут построены VPN каналы. Доступ к управляющему интерфейсу будет ограничен локальными правилами межсетевого экранирования.

Шлюзы С-терра 1000 включаются в сеть следующим образом:

– внешние (outside) интерфейсы подключаются к стеку внешних коммутаторов СОИБ ОКИИ, которые в свою очередь подключаются к основной и резервной линии связи между объектами ПАО «Нижнекамскнефтехим»;

– внутренние интерфейсы подключаются к стеку внутренних коммутаторов СОИБ ОКИИ, которые в свою очередь подключаются к сетевому оборудованию технологических сетей МДП Казань.

Управление шлюзами осуществляется централизованно ПО «Система управления С-терра КП», устанавливаемом на выделенный сервер в проектируемый сегмент СОИБ ОКИИ (МДП Нижнекамск) – НКНХ.5273-0000-С-SRV-024А.

Формирование правил сетевого разграничения доступа, маршрутизации осуществляется на этапе внедрения шлюзов на основе матрицы взаимодействия компонентов защищаемых ОКИИ с другими ОКИИ.

8.3.3.3 Криптошлюзы БКТП

Кластеры С-терра Шлюз 1000 включает следующие шлюзы:

– первый узел кластера С-терра Шлюз 1000 НКНХ.5273-0000-Т-FW-[08-27]1А, всего 20 узлов;

– первый узел кластера С-терра Шлюз 1000 НКНХ.5273-0000-Т-FW-[08-27]2А, всего 20 узлов.

Кластеры С-терра Шлюз 1000 БКТМ включаются в следующие сегменты технологической сети:

– внешние интерфейсы – в транзитный сегмент между удаленными объектами, в рамках которого будут построены VPN каналы;

– внутренние интерфейсы – в подсети ТМ и СОУ, СМПО, АСДУЭ для маршрутизации трафика на интерфейсы МЭ Infowatch АРМА Стена К1000 в МДП Нижнекамск;

– управляющий интерфейс – в транзитный сегмент между удаленными объектами, в рамках которого будут построены VPN каналы. Доступ к управляющему интерфейсу будет ограничен локальными правилами межсетевого экранирования.

Шлюзы С-терра 1000 включаются в сеть следующим образом:

– внешние (outside) интерфейсы подключаются к стеку внешних коммутаторов СОИБ ОКИИ, которые в свою очередь подключаются к основной и резервной линии связи между объектами ПАО «Нижнекамскнефтехим»;

– внутренние интерфейсы подключаются к стеку внутренних коммутаторов СОИБ ОКИИ, которые в свою очередь подключаются к сетевому оборудованию технологических сетей МДП Казань.

Управление шлюзами осуществляется централизованно ПО «Система управления С-терра КП», устанавливаемом на выделенный сервер в проектируемый сегмент СОИБ ОКИИ (МДП Нижнекамск) – НКНХ.5273-0000-С-SRV-024А.

Формирование правил сетевого разграничения доступа, маршрутизации осуществляется на этапе внедрения шлюзов на основе матрицы взаимодействия компонентов защищаемых ОКИИ с другими ОКИИ.

8.3.4 Описание комплекса технических средств подсистемы

Производительность и технические характеристики ПАК С-терра Шлюз 1000 приведены в Таблица 8.5.

Таблица 8.5 – Технические характеристики ПАК С-терра Шлюз 1000

Параметр	Описание
Производительность шифрования	270 Мбит/с
Максимальное количество туннелей	50
Количество сетевых интерфейсов 1 Гбит/с	6
Объем оперативной памяти (RAM)	4 Гб
Размер криптошлюза	1U

8.3.5 Сведения о сертификатах

Программный комплекс «С-терра Шлюз» версии 4.3 имеет сертификат ФСТЭК №4478 от 30.11.2021, действительный по 30.11.2026 на соответствие требованиям ФСТЭК: Требования доверия (4), Требования к МЭ, Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), сертификаты ФСБ на соответствие классам КС1, КС2, КС3.

8.3.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в Таблица 8.6.

Таблица 8.6 – Используемые для взаимодействия сетевые порты

Название сервиса / номер порт	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
С-терра Шлюз 1000	Сервер управления ПО «С-Терра КП»	TCP/22	Управление компонентами ПАК С-терра Шлюз 1000
С-терра Шлюз 1000	Сервер системы распознавания сетевых имен DNS	TCP/53	Интеграция с DNS
Сервер управления ПО «С-Терра КП»	Kuma	SYSLOG	Отправка журналов безопасности подсистемы криптографической защиты в SIEM

8.4 Подсистема межсетевого экранирования

8.4.1 Общие положения

Подсистема межсетевого экранирования предназначена для выполнения следующих задач:

– изоляция технологических сетей от корпоративной сети;

– фильтрация (и разграничение) сетевого трафика при взаимодействии сегментов технологических сетей объектов автоматизации в соответствии с заданными правилами межсетевого экранирования;

– потоковый анализ проходящего через ПАК МЭ сетевого трафика с целью обнаружения вредоносных файлов, сетевых атак, зараженных устройств в сети, обращающихся к известным ботнет сетям в точке подключения ТСПД к внешним сетям;

– автоматическое реагирование на сетевые вторжения: блокировка трафика с признаками вредоносной активности или оповещение администрирующего СрЗИ персонала.

Информационное взаимодействие АСУ со смежными системами эксплуатирующей организации осуществляется через выделенные компоненты систем управления, что определяется их архитектурой и параметрами конфигурации. Для контроля информационных потоков между АСУ и смежными системами управления используется МЭ с поддержкой технологических протоколов. Правило, предназначенное для контроля информационных потоков, должно разрешать информационное взаимодействие только между выделенными компонентами.

Правила межсетевого экранирования должны явным образом запрещать неконтролируемое информационное взаимодействие между АСУ и КСПД, а также внешними технологическими сетями.

Технологическая сеть и КСПД назначения должны быть разделены. При этом:

– взаимодействие технологической и КСПД осуществляется через МЭ;

– количество точек взаимодействия между технологической и корпоративной сетями должно быть сведено к минимуму;

– технологическая сеть не должна иметь соединений с сетью «Интернет».

8.4.2 Функциональные возможности подсистемы

Подсистема межсетевого экранирования обеспечивает выполнение функций, требуемых для реализации следующих мер обеспечения безопасности объекта КИИ:

– АУД.3 Генерирование временных меток и (или) синхронизация системного времени;

– АУД.4 Регистрация событий безопасности;

– СОВ.1 Обнаружение и предотвращение компьютерных атак;

– СОВ.2 Обновление базы решающих правил;

– ЗИС.2 Защита периметра информационной (автоматизированной) системы;

– ЗИС.3 Эшелонированная защита информационной (автоматизированной) системы;

– ЗИС.4 Сегментирование информационной (автоматизированной) системы (Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы);

– ЗИС.5 Организация демилитаризованной зоны;

– ЗИС.6 Управление сетевыми потоками;

– ЗИС.8 Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы;

– ЗИС.19 Защита информации при ее передаче по каналам связи;

– ЗИС.20 Обеспечение доверенных канала, маршрута;

– ЗИС.34 Защита от угроз отказа в обслуживании (DOS, DDOS-атак);

– ЗИС.35 Управление сетевыми соединениями.

В части межсетевого экранирования ПАК МЭ АРМА Стена обеспечивает выполнение следующих функций:

– экранирование сегментов технологических сетей ОКИИ АСУТП (ТМ и СОУ, СМПО, АСДУЭ), КИТСО, СМИС;

– периметровое экранирование для сегментов технологических сетей ОКИИ АСУТП (ТМ и СОУ, СМПО, АСДУЭ), КИТСО, СМИС, ЛСО;

– разграничение доступа к сетевым ресурсам ТСПД посредством фильтрации сетевых пакетов при межсегментном взаимодействии на основе данных канального, сетевого, транспортного и прикладного уровней сетевой модели стека сетевых протоколов OSI/ISO в соответствии с заданными правилами;

– контроль открытых сетевых соединений с передачей только тех сетевых пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений (statefull firewall);

– инспектирование протоколов до 7 уровня модели OSI (с разбором технологических протоколов Modbus TCP Modbus TCP x90 func. code (UMAS) S7 Communication S7 Communication plus OPC DA OPC UA IEC 60870-5-104 IEC 61850-8-1 MMS IEC 61850-8-1 GOOSE KRUG ADS TCP / EtherCAT) в режиме контроля состояния сессий на предмет компрометации конфиденциальности, нарушения целостности, доступности защищаемой информации, обхода механизмов безопасности сети вплоть до уровня приложений эталонной модели OSI;

– трансляция сетевых адресов (технология NAT);

– регистрация и учет фильтруемых пакетов с указанием адреса, времени и результата фильтрации, аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети;

– отправка зарегистрированных событий безопасности в систему централизованного сбора и обработки событий безопасности (SIEM).

В части обнаружения вторжений ПАК МЭ АРМА Стена обеспечивает выполнение следующих функций:

– анализ сетевого трафика на периметре технологической сети на предмет компрометации конфиденциальности, нарушения целостности, доступности защищаемой информации, обхода механизмов безопасности сети вплоть до уровня приложений сетевой модели стека сетевых протоколов OSI/ISO, в том числе специализированных протоколов SCADA;

– обнаружение сетевого трафика нежелательных приложений, управляющих команд АСУ;

– обнаружение и блокировка активности вредоносного ПО (сетевые «черви», «трояны», «шпионы» и т. д.);

– обнаружения аномалий сетевых протоколов;

– возможность создания собственных сигнатур сетевых атак;

– обновление базы знаний (базы сигнатур сетевых атак) в офлайн-режиме;

– автоматическое реагирование в случае обнаружения сетевых вторжений: блокировка трафика и/или оповещение администрирующего персонала СОИБ ОКИИ ТП в режиме реального времени;

– возможность установления исключений для анализа модулем IDS;

– регистрация информации об обнаруженных сетевых вторжениях.

8.4.3 Структура подсистемы

Подсистема межсетевого экранирования реализуется с помощью МЭ:

– Периметровый межсетевой экран ТСПД АСУТП – кластер ПАК МЭ Infowatch АРМА Стена К1000, устанавливаемый в МДП Нижнекамск (титул 2012);

– Периметровый межсетевой экран ТСПД ЛСО – кластер ПАК МЭ Infowatch АРМА Стена К1000, устанавливаемый в МДП Нижнекамск (титул 2012);

– Периметровый межсетевой экран ТСПД СМИС – кластер ПАК МЭ Infowatch АРМА Стена К1000, устанавливаемый в МДП Нижнекамск (титул 2012);

– Внутренний межсетевой экран ТСПД СМИС – кластер ПАК МЭ Infowatch АРМА Стена К1000, устанавливаемый в МДП Нижнекамск (титул 2012);

– Сервер управления ПАК МЭ АРМА Стена – Infowatch ARMA Management Console, обеспечивающий централизованное управление МЭ АРМА Стена.

8.4.3.1 Периметровый МЭ ТСПД АСУТП

Кластер периметрового МЭ ТСПД АСУТП включает следующие шлюзы:

– первый узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-021В;

– второй узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-022В.

Периметровый МЭ ТСПД АСУТП терминирует следующие сегменты технологической сети:

– подсети ТМ и СОУ (объектов МДП Нижнекамск, МДП Казань, всех БКТМ);

– подсети СМПО (объектов МДП Нижнекамск, МДП Казань, всех БКТМ);

– подсети АСДУЭ (объектов МДП Нижнекамск, МДП Казань, всех БКТМ);

– подсети КИТСО (объекта МДП Нижнекамск);

– сегмент СОИБ ОКИИ – проектируемый сетевой сегмент с маской 255.255.255.128 (/25), в который устанавливаются серверные компоненты СОИБ ОКИИ, а также управляющие интерфейсы сетевых устройств СОИБ ОКИИ (внешних и внутренних коммутаторов, межсетевых экранов, криптошлюзов).

Шлюзы периметрового МЭ ТСПД АСУТП включаются в сеть следующим образом:

– внешние (outside) интерфейсы подключаются к сетевому оборудованию, подключенному к каналам связи до ЦОД ШК 1.8 (титул 1268) – ДМЗ НКНХ 2025;

– внутренние интерфейсы (логические интерфейсы терминирующихся подсетей) подключаются к стеку внутренних коммутаторов СОИБ ОКИИ.

Управление шлюзами МЭ АРМА Стена К1000 осуществляется централизованно сервером управления Infowatch ARMA Management Console, устанавливаемом на выделенный сервер в проектируемый сегмент СОИБ ОКИИ (МДП Нижнекамск) – НКНХ.5273-0000-С-SRV-023А.

Формирование правил межсетевого экранирования осуществляется на этапе внедрения ПАК МЭ на основе матрицы взаимодействия компонентов защищаемых ОКИИ с другими ОКИИ / внешними системами.

8.4.3.2 Периметровый МЭ ЛСО

Кластер периметрового МЭ ЛСО включает следующие шлюзы:

– первый узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-025В;

– второй узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-026В.

Периметровый МЭ ЛСО терминирует следующие сегменты технологической сети:

– подсети ЛСО (объекта МДП Нижнекамск) при взаимодействии с сегментом ЕДСС.

– шлюзы периметрового МЭ ЛСО включаются в сеть следующим образом:

– внешние (outside) интерфейсы подключаются к сетевому оборудованию ЕДСС;

– внутренние интерфейсы подключаются к сетевому оборудованию (коммутаторам) ЛСО в МДП Нижнекамск.

Управление шлюзами МЭ АРМА Стена К1000 осуществляется локально путем подключения Мобильного АРМ СОИБ ОКИИ к управляющему интерфейсу АРМА Стена К1000.

Формирование правил межсетевого экранирования осуществляется на этапе внедрения ПАК МЭ на основе матрицы взаимодействия компонентов защищаемых ОКИИ с другими ОКИИ / внешними системами.

8.4.3.3 Периметровый МЭ СМИС

Кластер периметровый МЭ СМИС включает следующие шлюзы:

– первый узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-023В;

– второй узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-024В.

Периметровый МЭ СМИС включается в технологические сети СМИС и обеспечивает разграничение доступа при взаимодействии компонентов СМИС с ЕДСС.

Шлюзы периметрового МЭ СМИС включаются в сеть следующим образом:

– внешние (outside) интерфейсы подключаются к сетевому оборудованию ЕДСС;

– внутренние интерфейсы подключаются к сетевому оборудованию (коммутаторам) СМИС в МДП Нижнекамск.

Управление шлюзами МЭ АРМА Стена К1000 осуществляется централизованно сервером управления Infowatch ARMA Management Console, устанавливаемом на выделенный сервер в проектируемый сегмент СОИБ ОКИИ (МДП Нижнекамск) – НКНХ.5273-0000-С-SRV-023А.

Формирование правил межсетевого экранирования осуществляется на этапе внедрения ПАК МЭ на основе матрицы взаимодействия компонентов защищаемых ОКИИ с внешними системами.

8.4.3.4 Внутренний МЭ СМИС

Кластер внутреннего МЭ СМИС включает следующие шлюзы:

– первый узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-027В;

– второй узел кластера МЭ АРМА Стена К1000 НКНХ.5273-0000-С-FW-028В.

Внутренний МЭ СМИС терминирует следующие сегменты технологической сети:

– Подсети СМИС (объекта МДП Нижнекамск) для разграничения сетевого доступа при взаимодействии компонентов СМИС с другими ОКИИ / автоматизированными системами ТСПД.

Шлюзы внутреннего МЭ СМИС включаются в сеть следующим образом:

– внешние и внутренние интерфейсы подключаются к стеку внутренних коммутаторов СОИБ ОКИИ.

Управление шлюзами МЭ АРМА Стена К1000 осуществляется централизованно сервером управления Infowatch ARMA Management Console, устанавливаемом на выделенный сервер в проектируемый сегмент СОИБ ОКИИ (МДП Нижнекамск) – НКНХ.5273-0000-C-SRV-023A.

Формирование правил межсетевого экранирования осуществляется на этапе внедрения ПАК МЭ на основе матрицы взаимодействия компонентов защищаемых ОКИИ с другими ОКИИ.

8.4.3.5 Резервное копирование

Резервное копирование конфигураций осуществляется через консоль управления ARMA Management Console в соответствии с Руководством администратора.

8.4.3.6 Обновление компонентов

Обновление выполняется локально Администратором СОИБ ОКИИ, ПО для обновления необходимо запрашивать у службы технической поддержки производителя МЭ. Обновление МЭ может занять длительное время, рекомендуется планировать установку обновлений в технологические остановы.

Обновление базы сигнатур осуществляется в ручном режиме по мере поставки обновлений производителем МЭ. Файл обновления размещается в личном кабинете Заказчика и устанавливается путем загрузки на МЭ в настройках операций с сервером. Обновление базы сигнатур необходимо осуществлять не реже, чем 1 раз в неделю.

8.4.4 Описание комплекса ТС подсистемы

Производительность и технические характеристики ПАК МЭ ПАК МЭ InfoWatch ARMA Стена К1000 представлены в Таблица 8.7.

Таблица 8.7 – Технические характеристики ПАК МЭ InfoWatch ARMA Стена К1000

Параметр	Описание
Процессор	Intel Xeon D-1537
ОЗУ	32Гб DDR4
Пропускная способность режим МЭ	1 Гбит/с
Пропускная способность режим МЭ + СОВ (EMIX трафик)	300 Мбит/с
Габариты (Ш х Г х В), мм	420x290x43,7

8.4.5 Сведения о сертификатах

ПАК МЭ InfoWatch ARMA Industrial Firewall имеет сертификат ФСТЭК России № 4429 от 27.07.2021 г. по 27.07.2026 г. на соответствие требованиям документов: Требования доверия (4), Требования к МЭ, Профиль защиты МЭ (Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ).

8.4.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в Таблица 8.8.

Таблица 8.8 – Используемые для взаимодействия сетевые порты

Название сервиса / номер порта	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
TCP/443	Доступ администратора к веб-консоли управления МЭ АРМА Стена	АРМ Администратора СОИБ ОКИИ	МЭ АРМА Стена
TCP/22	Доступ администратора к интерфейсу командной строки (CLI) МЭ АРМА Стена по протоколу SSH	АРМ Администратора СОИБ ОКИИ	МЭ АРМА Стена
TCP/514 (Syslog) UDP/514 (Syslog)	Передача событий безопасности в SIEM	МЭ АРМА Стена	SIEM

8.5 Подсистема антивирусной защиты

8.5.1 Общие положения

Подсистема антивирусной защиты в составе СОИБ ОКИИ предназначена для защиты АРМ и серверов ОКИИ от вредоносного ПО с использованием следующих технологий:

– сигнатурный анализ;

– сканирование процесса/службы во время обращения;

– сканирование памяти;

– обнаружение шифровальщиков (ransomware);

– учет машинных носителей информации;

– контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;

– контроль подключения съемных машинных носителей информации.

8.5.2 Функциональные возможности подсистемы

Подсистема АВЗ обеспечивает реализацию следующих мер обеспечения безопасности объекта КИИ:

– ЗНИ.1 Учет машинных носителей информации;

– ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;

– ЗНИ.7 Контроль подключения съемных машинных носителей информации;

– АУД.3 Генерирование временных меток и (или) синхронизация системного времени;

– АУД.4 Регистрация событий безопасности;

– АВЗ.1 Реализация антивирусной защиты;

– АВЗ.4 Обновление базы данных признаков вредоносных компьютерных программ (вирусов);

– ОЦЛ.1 Контроль целостности программного обеспечения;

– ЗИС.3 Эшелонированная защита информационной (автоматизированной) системы.

ПО KICS for Nodes обеспечивает выполнение следующих функций:

– обнаружение фактов вирусного заражения средств защиты АСУ при выполнении по запросам пользователей и/или администраторов периодических проверок оперативной памяти, локальных носителей информации, томов, каталогов, файлов, файлов, получаемых по каналам связи;

– обнаружение фактов вирусного заражения, вызванного известными вирусами;

– сигнализация в случае обнаружения фактов вирусного заражения средствами службы сообщений (для пользователей) и средствами службы сообщений, запуска исполняемого файла или по электронной почте для администраторов подсистемы;

– обнаружение вирусов в таких объектах, как архивы, компрессированные исполняемые модули, динамические библиотеки и др.;

– удаление программного кода вируса из объектов, в которых он был обнаружен (Администратором подсистемы в «ручном режиме»);

– удаление файлов, в которых обнаружены вирусы (Администратором подсистемы совместно с Администратором ИБ в «ручном режиме»);

– блокирование доступа к отчуждаемым носителям информации в случае обнаружения фактов вирусного заражения и (или) активизации вируса;

– контроля регистрации и использования запоминающих устройств в целях защиты компьютера от угроз безопасности;

– периодическое обновление антивирусных средств (механизмов обнаружения и удаления, расширение списка известных вирусов и алгоритмов поиска и удаления

неизвестных вирусов). Обновление версий ПО антивирусной защиты допускается при наличии официального подтверждения возможности такого обновления от производителя (поставщика) АСУ;

– протоколирование результатов работы и действий эксплуатирующего персонала;

– контроля целостности передаваемой информации между компонентами антивирусных средств посредством механизма контрольных сумм.

8.5.3 Структура подсистемы

Подсистема антивирусной защиты включает следующие компоненты:

– ПО KICS for Linux Nodes, устанавливаемое на АРМ и серверы защищаемых ОКИИ под управлением ОС семейства Linux;

– ПО KICS for Nodes, устанавливаемое на АРМ и серверы защищаемых ОКИИ под управлением ОС семейства Windows;

– ПО Kaspersky Endpoint Security, устанавливаемое на серверы СОИБ ОКИИ;

– ПО централизованного управления Kaspersky Security Center (KSC), устанавливаемое в сегменте СОИБ ОКИИ на выделенный сервер.

Компоненты, на которые устанавливается клиентское ПО KICS for Nodes, указаны в Таблица 8.9.

Таблица 8.9 – Защищаемые подсистемой антивирусной защиты компоненты ОКИИ

№ п/п	ОКИИ	Площадка	Объект защиты	Компонент
1	АСУТП	МДП Нижнекамск (2012)	Сервер АСУТП	KICS for Nodes
2	АСУТП	МДП Нижнекамск (2012)	Сервер СМПО	KICS for Nodes
3	АСУТП	МДП Нижнекамск (2012)	Сервер АСДУЭ (1)	KICS for Linux Nodes
4	АСУТП	МДП Нижнекамск (2012)	Сервер АСДУЭ (2)	KICS for Linux Nodes
5	АСУТП	МДП Нижнекамск (2012)	Сервер АСДУЭ (3)	KICS for Linux Nodes
6	АСУТП	МДП Нижнекамск (2012)	Сервер АСДУЭ (4)	KICS for Linux Nodes
7	АСУТП	МДП Нижнекамск (2012)	Сервер АСДУЭ (5)	KICS for Linux Nodes
8	КИТСО	МДП Нижнекамск (2012)	Сервер КИТСО	KICS for Linux Nodes
9	АСУТП	МДП Нижнекамск (2012)	Сервер СМИС (1)	KICS for Linux Nodes
10	АСУТП	МДП Нижнекамск (2012)	Сервер СМИС (2)	KICS for Linux Nodes
11	АСУТП	АБК Нижнекамск (2060)	АРМ АСУТП (1)	KICS for Nodes
12	АСУТП	АБК Нижнекамск (2060)	АРМ АСУТП (2)	KICS for Nodes
13	АСУТП	АБК Нижнекамск (2060)	АРМ АСУТП (3)	KICS for Nodes
14	АСУТП	АБК Нижнекамск (2060)	АРМ СМПО	KICS for Nodes
15	АСУТП	АБК Нижнекамск (2060)	Мобильный АРМ инженера АСУТП	KICS for Nodes
16	АСУТП	АБК Нижнекамск (2060)	АРМ АСДУЭ (1)	KICS for Nodes
18	АСУТП	АБК Нижнекамск (2060)	Мобильный АРМ инженера АСДУЭ	KICS for Nodes
19	КИТСО	АБК Нижнекамск (2060)	АРМ КИТСО	KICS for Nodes

№ п/п	ОКИИ	Площадка	Объект защиты	Компонент
20	АСУТП	АБК Нижнекамск (2060)	АРМ СМИС	KICS for Nodes
21	ЛСО	АБК Нижнекамск (2060)	АРМ ЛСО	KICS for Nodes
22	АСУТП	МДП Казань (1012)	Мобильный АРМ инженера АСУТП	KICS for Nodes
23	АСУТП	МДП Казань (1012)	АРМ АСУТП (1)	KICS for Nodes
24	АСУТП	МДП Казань (1012)	АРМ АСУТП (2)	KICS for Nodes
25	АСУТП	МДП Казань (1012)	АРМ АСУТП (3)	KICS for Nodes
26	АСУТП	МДП Казань (1012)	АРМ АСУТП (4)	KICS for Nodes
27	АСУТП	МДП Казань (1012)	АРМ АСДУЭ (1)	KICS for Nodes
28	АСУТП	МДП Казань (1012)	АРМ АСДУЭ (2)	KICS for Nodes
29	ЛСО	МДП Казань (1012)	АРМ ЛСО	KICS for Nodes
30	СОИБ	МДП Нижнекамск (2012)	Мобильный АРМ СОИБ ОКИИ	Kaspersky Endpoint security (Windows)
31	СОИБ	МДП Нижнекамск (2012)	Сервер сбора и обработки событий ИБ KUMA (SIEM)	Kaspersky Endpoint security (Linux)
32	СОИБ	МДП Нижнекамск (2012)	Сервер управления С-терра КП	Kaspersky Endpoint security (Windows)
33	СОИБ	МДП Нижнекамск (2012)	Сервер управления МЭ АРМА	Kaspersky Endpoint security (Windows)
34	СОИБ	МДП Нижнекамск (2012)	Сервер контроля конфигураций	Kaspersky Endpoint security (Linux)
35	СОИБ	МДП Нижнекамск (2012)	Сервер Кибербекап	Kaspersky Endpoint security (Linux)
36	СОИБ	МДП Нижнекамск (2012)	Сервер управления KSC	Kaspersky Security Center

На изолированных АРМ и серверах управление политиками безопасности KICS for Nodes осуществляется локально Администратором СОИБ ОКИИ. АРМ и серверы, имеющие сетевой доступ к создаваемому сегменту СОИБ ОКИИ в МДП Нижнекамск, управляются централизованно сервером управления с установленным ПО Kaspersky Security Center, который обеспечивает выполнение следующих функций:

– удаленная централизованная установка ПО KICS for Nodes на компьютеры;

– управление политиками и задачами на группах АРМ и серверов;

– управление лицензиями, отслеживание выполнения лицензионного соглашения и срока его окончания;

– удаленное централизованное управление ПО KICS for Nodes, KES, функционирующим на серверах и АРМ;

– отслеживание распространения обновлений на серверы и АРМ;

– отправка обновлений сигнатурных баз на клиентское ПО Kaspersky Endpoint Security, KICS for Nodes;

– централизованный сбор статистики о работе клиентского ПО KICS for Nodes;

– формирование отчетности;

– аутентификация администрирующего персонала по логину и паролю условно-постоянного действия;

– разграничение доступа к управляющим функциям подсистемы.

8.5.3.1 Резервное копирование

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования следует восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center.

Резервная копия данных Сервера администрирования создается одним из следующих способов:

– создать и запустить задачу резервного копирования данных через Консоль администрирования;

– запустить утилиту klbackup на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке программы.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

– база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);

– конфигурационная информация о структуре групп администрирования и клиентских устройствах;

– хранилище дистрибутивов программ для удаленной установки;

– сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

8.5.3.2 Обновление компонентов

Для поддержания защиты компонентов в актуальном состоянии выбрана централизованная схема получения обновлений, состоящая из следующих этапов:

– загрузка пакетов обновлений в хранилище сервера администрирования KSC с сетевой папки КСПД;

– распространение необходимых пакетов обновлений с сервера KSC на соответствующие серверы и АРМ/серверы АСУТП в соответствии установленной программой безопасности;

– обновление модулей программы/установка критичных исправлений следует проводить в ручном режиме в период технологических останов. Порядок действий при обновлении модулей аналогична установке/удалению программы.

– Для использования установленных программных модулей требуется перезагрузка защищаемого устройства и / или перезапуск ПО KICS for Nodes.

8.5.4 Описание комплекса ТС подсистемы

Требования к производительности АРМ / серверов для установки компонентов подсистемы антивирусной защиты представлены в Таблица 8.10.

Таблица 8.10 – Требования к ТС подсистемы антивирусной защиты

№ п/п	Наименование компонента	Аппаратные требования			
		CPU	RAM	HDD	Сеть
1	Сервер администрирования KSC	x32 - 1 ГГц x64 - 1,4 Ггц	6 Гб	160 ГБ	1x1 Гбит/с
2	Агент администрирования KSC	x32 - 1 ГГц x64 - 1,4 Ггц	512 МБ	1 ГБ	1x1 Гбит/с
3	KICS for Nodes	1xCPU 1,4 ГГц	x32 – 512 МБ x64 - 1 ГБ	3,5 ГБ	1x1 Гбит/с

8.5.5 Сведения о сертификатах

Kaspersky Industrial CyberSecurity for Nodes имеет сертификат ФСТЭК №3907 от 03.04.2018, действительный по 03.04.2026 на соответствие требованиям: Требования доверия (3), Требования к САВЗ, Профиль защиты САВЗ (В третьего класса защиты. ИТ.САВЗ.В3.ПЗ), ЗБ.

Kaspersky Security Center имеет сертификат ФСТЭК №3155 от 06.05.2014, действительный по 06.05.2025 на соответствие требованиям: Требования доверия (2), Требования к САВЗ, Профиль защиты САВЗ (А второго класса защиты. ИТ.САВЗ.А2.ПЗ), ЗБ.

Kaspersky Endpoint Security для Linux имеет сертификат ФСТЭК №2534 от 27.12.2011, действительные по 27.12.2025 на соответствие требованиям: Требования доверия(2), Требования к САВЗ, Профиль защиты САВЗ(Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ), Профиль защиты САВЗ(В второго класса защиты. ИТ.САВЗ.В2.ПЗ), Профиль защиты САВЗ(Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ).

8.5.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в Таблица 8.11.

Таблица 8.11 – Используемые для взаимодействия сетевые порты

Название сервиса / номер порт	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
TCP/13000	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов	Агент администрирования	Сервер KSC
TCP/13291	Управление Сервером администрирования	Консоль администрирования	Сервер KSC

Название сервиса / номер порт	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
UDP/15000	Управление клиентскими устройствами (сигналы управления от Сервера администрирования)	Сервер KSC	Агент администрирования
TCP/123 (NTP), UDP/123 (NTP)	Синхронизация времени с NTP-сервером	Сервер KSC	Сервер точного времени
Определяется на этапе внедрения	Загрузка обновления	Сервер KSC	Сервер в КСПД

8.6 Подсистема анализа защищенности

8.6.1 Общие положения

Подсистема анализа защищенности предназначена для периодического инструментального анализа компонентов ОКИИ на наличие известных уязвимостей. Подсистема обеспечивает выявление уязвимостей на контролируемых сетевых узлах и обеспечивает сбор информации о настройках параметров безопасности контролируемых узлов, а также прочих конфигурационных параметров, некорректная настойка которых может привести к снижению защищенности контролируемых узлов.

8.6.2 Функциональные возможности подсистемы

Подсистема анализа защищенности обеспечивает выполнение функций, требуемых для реализации следующих мер обеспечения безопасности объекта КИИ:

- АУД.1 Инвентаризация информационных ресурсов;
- АУД.2 Анализ уязвимостей и их устранение.

XSpider 7.8 осуществляет сбор, в том числе, следующей информации о конфигурации актива: версия и производитель ОС, установленные обновления ОС, список установленного ПО, настройки ОС и ПО, пользователи и группы пользователей, аппаратное обеспечение, запущенные сетевые сервисы и службы ОС, настройки сети, настройки средств защиты.

Реализованы следующие модули для сбора событий в составе подсистемы анализа защищенности:

- Endpoint Monitor – активный сбор событий файловой системы;
- Filemonitor – активный сбор событий из текстовых файлов;
- Hostdiscovery – поиск узлов методами ICMP ping, TCP ping;
- Netflow – пассивный сбор событий по протоколу NetFlow;
- Networksensor-Manager – пассивный сбор событий о соединениях;
- Networkwatch – активный сбор событий о доступности узлов и сервисов;
- Odbclog – активный сбор событий из таблиц СУБД;
- Pentest – сканирование актива методом черного ящика;

– SAP RFC – активный сбор событий с сервера SAP на базе SAP NetWeaver ABAP;

– Snmptrapcollector – активный сбор событий по протоколу SNMP;

– Sshеventcollector – активный сбор событий из файлов по протоколу SSH;

– Syslog – пассивный сбор событий по протоколу Syslog;

– vSphereEventCollector – активный сбор событий платформы виртуализации VMware;

– vSphere;

– Webengine – сканирование веб-приложения;

– Windows File log – активный сбор событий из файлов Microsoft Windows;

– Wineventlog – активный сбор событий Windows Event log;

– Wmilog – активный сбор событий Windows Event Log через WMI;

– Wminotification – активный сбор событий WMI-классов по протоколу WMI;

– CustomEventCollector – запуск пользовательского сценария сбора событий, реализованного в виде исходного кода на языке Python;

– Remote Executor – удаленное исполнение сценариев одновременно на нескольких узлах и сбор результатов их выполнения.

8.6.3 Структура подсистемы

Подсистема реализуется на базе программного комплекса XSpider 7.8, установленного на Мобильный АРМ СОИБ ОКИИ, обеспечивающего сканирование доступных узлов из сегмента СОИБ ОКИИ, в том числе серверов СОИБ ОКИИ.

Мобильный АРМ для проведения сканирования устанавливается в сканируемые сетевые сегменты (подсети) ТСПД на время проведения сканирования. По результатам проведения сканирования мобильное АРМ подключается в сегмент СОИБ ОКИИ и отправляет результаты сканирования на сервер подсистемы регистрации и обработки событий безопасности (SIEM).

К сканируемым узлам относятся:

– серверы управления ОКИИ;

– АРМ операторов/инженеров ОКИИ;

– серверы СОИБ ОКИИ.

Контроль защищенности возможен вручную путем анализа известных уязвимостей для используемых версий системного ПО.

Анализ защищенности контролируемых узлов производится при сканировании в различных режимах с целью выявления уязвимостей, которые могут эксплуатироваться как внешним нарушителем, так и нарушителем, имеющим полный или ограниченный доступ к ОС или прикладному ПО контролируемого узла.

8.6.3.1 Резервное копирование

Резервное копирование и восстановление компонентов подсистемы осуществляется с помощью подсистемы резервного копирования путем создание полного образа диска ОС.

8.6.3.2 Обновление компонентов

Для корректной работы системы автоматического обновления необходимо наличие соединения с сервером обновлений (update.maxpatrol.com). Для обновления необходимо переключиться на закладку «Настройки – Основные» и нажать кнопку «Обновить» в панели «Обновления».

Внимание! В ходе обновления консоль потеряет соединения с сервером и в течение некоторого времени (одной-двух минут) не сможет подключиться к системе.

Запуск синхронизации обновлений осуществляется администратором.

8.6.4 Описание комплекса ТС подсистемы

Подсистема анализа защищенности представлена на объектах Мобильным АРМ СОИБ ОКИИ. Технические характеристики мобильного АРМ представлены в Таблица 8.12.

Таблица 8.12 – Характеристики мобильного АРМ

Параметр	Значение
Процессор	Один процессор Intel Core i5-1235U 1.3-4.4 ГГц / 10 ядер 12 потоков
Оперативное запоминающее устройство	16 ГБ DDR4
Накопители	SDD M.2 512GB
Сетевые интерфейсы	Один адаптер 1Gb RJ45 Wi-Fi 802.11 ax
Экран	15.6" Full HD 1920x1080 IPS

8.6.5 Сведения о сертификатах

ПО Сетевой сканер безопасности XSpider 7.8.25 имеет сертификат ФСТЭК России № 3247 от 24.10.2014 г. по 24.10.2025 г. на соответствие требованиям РД НДВ (4), ТУ.

8.6.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в Таблица 8.13.

Таблица 8.13 – Используемые для взаимодействия сетевые порты

Название сервиса/ номер порт	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
TCP/1024-65535	Сканирование, в зависимости от типа объекта	Мобильный АРМ СОИБ ОКИИ	Объект сканирования

Название сервиса/ номер порт	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
TCP/2002	Загрузка обновления/активация	Мобильный АРМ СОИБ ОКИИ	Соединение с сервером обновлений/активации

8.7 Подсистема регистрации и обработки событий безопасности

8.7.1 Общие положения

Подсистема регистрации и обработки событий безопасности предназначена для автоматизации и централизации процессов сбора, хранения, преобразования и выдачи пользователям информации об объектах информационной инфраструктуры и событиях ИБ в рамках этой инфраструктуры, автоматизации процесса выявления инцидентов ИБ и управления ими.

8.7.2 Функциональные возможности подсистемы

Подсистема обеспечивает выполнение функций, требуемых для реализации следующих мер обеспечения безопасности объекта КИИ:

– АУД.3 Генерирование временных меток и (или) синхронизация системного времени;

– АУД.4 Регистрация событий безопасности;

– АУД.6 Защита информации о событиях безопасности;

– АУД.7 Мониторинг безопасности;

– АУД.8 Реагирование на сбои при регистрации событий безопасности;

– ИНЦ.1 Выявление компьютерных инцидентов;

– ИНЦ.2 Информирование о компьютерных инцидентах;

– ИНЦ.3 Анализ компьютерных инцидентов;

– ИНЦ.6 Хранение и защита информации о компьютерных инцидентах.

Подсистема регистрации и обработки событий безопасности выполняет следующие функции:

– прием и обработка событий, передаваемых с использованием определенного протокола (UDP, TCP, NetFlow), а также от определенных типов источников модулей сбора (OSSEC, Beats) и транспортов (Syslog, JDBC, SNMP);

– хранение событий безопасности и выполнение поисковых запросов в сохраненных событиях;

– обеспечение возможности поиска данных через единую консоль в иерархической структуре для каждой из подчиненных инсталляций Платформы: поиск по событиям, которые хранятся в подчиненных компонентах;

– визуализация полученных результатов от поисковых запросов;

– учет узлов, объектов, контактов и другой информации о сети и обогащение поступающих событий безопасности тегами;

– выявление в наборах поступающих событий безопасности тех из них, на которые требуется обратить внимание (признаков инцидентов) в соответствии с заданными правилами;

– запись сведений о выявленных событиях (признак инцидента), обогащение событий дополнительной информацией, необходимой для приоритезации работы над выявленными признаками;

– автоматизированное выявление и учет подозрений на инцидент ИБ, сведений об ИТ-активах и осуществление операций мониторинга;

– расследование и реагирование на инциденты ИБ персоналом, выполняющим функции аналитиков ИБ.

8.7.3 Структура подсистемы

Подсистема регистрации и обработки событий безопасности реализуется на базе программного обеспечения Kaspersky Unified Monitoring and Analysis Platform (KUMA), которая включает следующие компоненты:

– сервер сбора и анализа событий безопасности KUMA в инсталляции все-в-одном, устанавливаемый в сегмент СОИБ ОКИИ.

Сервер сбора и анализа событий безопасности KUMA включает следующие компоненты:

– модуль сбора данных «Коллектор» и KUMA «Agent»;

– модуль анализа данных (на базе компонента KUMA «Коррелятор»);

– модуль хранения данных (на базе компонента KUMA «Хранилище»);

– модуль централизованного управления (на базе компонента KUMA «Ядро»).

Модуль сбора данных предназначена для получения предопределенных данных с целевых ресурсов, их первоначальной фильтрации, нормализации, агрегации, обогащения и последующей пересылки в подсистему анализа данных и/или в подсистему хранения данных.

Модуль анализа данных предназначена для корреляционного анализа собранных событий, их обработки и отправки обработанных событий на долговременное хранение в подсистему хранения данных.

Модуль хранения данных предназначена для долгосрочного хранения базовых событий и событий ИБ с возможностью настройки политик хранения и поиска информации.

Модуль централизованного управления предназначена для визуализации данных мониторинга, управления подсистемами сбора, анализа и хранения данных, управления правами и учетными записями, а также предоставляет графический пользовательский интерфейс для работы с событиями и инцидентами ИБ.

8.7.3.1 Модуль KUMA Agent

KUMA «Agent» используются для пересылки необработанных событий с серверов и рабочих станций (или других систем-источников) в KUMA «Коллектор».

Возможности по сбору необработанных событий:

– wmi – используются для получения данных с удаленных компьютеров под управлением ОС Windows с помощью Windows Management Instrumentation. Устанавливается на устройства под управлением ОС Windows;

– wec – используются для получения журналов Windows с локальных компьютеров с помощью Windows Event Collector. Устанавливается на устройства под управлением ОС Windows;

– file – используются для получения данных из файла. Устанавливается на устройства под управлением ОС Linux.

KUMA «Agent» может осуществлять активный сбор событий с систем-источников. Алгоритм работы компонента:

– программа осуществляет сетевое соединение с системой-источником либо устанавливается локально на систему-источник событий.

– после соединения в зависимости от типа системы-источника программа осуществляет сбор доступных событий.

После сбора событий программа осуществляет перенаправление этих событий в KUMA «Коллектор» в том же виде, в котором они получены программой.

8.7.3.2 Модуль KUMA Коллектор

KUMA «Коллектор» предназначен для:

– активного сбора необработанных («сырых») событий;

– пассивного сбора «сырых» событий;

– обработки событий (нормализация, фильтрация, агрегация, обогащение);

– отправки нормализованных событий в KUMA «Коррелятор» и KUMA «Хранилище» или во внешние системы.

Алгоритм работы KUMA «Коллектор» следующий:

– Получение сообщений из систем-источников:

  ○ в случае пассивного сбора программа осуществляет прослушивание назначенного сетевого порта в ожидании получения сообщений;

– в случае активного сбора программа осуществляет сетевое соединение с системой-источником.

– парсинг и нормализация событий: полученные события обрабатываются с помощью парсера и правил нормализации;

– фильтрация нормализованных событий: позволяет отбирать для дальнейшей обработки только события, удовлетворяющие заданным условиям. События, не

удовлетворяющие условиям фильтрации, на этом этапе отсеиваются и далее не обрабатываются;

– агрегация нормализованных событий: позволяет уменьшить количество схожих сообщений, передаваемых в KUMA «Коррелятор» и/или KUMA «Хранилище» или другие внешние системы с помощью правил агрегации;

– обогащение и преобразование нормализованных событий позволяет дополнить содержащуюся в событии информацию данными из внутренних и внешних источников или изменить формат и содержимое полей события. В программе представлены следующие источники обогащения:

o constant: добавляет в поле события константное значение (заданное заранее);

o cybertrace: добавляет в событие сведения из потоков данных CyberTrace;

o dictionary: добавляет в поле события сведения из словаря;

o dns: используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот;

o event: добавляет в поле события значение другого поля события;

o template: добавляет в поле события значение на основании шаблона «Go»;

o LDAP: добавляет в поле события сведения о учетной записи пользователя из LDAP;

– передача нормализованных событий: по завершении всех этапов обработки событие отправляется в настроенные точки назначения.

8.7.3.3 Модуль KUMA Коррелятор

KUMA «Коррелятор» предназначен для:

– анализа нормализованных и корреляционных событий;

– выявления событий ИБ и создания алертов;

– отправки событий корреляции в настроенные точки назначения.

Алгоритм работы KUMA «Коррелятор» следующий:

– получение нормализованного события из KUMA «Коллектор».

– применение правил корреляции, которые можно настроить на срабатывание на основе одного события или последовательности событий. Если по правилам корреляции не было выявлено событие ИБ, обработка события завершается.

– реагирование на обнаружение события ИБ:

o обогащение события;

o операции с активными листами;

o отправка уведомлений;

o сохранение корреляционного события;

o управление категориями устройства;

– передача событий корреляции: по завершении всех этапов событие отправляется в настроенные точки назначения (в том числе в хранилище KUMA Хранилище).

8.7.3.4 Модуль KUMA Хранилище

KUMA «Хранилище» используется для хранения нормализованных событий и событий корреляции таким образом, чтобы обеспечить к ним быстрый и бесперебойный доступ из KUMA «Ядро» с целью извлечения аналитических данных. Скорость и бесперебойность доступа обеспечиваются за счет использования нереляционной высокопроизводительной базы данных. Таким образом, хранилище – это база данных, связанная с сервисом хранилища KUMA.

Алгоритм работы KUMA «Хранилище» следующий:

– получение нормализованного события из KUMA «Коллектор» или события корреляции из KUMA «Коррелятор».

– сохранение события в структуре базы данных.

– получение запроса от KUMA «Ядро» на предоставление данных по заданным критериям.

– поиск данных.

– предоставление данных KUMA «Ядро».

8.7.3.5 Модуль KUMA Ядро

KUMA «Ядро» – это центральный компонент подсистемы. Предоставляемый KUMA «Ядро» графический пользовательский веб-интерфейс предназначен как для повседневного использования операторами и аналитиками, так и для настройки подсистемы в целом.

Ядро позволяет выполнять следующие задачи:

– централизованное управление подсистемы;

– настройка компонентов подсистемы;

– работа с контентными ресурсами подсистемы: правилами корреляции, агрегации, обогащения и реагирования, нормализаторами, коннекторами;

– визуализация информации из базовых событий и событий ИБ;

– расследование угроз безопасности на основе получаемых событий;

– мониторинг состояния компонентов подсистемы.

8.7.4 Описание комплекса ТС подсистемы

Подсистема регистрации и обработки событий безопасности рассчитана на хранение событий сроком до 6 мес.

Расчёт производительности сервера KUMA с учётом планируемого состава и количества компонентов ОКИИ, а также с учётом резерва мощности для возможности увеличения количества подключаемых источников, производительность компонентов Подсистемы рассчитана на 1000 EPS.

Требования к ТС для установки компонентов Платформы представлены в Таблица 8.14.

Таблица 8.14 – Требования к компонентам подсистемы регистрации и обработки событий безопасности

Компонент	Параметр	Системные требования
Сервер KUMA (до 1000 EPS)	ОС	– Oracle Linux 8.6, 8.7, 9.2. – Astra Linux Special Edition РУСБ.10015-01 (2021-1126SE17 оперативное обновление 1.7.1). – Astra Linux Special Edition РУСБ. 10015-01 (2022-1011SE17MD оперативное обновление 1.7.2.UU.1). – Astra Linux Special Edition РУСБ.10015-01 (2022-1110SE17 оперативное обновление 1.7.3). Требуется версия ядра 5.15.0.33 или выше. – Astra Linux Special Edition РУСБ.10015-01 (2023-0630SE17MD срочное оперативное обновление 1.7.4.UU.1).
	Процессор	– 16 ядер (vCPU)
	Оперативная память	– 32 ГБ
	Жесткий диск	– OS: 480Gb SSD; – Hot data: 2 x 1.92Tb SSD; – Warm data: 2 x 10Tb SAS
	Сетевой интерфейс	– 1Gbps

8.7.5 Сведения о сертификатах

ПО Kaspersky Unified Monitoring and Analysis Platform имеет сертификат ФСТЭК России № 4455 от 28.09.2021 г. по 28.09.2026 г. на соответствие требованиям доверия (4), ТУ.

8.7.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в следующей Таблица 8.15.

Таблица 8.15 – Используемые для взаимодействия сетевые порты

Название сервиса / номер порт	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
SMTP TCP/25	Уведомление о событии по электронной почте	Сервер KUMA	Почтовый сервер
TCP/514 UDP/514	Сбор с источников событий, направляющих по протоколу syslog	Источник событий Syslog	Сервер KUMA
TCP/5985	Сбор событий Windows с использованием WEC	Источники Windows Event Collector	Сервер KUMA
TCP/123 (NTP), UDP/123 (NTP)	Синхронизация времени с NTP-сервером	Сервер KUMA	Сервер точного времени

8.8 Подсистема контроля конфигураций

8.8.1 Общие положения

Подсистема контроля конфигураций предназначена для выполнения следующих задач:

– контроль изменения конфигураций сетевого оборудования;

– контроль изменения конфигураций МЭ;

– проверки соответствия безопасности сетевого оборудования;

– проверки соответствия безопасности МЭ;

– моделирование трафика на основе маршрутов и правил МЭ.

– контроль изменения конфигураций ОС, виртуализации, контейнеров и прикладного программного обеспечения (ППО);

– контроль целостности файлов ОС, виртуализации, контейнеров и ППО;

– проверки соответствия безопасности ОС, виртуализации, контейнеров и ППО.

8.8.2 Функциональные возможности подсистемы

Подсистема контроля конфигураций обеспечивает выполнение функций, требуемых для реализации следующих мер обеспечения безопасности объекта КИИ:

– АУД.4 Регистрация событий безопасности;

– АУД.9 Анализ действий отдельных пользователей;

– ОЦЛ.1 Контроль целостности программного обеспечения;

– ОЦЛ.2 Контроль целостности информации;

– ОДТ.3 Контроль безотказного функционирования средств и систем;

– УКФ.2 Управление изменениями;

– УКФ.4 Контроль действий по внесению изменений.

ПК «Efros DO» реализует следующие функциональные возможности:

– единая точка доступа (веб-интерфейс) к функциям комплекса и модулям интеграции;

– получение, обработка, интеграция и хранение данных, полученных из событий по объектам защиты в ПК «Efros DO»;

– инвентаризация и ведение единого списка объектов защиты;

– топология сети;

– мониторинг уведомлений о событиях контроля и об ошибках с объектами защиты;

– мониторинг состояния объектов защиты, подключенных к системе, в графическом и текстовом виде;

– формирование отчетов событий по объектам защиты для модулей интеграции;

– ведение журнала системных событий;

– администрирование и настройка ПК «Efros DO»;

– идентификация и аутентификация администраторов комплекса на сервере ПК «Efros DO» с использованием идентификаторов и паролей;

– ведение списка администраторов комплекса с возможностью управления пользователями (добавление пользователей, групп пользователей, блокировка, активация, деактивация, удаление учетной записи пользователя, смена пароля пользователя);

– ролевое и дискреционное разграничение доступа пользователей комплекса к серверу ПК «Efros DO», к списку контролируемых на сервере объектов защиты;

– передача событий безопасности для дальнейшей обработки (SIEM-системы);

– импорт сущностей из сторонних систем согласно заданному шаблону в формате .csv;

– управление ролями пользователей комплекса;

– построение иерархии серверов;

– функции модуля контроля конфигураций и топологии сети «Efros NA»;

– функции модуля контроля целостности и проверки соответствия хостов и конечных точек «Efros ICC».

8.8.3 Структура подсистемы

Подсистема контроля конфигураций реализуется программным комплексом Efros Defence Operations (Efros DO), устанавливаемым на выделенный сервер НКНХ.5273-0000-С-SRV-022A, размещаемый в сегменте СОИБ ОКИИ, включающий следующие программные модули:

– модуль контроля целостности и проверки соответствия хостов и конечных точек «Efros Integrity Check Compliance (Efros ICC)»;

– модуль контроля конфигураций и топологии сети «Efros Network Assurance (Efros NA)»;

– Windows-агент ПК «Efros DO»;

– агент ПК «Efros DO» для ОС Windows;

– агент ПК «Efros DO» для ОС РЕД ОС;

– агент ПК «Efros DO» для ОС Astra Linux Special Edition или ОС Ubuntu.

8.8.3.1 Резервное копирование

Резервное копирование и восстановление компонентов подсистемы осуществляется с помощью подсистемы резервного копирования путем создания полного образа системного диска ОС.

8.8.3.2 Обновление компонентов

Обновление ПК «Efros DO» осуществляется после предоставления нового дистрибутива разработчиком.

8.8.4 Описание комплекса ТС подсистемы

Сервер управления ПО Efros DO устанавливается на выделенный сервер, системные требования представлены в Таблица 8.16.

Таблица 8.16 – Системные требования для установки Сервера управления ПО Efros DO

Параметр	Описание
Операционная система	– Astra Linux Special Edition (v.1.7), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.), поддерживается установка на ОС с ядром 5.15-Generic; – Альт Server 10; – РЕД ОС (v. 7.3), сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)
Поддерживаемые системы управления базами данных (СУБД)	– СУБД PostgreSQL 13; – СУБД «Jatoba» (поддерживается версия «ядра» 4)
Прикладное программное обеспечение	– Docker v. 18.03.0 и выше; – Docker-compose v. 2.9.0; – Confluent Kafka v. 5.5.0; – СУБД OpenSearch v. 1.3.7; – СУБД MinIO v. 220218
Процессор	16 ядер (от 2 ГГц)
Оперативная память	от 32 Гб
Жесткий диск (свободное пространство)	от 600 Гб
Сетевая карта	1 Гбит/с

Агентское ПО Efros DO устанавливается на АРМ и серверы под управлением ОС семейства Windows, Linux, системные требования представлены в Таблица 8.17.

Таблица 8.17 – Системные требования для установки Агентского ПО Efros DO

Параметр	Описание
Windows-агент	
Операционная система	Windows*
Процессор	1,6 ГГц
Оперативная память	1 Гб
Жесткий диск	100 Мб
Агент ПК «Efros DO»	
Операционная система	– Windows* (поддерживается только 64-разрядная версия ОС); – РЕД ОС (рабочая станция, сервер) (7.3 и выше); – Astra Linux Special Edition (1.6 и выше); – Ubuntu (22.04 и выше); – MacOS Monterey (12.6 и выше) x86_64
Процессор	Минимальные требования к производительности рабочей станции, на

Параметр	Описание
Оперативная память	которую устанавливается агент ПК «Efros DO», обусловлены требованиями используемой ОС
Жесткий диск	
Windows*	– Windows Server 2008R2 Foundation Edition SP1 (64-разрядная); – Windows Server 2008R2 Standard Edition SP1 (64-разрядная); – Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная); – Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная); – Windows Server 2012/2012R2 Foundation (64-разрядная); – Windows Server 2012/2012R2 Essentials (64-разрядная); – Windows Server 2012/2012R2 Standard (64-разрядная); – Windows Server 2012/2012R2 Datacenter (64-разрядная); – Windows Server 2016 Standard (64-разрядная); – Windows Server 2016 Datacenter (64-разрядная); – Windows Server 2016 Essentials (64-разрядная); – Windows Server 2019 Standard (64-разрядная); – Windows Server 2019 Datacenter (64-разрядная); – Windows Server 2019 Essentials (64-разрядная); – Windows 7 Professional SP1 (32-разрядная/64-разрядная); – Windows 7 Enterprise SP1 (32-разрядная/64-разрядная); – Windows 7 Ultimate SP1 (32-разрядная/64-разрядная); – Windows 8.1 Core (32-разрядная/64-разрядная); – Windows 8.1 Professional (32-разрядная/64-разрядная); – Windows 8.1 Enterprise (32-разрядная/64-разрядная); – Windows 10 Home (32-разрядная/64-разрядная); – Windows 10 Pro (32-разрядная/64-разрядная); – Windows 10 Enterprise (32-разрядная/64-разрядная); – Windows 11 Home (64-разрядная); – Windows 11 Pro (64-разрядная); – Windows 11 Enterprise (64-разрядная)

8.8.5 Сведения о сертификатах

ПО Efros DO имеет сертификат ФСТЭК России №4618 от 07.12.2022 действителен до 07.12.2027 на соответствие требованиям руководящих документов по 4 уровню доверия.

8.8.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в следующей Таблица 8.18.

Таблица 8.18 – Используемые для взаимодействия сетевые порты

Название сервиса / номер порта	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
TCP/53, UDP/53	Синхронизация имен с DNS-сервером	Сервер управления	DNS сервер
TCP/20002	Для подключения Windows-агента	Windows-агент	Сервер управления
UDP/514	Syslog	Агент	Сервер управления
UDP/162	SNMP Trap / Inform	Агент	Сервер управления

8.9 Подсистема резервного копирования

8.9.1 Общие положения

Подсистема предназначена для резервного копирования и оперативного восстановления конфигурации АРМ, серверов, сетевого оборудования и СрЗИ в случае физического или логического сбоя выполняется резервное копирование конфигураций и создание образов системных дисков АРМ и серверов.

8.9.2 Функциональные возможности подсистемы

Подсистема обеспечивает выполнение функций, требуемых для реализации следующих мер обеспечения безопасности объекта КИИ:

– АУД.3 Генерирование временных меток и (или) синхронизация системного времени;

– АУД.4 Регистрация событий безопасности;

– ОДТ.4 Резервное копирование информации;

– ОДТ.5 Обеспечение возможности восстановления информации;

– ОДТ.6 Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях;

– ДНС.5 Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций.

Подсистема резервного копирования выполняет следующие функции:

– создание резервных копий образов серверов СОИБ ОКИИ в ручном и автоматическом режиме;

– оперативное восстановление серверов СОИБ ОКИИ в случае нарушения их функционирования.

В случае необходимости, резервное копирование может быть расширено на компоненты ОКИИ, для которых резервное копирование и восстановление не обеспечено поставщиком ПТК ОКИИ.

Для всех планов резервных копий устанавливается максимальный уровень сжатия. План резервного копирования запускается Администратором ИБ вручную.

Для хранения резервных копий используются отказоустойчивые узлы хранения, которые размещены в Системе хранения данных СОИБ ОКИИ.

Резервному копированию подлежат только системные диски и базы данных серверов СОИБ ОКИИ для их оперативного восстановления.

Долгосрочный архив событий безопасности подсистемы регистрации и обработки событий безопасности не подлежит резервному копированию. Доступность и целостность архива событий обеспечивается средствами системы хранения данных СОИБ ОКИИ.

8.9.3 Структура подсистемы

Подсистема резервного копирования реализуется на базе программного комплекса КиберБэкап Расширенный и включает следующие компоненты:

– сервер управления КиберБэкап НКНХ.5273-0000-С-SRV-026А, устанавливаемый в создаваемый сегмент СОИБ ОКИИ на выделенный сервер;

– клиентское ПО КиберБэкап, устанавливаемый на АРМ и серверы защищаемых ОКИИ, СОИБ ОКИИ, обеспечивающий создание резервных копий, восстановление данных, а также проверку целостности резервных копий.

Объем дискового пространства, необходимый для хранения резервных копий на сервере, рассчитывается исходя из объема копируемой информации и следующих условий:

– размер полной резервной копии составляет 60% от объема копируемой информации (с учетом сжатия);

– производится хранение не менее одной полной резервных копий;

– добавлен резерв дискового пространства размером 20%.

Управление компонентами подсистемы резервного копирования осуществляется программным модулем «Web-консоль управления» (порт TCP/9877), установленная на сервере управления Кибербекап НКНХ.5273-0000-С-SRV-026А.

8.9.3.1 Требования к параметрам настройки

На этапе внедрения должны быть выполнены следующие настройки:

– создание хранилища резервных копий;

– создание планов резервного копирования для защищаемых АРМ/серверов СОИБ ОКИИ;

– создание учетных записей согласно ролевой модели;

– ограничение доступа к консоли управления только администратору;

– настройка почтовых уведомлений администратору.

8.9.3.2 Резервное копирование

Резервное копирование и восстановление компонентов подсистемы осуществляется с помощью подсистемы резервного копирования (Раздел 0) путем создание полного образа диска ОС.

8.9.3.3 Обновление компонентов

Обновление ПО ПРК осуществляется после выхода новых версий и/или при наличии уведомлений от производителя о необходимости установки критических обновлений (патчей). Обновление должно выполняться в соответствии с требованиями эксплуатационной документации.

8.9.4 Описание комплекса ТС подсистемы

Подсистема резервного копирования включает в себя сервер резервного копирования Кибер Бэкап и узел хранения данных в Системе хранения данных СОИБ ОКИИ.

Требования к ТС для установки компонентов Платформы представлены в Таблица 8.19.

Таблица 8.19 – Требования к компонентам подсистемы резервного копирования

Компонент	Параметр	Системные требования
Сервер Кибер Бэкап	ОС	– Astra Linux Special Edition 1.7
	Процессор	– 4 vCPU
	Оперативная память	– 8 ГБ
	Жесткий диск	– Системный диск: 150 ГБ – Том для резервных копий: 4 ТБ
	Сетевой интерфейс	– 1 Gb

8.9.5 Сведения о сертификатах

ПО Кибер Бэкап имеет сертификат ФСТЭК России № 4337 от 11.12.2020 г. (переоформлен 12.05.2022 г.) по 11.12.2025 г. Соответствует требованиям документов: Требования доверия (4), ТУ.

8.9.6 Взаимодействие со смежными подсистемами и между компонентами

Для обеспечения информационного взаимодействия компонентов со смежными подсистемами используются порты, указанные в следующей Таблица 8.20.

Таблица 8.20 – Используемые для взаимодействия сетевые порты

Название сервиса/ номер порта	Описание сервиса	Взаимодействующие компоненты	
		Источник	Назначение
TCP/9877	Взаимодействие компонентов Кибер Бэкап	АРМ и серверы СОИБ	Сервер резервного копирования
TCP/7780	Агенты используют эти порты для обмена данными с сервером управления	АРМ и серверы СОИБ	Сервер резервного копирования
TCP/445, 25001,43234	Для удаленной установки и обновления агентов	Сервер резервного копирования	АРМ и Серверы СОИБ
TCP/9850, TCP/9852, TCP/9862, TCP/9876	Передача данных от агентов при выполнении резервного копирования	АРМ и серверы СОИБ	Сервер резервного копирования
TCP/123 (NTP), UDP/123 (NTP)	Синхронизация времени с NTP-сервером	Сервер резервного копирования	Сервер точного времени

9 РЕШЕНИЯ ПО РЕЖИМАМ ФУНКЦИОНИРОВАНИЯ, ДИАГНОСТИРОВАНИЮ РАБОТЫ СИСТЕМЫ

СОИБ ОКИИ функционирует в следующих режимах:

– штатный;

– сервисный;

– аварийный.

9.1 Штатный режим функционирования

Штатное функционирование СОИБ ОКИИ включает:

– контроль доступа пользователей к ресурсам и контроль за выполнением правил политики безопасности на программно-техническом и организационном уровнях;

– администрирование и регламентное обслуживание компонентов СОИБ ОКИИ, не требующее останова СОИБ ОКИИ.

– В штатном режиме осуществляется:

– планирование проверки соответствия действий пользователей требованиям ИБ (комплексу нормативно-организационных документов);

– периодическая проверка выполнения правил политики безопасности;

– периодическая проверка соответствия прав пользователей по доступу к ресурсам АСУ ТП их должностным обязанностям;

– периодическая проверка АРМ операторов на предмет соответствия конфигурации требованиям ИБ – отсутствие нелегального оборудования, отсутствие постороннего ПО и т.д.;

– периодическая проверка процедур резервного копирования и восстановления, их полноты и соответствия текущей конфигурации СОИБ ОКИИ;

– периодическая проверка процедур восстановления работоспособности СОИБ ОКИИ, их полноты и соответствия текущей конфигурации и задачам СОИБ ОКИИ;

– периодическая ручная и автоматическая проверки файлов журналирования и архивов электронных документов;

– автоматическое реагирование на попытки НСД;

– постоянный сбор и анализ статистических данных об активности пользователей и приложений, сетевой активности пользователей, анализ объемов информационного обмена, анализ используемых для информационного обмена адресов, форматов, данных;

– анализ планов и проектов развития и модернизации СОИБ ОКИИ на предмет соответствия политике безопасности;

– документирование и подготовка отчетов о проведении проверок, аудита, документирование предложений по совершенствованию политики безопасности.

9.2 Сервисный режим функционирования

При установке и настройке компонентов, их модернизации или ремонте СОИБ ОКИИ функционирует в сервисном режиме, при этом осуществляются установка, замена, первоначальное конфигурирование и дополнительная настройка компонентов программно-аппаратных СрЗИ.

Установка, замена, первоначальное конфигурирование и дополнительная настройка указанных выше компонентов СОИБ ОКИИ производится в соответствии с эксплуатационной документацией на эти средства в режимах, обеспечивающих сервисное обслуживание программно-аппаратных средств и предусматривающих временный останов СОИБ ОКИИ или отдельных ее компонентов.

В сервисном режиме также проверяется функционирование и осуществляется тестирование защищенности АСУ ТП (при этом АСУ ТП должна быть переведена в аналогичный режим работы).

При успешном завершении сервисного обслуживания (прохождении всех тестов и проверок по функционированию СОИБ ОКИИ) система переводится в штатный режим функционирования.

9.3 Аварийный режим работы

Переход СОИБ ОКИИ в аварийный режим может происходить по следующим причинам:

– нарушение работоспособности отдельных компонентов СОИБ ОКИИ;

– нарушение функционирования поддерживающей инфраструктуры – общесистемных сервисов, сетей электропитания, каналов связи и т.п.;

– несанкционированный доступ к ресурсам АСУ ТП.

Аварийный режим включает в себя:

– диагностирование инцидентов или проблем, связанных либо со сбоями или авариями в работе СОИБ ОКИИ, либо с попытками НСД к ресурсам сети;

– оперативное противодействие попыткам НСД;

– восстановление при необходимости программно-аппаратной конфигурации СОИБ ОКИИ и АСУ ТП (сетевого оборудования и АРМ, СрЗИ);

– восстановление информации при ее утере (средствами ПО резервного копирования и восстановления);

– расследование причин НСД или аварии и определение источника инцидента или проблемы (возможно, с привлечением экспертных организаций и правоохранительных органов).

Реагирование на попытки НСД и аварийные ситуации включает принятие контрмер, необходимое восстановление информации, выработку и проведение профилактических мероприятий.

После проведения первичной диагностики и определения причин НСД или аварии СОИБ ОКИИ переводится из аварийного режима в сервисный режим, а затем, после проверки функционирования – в штатный режим.

10 РЕШЕНИЯ ПО ЧИСЛЕННОСТИ, КВАЛИФИКАЦИИ И ФУНКЦИЯМ ПЕРСОНАЛА СИСТЕМЫ, РЕЖИМАМ ЕГО РАБОТЫ, ПОРЯДКУ ВЗАИМОДЕЙСТВИЯ

Для эксплуатации СОИБ ОКИИ предусмотрены роли:

– Системный администратор СОИБ ОКИИ – специалист по информационным технологиям для обслуживания ПО и ТС СОИБ ОКИИ в технологических сетях АСУ ТП;

– Системный администратор – специалист по информационным технологиям для обслуживания агентского ПО СОИБ ОКИИ в технологических сетях АСПЗ, ЛСО, КИТСО;

– Администратор ИБ СОИБ ОКИИ – специалист по ИБ для обеспечения безопасности ИС, информационно-телекоммуникационных сетей и АСУ;

– Начальник службы ИБ – ответственный за обеспечение безопасности ОКИИ ПАО «Нижнекамскнефтехим».

Системный администратор СОИБ ОКИИ выполняет (но не ограничиваясь) следующие функции:

– установка ПО комплекса СрЗИ;

– конфигурация и поддержка функционирования комплекса СрЗИ;

– мониторинг состояния комплекса СрЗИ;

– получение и распространение обновлений средств комплекса СрЗИ, включая настройку ПО и ТС;

– конфигурация встроенных механизмов безопасности системного ПО компонентов ОКИИ (АСУ) в соответствии с требованиями Администратора ИБ СОИБ ОКИИ;

– периодическое резервное копирование конфигурационных файлов СрЗИ;

– принятие мер по восстановлению работоспособности СрЗИ в случае возникновения сбоев;

– участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации.

Системный администратор выполняет (но не ограничиваясь) следующие функции:

– установка, конфигурация и поддержка функционирования агентского ПО СОИБ ОКИИ на АРМ, серверы в технологических сетях АСПЗ, ЛСО, КИТСО;

– конфигурация встроенных механизмов безопасности системного ПО АРМ, серверов в технологических сетях АСПЗ, ЛСО, КИТСО в соответствии с требованиями Администратора ИБ СОИБ ОКИИ;

– получение и распространение обновлений агентского ПО СОИБ ОКИИ (в том числе базы сигнатур вредоносного ПО);

– периодическое резервное копирование конфигурационных файлов СрЗИ;

– принятие мер по восстановлению работоспособности СрЗИ в случае возникновения сбоев;

– участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации.

Администратор СОИБ ОКИИ выполняет (но не ограничиваясь) следующие функции:

– заведение и удаление учетных записей пользователей СОИБ ОКИИ, а также управление их полномочиями;

– поддержание правил разграничения доступа в СОИБ ОКИИ;

– регистрация новых администраторов СОИБ ОКИИ, определение их полномочий и политик безопасности, назначение им идентификаторов и паролей, управление доступом;

– еженедельный сбор журналов регистрации событий ИБ с комплексов средств СОИБ ОКИИ и организация хранения журналов;

– контроль конфигураций СрЗИ и выявление несанкционированных изменений и нарушений, а также попыток НСД в СОИБ ОКИИ;

– ежедневный мониторинг комплекса средств СОИБ ОКИИ и просмотр журнала регистрации событий на предмет наличия инцидентов ИБ;

– контроль учета и хранения машинных носителей информации, содержащих защищаемую информацию;

– взаимодействие с эксплуатационным персоналом защищаемых АСУ по вопросам обеспечения безопасности информации;

– ведение учетной документации в соответствии с требованиями внутренних нормативных документов по обеспечению ИБ;

– проведение ежемесячного контроля наличия обновлений компонентов комплексов СрЗИ;

– анализ результатов функционирования компонентов комплексов СрЗИ, подготовка предложений и отчетов по результатам анализа;

– разработка и реализация мер защиты информации;

– разработка правил корреляции событий, правил реагирования на инциденты ИБ;

– контроль обновления антивирусных баз;

– проведение анализа записей журналов событий безопасности компонентов комплексов СрЗИ;

– проведение оценки текущей надежности компонентов комплексов СрЗИ;

– проверка целостности компонентов ПО СОИБ ОКИИ;

– инициирование проведения служебных расследований по фактам нарушения установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических компонентов СОИБ ОКИИ;

– устранение недостатков, выявленных по результатам проверок состояния ИБ СОИБ ОКИИ, в рамках аудита защищаемых систем и проверок регулирующих органов;

– информирование руководителя организации о выявленных нарушениях и несанкционированных действиях пользователей и технического персонала, принятие необходимых мер по устранению нарушений;

– участие в разработке предложений по совершенствованию СОИБ ОКИИ;

– проведение иных мероприятий, направленных на поддержание режима в СОИБ ОКИИ.

Начальник службы ИБ в рамках СОИБ ОКИИ выполняет (но не ограничиваясь) следующие функции:

– определение, формализация и контроль соблюдения политики информационной безопасности, внутренних нормативных документов по информационной безопасности;

– обеспечение взаимодействия с эксплуатационным персоналом защищаемых АСУ по вопросам обеспечения безопасности информации;

контроль ведения учетной документации в соответствии с требованиями внутренних нормативных документов по обеспечению ИБ;

– проведение ежемесячного контроля окончания срока действия лицензионных соглашений на использование компонентов комплекса СрЗИ и их сертификатов по требованиям безопасности;

– проведение инструктажа или консультирование администраторов защищаемых АСУ по вопросам ИБ, а также контроль их знаний в области обеспечения ИБ;

– проведение контроля выполнения мероприятий по повышению осведомленности пользователей защищаемых АСУ о методах и средствах фишинговых атак;

– организация работ по тестированию процедуры восстановления работоспособности компонентов СОИБ ОКИИ и участие в них;

– обеспечение проведения служебных расследований по фактам нарушения установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических компонентов СОИБ ОКИИ;

– контроль устранения недостатков, выявленных по результатам проверок состояния ИБ СОИБ ОКИИ, в рамках аудита защищаемых систем и проверок регулирующих органов.

Персонал СОИБ ОКИИ должен принимать на себя обязательства не разглашать и не использовать в целях, не связанных с выполнением должностных обязанностей, сведения, отнесенные к сведениям ограниченного распространения, ставшие им известными в связи с исполнением должностных обязанностей. Персонал СОИБ ОКИИ принимает на себя обязательства добросовестно исполнять требования

локальных актов и должностные обязанности согласно должностной инструкции по занимаемой должности.

Для снижения информационных рисков, связанных с потенциальной возможностью совершения неумышленных ошибок или злонамеренных действий этой категории лиц, должны проводиться общие мероприятия по повышению доверия к Администратору СОИБ ОКИИ:

- подбор, подготовка и обучение персонала;
- проверка соответствия занимаемой должности;
- повышение мотивации персонала;
- выявление нелояльных сотрудников.

Одна функциональная роль может быть закреплена за одним или несколькими лицами.

При необходимости для технического обслуживания и эксплуатации СОИБ ОКИИ могут привлекаться внешние организации (аутсорсинг), которые имеют лицензии на определенный вид деятельности в соответствии с Федеральным законом Российской Федерации от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». В рамках технического обслуживания СОИБ ОКИИ внешней организации необходимо иметь лицензию на деятельность по технической защите конфиденциальной информации, а также лицензию на деятельность по техническому обслуживанию шифровальных (криптографических) средств (в случае если внешняя организация привлекается для технического обслуживания средств криптографической защиты информации).

На роль Системных администраторов рекомендуется назначать лица, имеющие высшее профессиональное образование в области информационных технологий по специальности 230000 «Информатика и вычислительная техника».

На роль Администратора ИБ СОИБ ОКИИ рекомендуется назначать лицо, имеющее высшее профессиональное образование в области ИБ по специальности 090000 «Информационная безопасность» в соответствии с «Общероссийским классификатором специальностей», с квалификацией бакалавра, магистра или специалиста. В отсутствие профильного высшего образования сотрудник должен пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность».

Начальник службы ИБ должен иметь высшее образование по направлению подготовки (специальности) в области информационной безопасности, но также допускаются области математических и естественных наук, инженерного дела, технологий и технических наук (в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации), или иное высшее образование, при условии наличия стажа работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет при условии профессиональной подготовки по программе «Информационная безопасность» длительностью не менее 512 академических часов.

Рекомендуется, чтобы опыт работы по специальности лица, назначаемого на роль Администратора СОИБ ОКИИ, составлял не менее трех лет. На роли Администратора СОИБ ОКИИ могут быть назначены лица, не имеющие профильного образования, но имеющие опыт непрерывной работы на аналогичной должности.

Перед получением допуска к самостоятельной работе Администратор СОИБ ОКИИ должен:

– ознакомиться с эксплуатационной документацией СОИБ ОКИИ по обеспечению ИБ;

– по возможности пройти специализированные курсы с последующей проверкой полученных знаний и навыков.

Техническое обслуживание, осмотр, подключение и отключение электроустановок могут проводиться лицом, имеющим квалификационную группу по электробезопасности не ниже третьей.

Расчет трудозатрат Системных администраторов (Системный администратор СОИБ ОКИИ, Системный администратор) и Администратора СОИБ ОКИИ представлен в Таблица 10.1 по подсистемам СОИБ ОКИИ.

Таблица 10.1 – Расчет трудозатрат Системных администраторов и Администратора ИБ СОИБ ОКИИ

Действия по администрированию	**Периодичность действия (в месяц)**	**Время действия (час)**	**Системный администратор (часов в месяц)**	**Администратор ИБ СОИБ ОКИИ (часов в месяц)**
Подсистема защиты от НСД				
Анализ системных журналов ОС, ПО	4,0	1,0	4,0	-
Изменение политик безопасности	2,0	4,0	-	8,0
Ежедневный анализ событий безопасности	22,0	1,0	-	22
Периодическое резервное копирование конфигурационных файлов	1,0	2,0	2,0	-
Подсистема межсетевого экранирования и обнаружения вторжений				
Создание/изменение настроек межсетевого экранирования	1,0	2,0	2,0	-
Анализ системных журналов ПО/ работоспособности компонента СрЗИ	4,0	0,5	2,0	-
Установка обновлений	0,5	2,0	1,0	-
Контроль корректности настроек МЭ	2,0	3,0	-	6,0

Действия по администрированию	Периодичность действия (в месяц)	Время действия (час)	Системный администратор (часов в месяц)	Администратор ИБ СОИБ ОКИИ (часов в месяц)
Периодическое резервное копирование конфигурационных файлов	1,0	2,0	2,0	-
Принятие мер по восстановлению работоспособности СрЗИ в случае возникновения сбоев	1,0	2,0	2,0	-
Анализ системных журналов ПО/ работоспособности компонента СрЗИ	4,0	1,0	4,0	-
Установка обновлений	0,5	8,0	4,0	-
Создание политик/правил обнаружения сетевых атак	2,0	2,0	-	4,0
Периодическое резервное копирование конфигурационных файлов	1,0	2,0	2,0	-
Принятие мер по восстановлению работоспособности СрЗИ в случае возникновения сбоев	1,0	2,0	2,0	-
Подсистемы антивирусной защиты				
Анализ системных журналов ПО/ работоспособности компонента СрЗИ	4,0	1,0	4,0	-
Установка обновлений	1,0	1,0	1,0	-
Создание/изменение конфигурации компонентов	4,0	1,0	-	4,0
Ежедневный контроль настроек и анализ событий СрЗИ	22,0	0,5	-	11,0
Периодическое резервное копирование конфигурационных файлов	1,0	2,0	2,0	-
Принятие мер по восстановлению работоспособности СрЗИ в случае возникновения сбоев	1,0	2,0	2,0	-
Подсистема регистрации и обработки событий безопасности				
Анализ системных журналов ПО/ работоспособности компонента СрЗИ	4,0	1,0	4,0	-
Установка обновлений	1,0	4,0	4,0	-

Действия по администрированию	Периодичность действия (в месяц)	Время действия (час)	Системный администратор (часов в месяц)	Администратор ИБ СОИБ ОКИИ (часов в месяц)
Создание/изменение конфигурации и правил	2,0	4,0	-	8,0
Ежедневный анализ событий безопасности	22,0	1,0	-	22,0
Периодическое резервное копирование конфигурационных файлов	1,0	2,0	2,0	-
Принятие мер по восстановлению работоспособности СрЗИ в случае возникновения сбоев	1,0	2,0	2,0	-
Подсистема криптографической защиты информации				
Создание/изменение настроек межсетевого экранирования на криптошлюзах	1,0	2,0	2,0	-
Анализ системных журналов ПО/ работоспособности криптошлюзов	4,0	0,5	2,0	-
Установка обновлений	0,5	2,0	1,0	-
Контроль корректности настроек криптошлюзов	2,0	3,0	-	6,0
Периодическое резервное копирование конфигурационных файлов	1,0	2,0	2,0	-
Принятие мер по восстановлению работоспособности криптошлюзов в случае возникновения сбоев	1,0	2,0	2,0	-
Анализ системных журналов ПО/ работоспособности криптошлюзов	4,0	1,0	4,0	-
Установка обновлений	0,5	8,0	4,0	-
Периодическое резервное копирование конфигурационных файлов	1,0	2,0	2,0	-
Принятие мер по восстановлению работоспособности СЗИ в случае возникновения сбоев	1,0	2,0	2,0	-
Подсистема анализа защищенности				
Создание задач сканирования	0,3	4,0	-	1,2
Выполнение резервного копирования в ручном режиме	0,3	16,0	-	4,8

Действия по администрированию	Периодичность действия (в месяц)	Время действия (час)	Системный администратор (часов в месяц)	Администратор ИБ СОИБ ОКИИ (часов в месяц)
Анализ результатов сканирования	0,3	8,0	-	2,4
Подсистема резервного копирования СОИБ				
Создание и корректировка плана резервного копирования серверов СОИБ	0,5	4,0	2	-
Контроль выполнения резервного копирования	0,5	4,0	2	-
ИТОГО:	-	-	73,0	99,4

Необходимая численность администраторов находится в прямой зависимости от TF – времени, затрачиваемого в месяц на выполнение всех функций по сопровождению СОИБ данной ролью и в обратной зависимости от:

– U – процента рабочего времени, которое сотрудник непосредственно тратит на выполнение функций;

– A – доступности сотрудника (сотрудник может быть в отпуске или на больничном);

– NH – количестве часов в месяце.

Тогда N – необходимое количество сотрудников – определяется формулой:

$$N = \frac{TF}{U \bullet A \bullet NH}$$

При проведении расчетов учитывалось, что:

– NH = 22•8=176 часов;

– U = 0,8 часа;

– A = 0,75 часа;

– TFадмСист = 73,0 часов;

– TFадмСОИБ = 99,4 часов;

Итого получилось NадмСист = 0,69 и NадмСОИБ = 0,94.

Таким образом, для обслуживания СОИБ необходим как минимум один Администратор ИБ СОИБ ОКИИ, один системный администратор СОИБ ОКИИ, один Системный администратор. С учетом распределенной структуры площадок ПАО «Нижнекамскнефтехим» количество сотрудников на каждую из ролей может быть увеличено для проведения выездных работ по обслуживанию компонентов СОИБ ОКИИ.

В случае сбоя и нештатного режима функционирования СОИБ численность работников может быть увеличена пропорционально количеству и сложности решаемых задач.

Квалификация персонала СОИБ ОКИИ (Администратор ИБ СОИБ ОКИИ, Системные администраторы) предполагает владение следующими знаниями:

– стек протоколов TCP/IP;

– теоретические основы, стандарты, принципы работы МЭ;

– теоретические основы, стандарты, принципы работы средств терминального доступа;

– принципы работы ПО, задействованного в СОИБ ОКИИ;

– основы администрирования ОС Microsoft Windows Server 2012 R2;

– законодательство Российской Федерации в области защиты информации;

Квалификация Начальника службы ИБ предполагает владение следующими знаниями:

– основные международные и российские стандарты, регламентирующие управление ИБ;

– подходы к управлению ИБ;

– принципы разработки процессов управления ИБ;

– принципы построения системы управления ИБ;

– принципы создания основных документов, регламентирующих вопросы управления ИБ;

– подходы к интеграции системы управления ИБ в общую систему управления безопасностью организации;

– основы управления рисками ИБ;

– основы управления инцидентами ИБ и непрерывностью процессов.

11 ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИБ

Одним из необходимых условий эффективного функционирования и устойчивости защищаемых ОКИИ является выполнение комплекса организационных мероприятий по обеспечению ИБ. Организационные мероприятия обеспечиваются подразделением по защите информации Эксплуатирующей организации.

Организационные (административные) мероприятия регламентируют процессы функционирования СОИБ ОКИИ, использования ее ресурсов, деятельности персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы обеспечить снижение вероятности нарушения заданных характеристик безопасности информации в результате реализации угроз ИБ.

К организационным мероприятиям по обеспечению ИБ относятся:

- Формирование системы нормативного обеспечения.
- Организация защиты компонентов ОКИИ.
- Решения по персоналу.

11.1 Формирование системы нормативного обеспечения

Формирование системы нормативного обеспечения представляет собой упорядоченную совокупность взаимосвязанных документов, регламентирующих деятельность в области обеспечения ИБ, и организацию контроля соблюдения установленных этими документами правил и требований.

Рекомендованный перечень основных организационно-распорядительных документов:

- Приказ о назначении (структурного подразделения) должностного лица ответственного за защиту СОИБ ОКИИ;
- Инструкция по эксплуатации компонентов ИБ ОКИИ;
- Политика обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- Политика по защите от вредоносного кода;
- Политика использования съемных носителей;
- Политика контроля и управления доступом;
- Политика обеспечения непрерывности;
- Политика парольной защиты;
- Политика управления инцидентами ИБ;
- Политика физического доступа;
- Политика внутреннего аудита безопасности;
- Порядок повышения осведомленности и обучения в области ИБ.

На основе нормативно-методических и организационно-распорядительных документов по вопросам организации ИБ выполняется распределение функций и определение порядка взаимодействия участников процесса на всех этапах жизненного цикла СОИБ ОКИИ, обеспечивающее четкое разделение полномочий и ответственности.

Должно быть произведено ознакомление пользователей ОКИИ с их уровнями полномочий, а также с организационно-распорядительной документацией, определяющей требования и порядок обработки информации.

12 СВЕДЕНИЯ ОБ ОБЕСПЕЧЕНИИ ЗАДАННЫХ В ТЕХНИЧЕСКОМ ЗАДАНИИ ПОТРЕБИТЕЛЬСКИХ ХАРАКТЕРИСТИК СИСТЕМЫ (ПОДСИСТЕМ), ОПРЕДЕЛЯЮЩИХ ЕЕ КАЧЕСТВО

СОИБ выполняет автоматизацию процессов и действий по обеспечению ИБ в ОКИИ магистрального этиленопровода «Нижнекамск - Казань» ПАО «Нижнекамскнефтехим» с учетом требований Приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» для 3 категории значимости.

Меры по защите информации в ОКИИ направлены на защиту от актуальных угроз безопасности информации и реализуются организационными мерами, а также за счет применения СрЗИ.

Перечень актуальных угроз безопасности информации ОКИИ и меры их нейтрализующие приведены в документе «Техническое задание на создание системы обеспечения информационной безопасности объектов критической информационной инфраструктуры ПАО «Нижнекамскнефтехим».

Меры обеспечения безопасности объектов КИИ, выполняемые средствами защиты информации, входящими в состав СОИБ ОКИИ, приведены в разделе 8.

Порядок выполнения организационных мер определяется организационно-распорядительными документами Заказчика.

13 МЕРОПРИЯТИЯ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ В ДЕЙСТВИЕ

13.1 Создание необходимых подразделений и штатных должностей

Решение о вводе дополнительных штатных должностей для настройки и эксплуатации СрЗИ принимается Эксплуатирующей организацией.

Выполнение функций администраторов ИБ возлагается на специалистов из числа работников Эксплуатирующей организации.

13.2 Подготовка персонала

Руководство Эксплуатирующей организации разрабатывает, утверждает и внедряет план мероприятий по обучению и проверки квалификации персонала.

Персонал, эксплуатирующий СрЗИ, должен иметь достаточные знания и навыки по настройке и обслуживанию СрЗИ и обеспечению защиты информации.

14 МЕРОПРИЯТИЯ ПО ВВОДУ СОИБ ОКИИ В ДЕЙСТВИЕ

Для установки компонентов СОИБ ОКИИ и проведения необходимых настроек СрЗИ в условиях эксплуатации Эксплуатирующая организация должна обеспечить:

– готовность инфраструктуры к установке компонентов СОИБ ОКИИ;

– определение полномочий по доступу к информации для всех пользователей и процессов (матрица доступа) и оформление их документально;

– завершение работ по строительству и отделке серверных помещений;

– предоставление доступа к каналам связи путем соответствующих настроек на коммутационном и каналообразующем оборудовании;

– наличие обученного персонала для обеспечения эксплуатации СОИБ ОКИИ;

– содействие обслуживающего персонала по внесению корректировок в настройки компоненты СОИБ ОКИИ.

Для осуществления работ по вводу СОИБ ОКИИ в действие необходимо произвести следующие работы:

– Наладочные работы;

– Заводские испытания СОИБ ОКИИ;

– Автономная наладка;

– Комплексная наладка СОИБ ОКИИ;

– Предварительные испытания СОИБ ОКИИ;

– Приемосдаточные испытания СОИБ ОКИИ.

ПЕРЕЧЕНЬ НОРМАТИВНОЙ ДОКУМЕНТАЦИИ

– Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Приказ ФСТЭК России от 14 марта 2014 г. № 31 Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, предоставляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

– Приказ ФСТЭК России от 25 декабря 2017 г. № 239 Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– СР/09-01-01/ МУ30 Методические указания по обеспечению информационной безопасности АСУ ТП;

– Федеральный закон от 21.07.1997 г. № 116-ФЗ (с изменениями от 07.08.2000 г., 10.01. 2003 г., 22.08.2004 г., 09.05.2005 г., 18.12.2006 г., 30.12.2008 г., 27.12.2009 г.) «О промышленной безопасности опасных производственных объектов»;

– Федеральный закон от 22.07.2008 г. № 123-ФЗ (редакция, действующая с 31 июля 2018 года) Технический регламент о требованиях пожарной безопасности;

– ГОСТ 12.1.030-81 Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление (с Изменением №1);

– ГОСТ 12.2.007.14-75 Система стандартов безопасности труда. Кабели и кабельная арматура. Требования безопасности (с Изменением №1, 2);

– ГОСТ 21.208-2013 Система проектной документации для строительства. Автоматизация технологических процессов. Обозначения условные приборов и средств автоматизации в схемах;

– ГОСТ 21.408-2013 Система проектной документации для строительства. Правила выполнения проектной документации автоматизации технологических процессов (с поправками);

– ГОСТ 24.301-80 Система технической документации на АСУ. Общие требования к выполнению текстовых документов (с изменениями №1, 2);

– ГОСТ 24.701-86 Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения;

– ГОСТ 31565-2012 Кабельные изделия. Требования пожарной безопасности;

– ГОСТ 33542-2015 (IEC 60445:2010) Основополагающие принципы и принципы безопасности для интерфейса «человек-машина», выполнение и идентификация. Идентификация выводов электрооборудования, концов проводников и проводников;

– ГОСТ 34.201-2020 Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;

– ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

– ГОСТ 34.602-2020 Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

– ГОСТ Р 59792-2021 Информационная технология. Виды испытаний автоматизированных систем;

– ГОСТ Р 50462-2009 (МЭК 60446:2007) Базовые принципы и принципы безопасности для интерфейса «человек-машина», выполнение и идентификация. Идентификация проводников посредством цветов и буквенно-цифровых обозначений;

– ГОСТ Р 50571.5.54-2013/МЭК 60364-5-54:2011 Электроустановки низковольтные. Часть 5-54. Заземляющие устройства, защитные проводники и защитные проводники уравнивания потенциалов;

– ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели;

– ГОСТ Р 56498-2015/IEC/PAS 62443-3:2008 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления;

– ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики;

– ГОСТ Р МЭК 62443-3-3-2016 Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности;

– ПУЭ Правила устройства электроустановок. Седьмое издание;

– Приказ Ростехнадзора от 11.12.2020 № 517 Федеральные нормы и правила в области промышленной безопасности «Правила безопасности для опасных производственных объектов магистральных трубопроводов».

Таблица регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в док.	Номер док.	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных				

АО НИП «ИНФОРМЗАЩИТА»

Информзащита
Системный интегратор

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Предварительные настройки комплекса средств защиты информации

НКНХ.5273-ПД-ИБ1-ИД4

2024

СОДЕРЖАНИЕ

Лист

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	НКНХ.5273-ПД-ИБ1-ИД4		
Разраб.		Черкасов			11.09.24	Предварительные настройки комплекса средств защиты информации	Стадия	Лист	Листов
							П	1	39
Н. контр.		Скиткин			11.09.24		Информзащита Системный интегратор		
ГИП		Черкасов			11.09.24				

1 ОПИСАНИЕ НАСТРОЕК

1.1 Подсистема защиты от несанкционированного доступа

Описание настроек подсистемы защиты от несанкционированного доступа приведены в Таблица 1.1, Таблица 1.2, Таблица 1.3, Таблица 1.4, Таблица 1.5, Таблица 1.6.

Таблица 1.1 – Описание аппаратной платформы Secret Net Studio

Параметр	Значение
Процессор	<Уточняется на этапе реализации>
Оперативная память	<Уточняется на этапе реализации>
Жесткий диск (свободное место)	<Уточняется на этапе реализации>
Операционная система	Windows Server 2022
IP-адрес	<Уточняется на этапе реализации>
Hostname	<Уточняется на этапе реализации>
FQDN	<Уточняется на этапе реализации>
Mask	<Уточняется на этапе реализации>
Default Gateway	<Уточняется на этапе реализации>
DNS-серверы	<Уточняется на этапе реализации>

Таблица 1.2 – Параметры механизмов защиты Secret Net Studio

Параметр	Значение
Дискреционное управление доступом	Включено
Затирание данных	Включено
Контроль устройств	Выключено
Замкнутая программная среда	Выключено
Полномочное управление доступом	Выключено
Контроль печати	Включено
Межсетевой экран	Выключено
Обнаружение вторжений	Включено
Шифровать трафика	Выключено
Антивирус	Выключено

Таблица 1.3 – Параметры политики безопасности Secret Net Studio

Параметр	Значение
Группа параметров «Базовая защита»	
«Вход в систему»	
Максимальный период неактивности для блокировки экрана	15 мин.
Запрет вторичного входа в систему	Нет
Реакция на изъятие идентификатора	Не блокировать
Количество неудачных попыток аутентификации	7

Параметр	Значение
Режим идентификации пользователя	Смешанный
Режим аутентификации пользователя	Усиленная аутентификация по паролю
Регистрировать неверные аутентификационные данные	Включено
Парольная политика	Задать свои значения
Минимальная длина пароля	не менее 8 символов
Срок действия пароля	не более 60 дней
Сложность пароля с ограничениями на содержание символов	Включено
«Журнал»	
Максимальный размер журнала системы защиты	4096 кБ
Политика перезаписи событий	Затирать по мере необходимости
Журнал: Учетные записи с привилегией просмотра журнала системы защиты	BUILTIN\Администраторы
Журнал: Учетные записи с привилегией управления журналом системы защиты	BUILTIN\Администраторы
«Теневое копирование»	
Теневое копирование: Размер хранилища	20%, Автоматически перезаписывать старые данные при переполнении хранилища
«Ключи пользователя»	
Максимальный срок действия ключа	360
Минимальный срок действия ключа	не определено
Предупреждение об истечении срока действия ключа	14
«Оповещение о тревогах»	
Оповещение о тревогах: Локальное оповещение о тревогах	Включено
Группа параметров «Защита локальных ресурсов»	
«Дискреционное управление доступом»	
Учетные записи с привилегией управления правами доступа	BUILTIN\Администраторы
Группа параметров «Защита локальных ресурсов» - «Затирание данных»	
Количество циклов затирания на локальных дисках	1
Количество циклов затирания на сменных носителях	1
Количество циклов затирания оперативной памяти	1
«Полномочное управление доступом»	
Название уровней конфиденциальности	По-умолчанию
Режимы работы	Контроль потоков включен
Режимы работы, строгий контроль терминальных подключений	Включено
Режимы работы, автоматический выбор максимального уровня сессии	Отключено

Параметр	Значение
«Замкнутая программная среда»	
Учетные записи, на которые не действуют правила ЗПС	BUILTIN\Администраторы
«Защита диска и шифрование данных»	
Учетные записи с привилегией на создание криптоконтейнера	BUILTIN\Администраторы BUILTIN\Пользователи
Группа параметров «Защита локальных ресурсов» - «Контроль приложений»	
Перенаправление буфера обмена в RDP-приложениях	Разрешено
Группа параметров «Контроль устройств»	
Теневое копирование	Отключено для всех устройств
Перенаправление устройств в RDP-подключениях	Разрешено для всех типов устройств
Группа параметров «Контроль печати»	
Контроль печати: Маркировка документов	Отключена
Контроль печати: Теневое копирование	Отключено для всех принтеров
Контроль печати: Перенаправление принтеров в RDP-подключениях	Разрешено
Группа параметров «Обнаружение вторжений»	
Включить детектор атак	Включено
Блокировка атакующего хоста при обнаружении атак	15 минут
Используемые сетевые сервисы	По умолчанию
«Детекторы»	
Сканирование портов	Включено
Сканирование портов - Период обнаружения	60 секунд
Сканирование портов – Максимальное количество обращений к портам за указанный период	200
ARP-spoofing	Включено
ARP-spoofing – Время после ARP-запроса, в течении которого ожидается ARP-ответ	1500 миллисекунд
ARP-spoofing – Действие с ARP-ответами, полученными без ARP-запросов	Логировать
SYN-FLOOD	Включено
SYN-FLOOD – Время, за которое учитываются полуоткрытые соединения	30 секунд
SYN-FLOOD – Количество полуоткрытых соединений, после которых хост считается атакующим	20
SYN-FLOOD – Блокировать пакет, если детектор сработал	Включено
Аномальный трафик	Включено
Аномальный трафик – Блокировать пакет, если детектор сработал	Включено
DDoS	Включено

Параметр	Значение
DDoS – Максимальное количество активных удаленных хостов, при превышении которого срабатывает детектор	1000
DoS	Включено
DoS – Отрезок времени, за который учитывается обращение к порту	60
DoS – Максимальное количество пакетов, при превышении которого будет детектирована атака	52428
DoS – Максимальный размер данных, при превышении которого будет детектирована атака	76800
DoS – Замедлять трафик с атакующего хоста	Включено
«Сигнатурные анализаторы»	
Включить сигнатурные анализаторы	Включено
Анализатор HTTP	Включено
Контроль входящего трафика	Включено
Контроль исходящего трафика	Включено
Список портов	80; 8080; 3128
Группа параметров «Обновление»	
Расписание запуска проверки обновлений – Частота запуска	Ежечасно
Размещение сервера обновлений	Обновлять с сервера ООО «Код Безопасности»

Таблица 1.4 – Параметры политики безопасности операционной системы Windows

Параметр	Значение
Политика учетных записей → Политика паролей	
Минимальная длина пароля	8
Пароль должен отвечать требованиям сложности	Enabled
Вести журнал паролей	3
Максимальный срок действия пароля	90
Параметры безопасности → Политика учетных записей → Политика блокировки учетных записей	
Пороговое значение блокировки	7
Время до сброса счетчика блокировки (мин)	15
Продолжительность блокировки учетной записи (мин)	15
Параметры безопасности → Локальные политики → Параметры безопасности	
Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее	14 дн.
Интерактивный вход в систему: предел простоя компьютера	900 сек.
Параметры безопасности → Локальные политики → Политика аудита	
Аудит входа в систему	Успех / Отказ
Аудит доступа к объектам	Нет аудита

Параметр	Значение
Аудит доступа к службе каталогов	Успех / Отказ
Аудит изменения политики	Успех
Аудит использования привилегий	Отказ
Аудит отслеживания процессов	Нет аудита
Аудит системных событий	Успех
Аудит событий входа в систему	Успех / Отказ
Аудит управления учетными записями	Успех
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Вход учетной записи	
Аудит других событий входа учетных записей	Не настроено
Аудит операций с билетами службы Kerberos	Не настроено
Аудит проверки учетных данных	Успех / Отказ
Аудит службы проверки подлинности Kerberos	Не настроено
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Управление учетными записями	
Аудит других событий управления учетными записями	Успех / Отказ
Аудит управления группами безопасности	Успех / Отказ
Аудит управления группами приложений	Успех / Отказ
Аудит управления группами распространения	Не настроено
Аудит управления учетными записями компьютеров	Успех / Отказ
Аудит управления учетными записями пользователей	Успех / Отказ
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Подробное отслеживание	
Аудит активности DPAPI	Не настроено
Аудит завершения процессов	Не настроено
Аудит событий RPC	Не настроено
Аудит создания процессов	Успех
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Доступ к службе каталогов (DS)	
Аудит доступа к службе каталогов	Не настроено
Аудит изменения службы каталогов	Не настроено
Аудит подробной репликации службы каталогов	Не настроено
Аудит репликации службы каталогов	Не настроено
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Вход / Выход	
Аудит блокировки учетных записей	Успех / Отказ
Аудит быстрого режима IPsec	Не настроено
Аудит входа в систему	Успех/Отказ
Аудит выхода из системы	Успех
Аудит других событий входа и выхода	Успех / Отказ
Аудит основного режима IPsec	Не настроено
Аудит расширенного режима IPsec	Не настроено
Аудит сервера политики сети	Не настроено
Аудит специального входа	Успех

Параметр	Значение
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Доступ к объектам	
Аудит диспетчера учетных записей безопасности	Не настроено
Аудит других событий доступа к объектам	Успех / Отказ
Аудит общих папок	Не настроено
Аудит объектов ядра	Не настроено
Аудит отбрасывания пакетов платформой фильтрации	Не настроено
Аудит подключения платформы фильтрации	Не настроено
Аудит работы с дескриптором	Не настроено
Аудит реестра	Не настроено
Аудит сведений об общем файловом ресурсе	Не настроено
Аудит служб сертификации	Не настроено
Аудит событий, создаваемых приложениями	Не настроено
Аудит файловой системы	Не настроено
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Изменение политики	
Аудит других событий изменения политики	Не настроено
Аудит изменения политики авторизации	Успех
Аудит изменения политики аудита	Успех / Отказ
Аудит изменения политики на уровне правил MPSSVC	Не настроено
Аудит изменения политики платформы фильтрации	Не настроено
Аудит изменения политики проверки подлинности	Успех
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Использование прав	
Аудит других событий использования прав	Не настроено
Аудит использования прав, затрагивающих конфиденциальные данные	Не настроено
Аудит использования прав, не затрагивающих конфиденциальные данные	Не настроено
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Система	
Аудит драйвера IPsec	Успех / Отказ
Аудит других системных событий	Успех / Отказ
Аудит изменения состояния безопасности	Успех
Аудит расширения системы безопасности	Успех / Отказ
Аудит целостности системы	Успех / Отказ
Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы → Аудит доступа к глобальным объектам	
Реестр	Не настроено
Файловая система	Не настроено

Таблица 1.5 – Параметры раздела «Журнал событий»

Параметр	Значение
Максимальный размер журнала безопасности	102400 КБ
Максимальный размер журнала приложений	102400 КБ

Параметр	Значение
Максимальный размер системного журнала	102400 КБ
Метод сохранения событий в журнале безопасности	Переписывать события по мере необходимости (сначала старые события)
Сохранение событий в журнале приложений	Переписывать события по мере необходимости (сначала старые события)
Метод сохранение событий в журнале системы	Переписывать события по мере необходимости (сначала старые события)

Таблица 1.6 – Параметры политики безопасности операционной системы Linux

Параметр	Значение
/etc/ssh/sshd_config	
TCPKeepAlive	no
ClientAliveInterval	900
ClientAliveCountMax	0
/etc/profile.d/tmout.sh	
TMOUT=	900
readonly	TMOUT
export	TMOUT
/etc/pam.d/common-auth	
auth [success=ignore default=die] pam_tally.so	deny=7 unlock_time=900 lock_time=5
/etc/pam.d/common-account	
account required pam_tally.so	deny=7 unlock_time=900 lock_time=5
/etc/pam.d/common-password	
password requisite pam cracklib.so	retry=3 minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1
password requisite pam_pwhistory.so	remember=5 retry=3
/etc/login.defs	
PASS_MAX_DAYS	90
PASS_WARN_AGE	14
/etc/logrotate.d/audit	

/var/log/audit/audit.log	{
	create 0600 root root
	weekly
	rotate 12
	missingok
	notifempty
	compress
	sharedscripts
	postrotate
	/usr/bin/systemctl kill -s SIGUSR1 auditd.service >/dev/null 2>&1 || true
	endscript
	}

1.2 Подсистема контроля конфигураций

Описание настроек подсистемы контроля конфигураций приведены в Таблица 1.7, Таблица 1.8, Таблица 1.9.

Таблица 1.7 – Описание аппаратной платформы

Параметр	Значение
Процессор	<Уточняется на этапе реализации>
Оперативная память	<Уточняется на этапе реализации>
Жесткий диск (свободное место)	<Уточняется на этапе реализации>
Операционная система	Windows 11
IP-адрес	<Уточняется на этапе реализации>
Hostname	<Уточняется на этапе реализации>
FQDN	<Уточняется на этапе реализации>
Mask	<Уточняется на этапе реализации>
Default Gateway	<Уточняется на этапе реализации>
DNS-серверы	<Уточняется на этапе реализации>

Таблица 1.8 – Описание настроек устройств типа Сетевые устройства

Параметр	Значение
Поле «Название»	<Уточняется на этапе реализации>
Поле «Описание»	<Уточняется на этапе реализации>
Поле «Группа»	<Уточняется на этапе реализации>
Поле «Тип»	<Уточняется на этапе реализации>
Поле «Профиль отчетов»	<Уточняется на этапе реализации>
Поле «Проверка доступности»	Включена (каждые 15 мин.)
Поле «Сервисный режим»	Отключено
Группа полей «Типы контроля»	
Переключатель «Network Assurance»	Включено
Переключатель «Firewall Assurance»	Включено
Переключатель «Integrity Check Compliance»	Включено
Переключатель «Vulnerability Control»	Отключено
Переключатель «Change Manager»	Отключено
Возможное информационное сообщение под переключателем	-
Группа полей «Параметры подключения»	
Поле «Адрес»	<Уточняется на этапе реализации>
Поле «Пользователь»	<Уточняется на этапе реализации>
Поле «Способ аутентификации»	<Уточняется на этапе реализации>
Поле «Порт SSH»	<Уточняется на этапе реализации>
Поле «Профиль аутентификации»	<Уточняется на этапе реализации>
Кнопка «Проверить подключение»	-
Группа полей «SNMP»	
Поле «SNMP профиль»	<Уточняется на этапе реализации>

Таблица 1.9 – Описание настроек устройств типа АРМ и серверы

Параметр	Значение
Поле «Название»	<Уточняется на этапе реализации>
Поле «Описание»	<Уточняется на этапе реализации>
Поле «Группа»	<Уточняется на этапе реализации>
Поле «Тип»	<Уточняется на этапе реализации>
Поле «Профиль отчетов»	<Уточняется на этапе реализации>
Поле «Проверка доступности»	Включена (каждые 15 мин.)
Поле «Сервисный режим»	Отключено
Группа полей «Типы контроля»	
Переключатель «Network Assurance»	Отключено
Переключатель «Firewall Assurance»	Отключено
Переключатель «Integrity Check Compliance»	Включено
Переключатель «Vulnerability Control»	Отключено
Переключатель «Change Manager»	Отключено
Возможное информационное сообщение под переключателем	-
Группа полей «Параметры подключения»	
Поле «Адрес»	<Уточняется на этапе реализации>
Поле «Пользователь»	<Уточняется на этапе реализации>
Поле «Способ аутентификации»	<Уточняется на этапе реализации>
Поле «Порт SSH»	<Уточняется на этапе реализации>
Поле «Профиль аутентификации»	<Уточняется на этапе реализации>
Кнопка «Проверить подключение»	-
Группа полей «SNMP»	
Поле «SNMP профиль»	Отключено

1.3 Подсистема межсетевого экранирования и обнаружения вторжений

Описание настроек межсетевого экранирования и обнаружения вторжений приведены в Таблица 1.10, Таблица 1.11, Таблица 1.12, Таблица 1.13, Таблица 1.14.

Таблица 1.10 – Сетевые настройки серверных компонентов

Компонент	Наименование параметра	Значение
ARMA СТЕНА К1000 (кластер 1)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>

Компонент	Наименование параметра	Значение
ARMA СТЕНА К1000 (кластер 2)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
ARMA СТЕНА К1000 (кластер 2)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>

Таблица 1.11 – Настройки сетевых интерфейсов

Параметр	Значение
ARMA СТЕНА К1000 (кластер 1)	
Network Interfaces – Outside	
Virtual context	Outside
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Внешний интерфейс до ПАК МЭ корпоративной сети передачи данных
Network Interfaces – DMZ	
Virtual context	DMZ
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Сегмент ДМЗ ТСПД для взаимодействия ТСПД с КСПД
Network Interfaces – SOIB_OKII	
Virtual context	SOIB_OKII
Addressing mode	static

Параметр	Значение
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Сегмент СОИБ ОКИИ
Network Interfaces - Inside	
Virtual context	Inside
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Серверный АСУТП
Interface HA	
Chosen Interfaces	<Уточняется на этапе реализации>
Operation Mode	Active-Backup
Comment	Интерфейс синхронизации
ARMA СТЕНА К1000 (кластер 2)	
Network Interfaces – Outside	
Virtual context	Outside
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Внешний интерфейс до ПАК МЭ корпоративной сети передачи данных
Network Interfaces – DMZ	
Virtual context	DMZ
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Сегмент ДМЗ ТСПД для взаимодействия ТСПД с КСПД
Network Interfaces – SOIB_OKII	
Virtual context	SOIB_OKII
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>

Параметр	Значение
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Сегмент СОИБ ОКИИ
Network Interfaces - Inside	
Virtual context	Inside
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Серверный АСУТП
Interface HA	
Chosen Interfaces	<Уточняется на этапе реализации>
Operation Mode	Active-Backup
Comment	Интерфейс синхронизации
ARMA СТЕНА К1000 (кластер 3)	
Network Interfaces – Outside	
Virtual context	Outside
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Внешний интерфейс до ПАК МЭ корпоративной сети передачи данных
Network Interfaces – DMZ	
Virtual context	DMZ
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Сегмент ДМЗ ТСПД для взаимодействия ТСПД с КСПД
Network Interfaces – SOIB_OKII	
Virtual context	SOIB_OKII
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>

Параметр	Значение
Allow access	<Уточняется на этапе реализации>
Comment	Сегмент СОИБ ОКИИ
Network Interfaces - Inside	
Virtual context	Inside
Addressing mode	static
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	Серверный АСУТП
Interface HA	
Chosen Interfaces	<Уточняется на этапе реализации>
Operation Mode	Active-Backup
Comment	Интерфейс синхронизации

Таблица 1.12 – Настройки маршрутизации

Адрес назначения	Шлюз (Gateway)	Примечание
ARMA СТЕНА К1000 (кластер 1)		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
ARMA СТЕНА К1000 (кластер 2)		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
ARMA СТЕНА К1000 (кластер 3)		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

Таблица 1.13 – Базовые параметры профиля IPS

Параметр	Значение
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

Таблица 1.14 – Настройки профиля IPS

Параметр	Значение
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

1.4 Подсистема криптографической защиты

Описание настроек подсистемы криптографической защиты приведены в Таблица 1.15, Таблица 1.16, Таблица 1.17, Таблица 1.18, Таблица 1.18.

Таблица 1.15 – Сетевые настройки серверных компонентов

Компонент	Наименование параметра	Значение
С-Терра Шлюз 1000 (МДП г. Нижнекамск)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (МДП г. Казань)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ Охранный КУ)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 18 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 23 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>

Компонент	Наименование параметра	Значение
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 29 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 31 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 38 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 40 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 42 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>

Компонент	Наименование параметра	Значение
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 45 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 60 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 79 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 99 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 119 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>

Компонент	Наименование параметра	Значение
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 137 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 156 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ УПЗОУ 176 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 194 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (КУ 213 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>

Компонент	Наименование параметра	Значение
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ КУ 232 км)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>
С-Терра Шлюз 1000 (БКТМ Охранный КУ Казанской КС)	Host Name	<Уточняется на этапе реализации>
	Domain Name	<Уточняется на этапе реализации>
	IP-address/mask	<Уточняется на этапе реализации>
	Primary DNS Server	<Уточняется на этапе реализации>
	Secondary DNS Server	<Уточняется на этапе реализации>
	NTP Server	<Уточняется на этапе реализации>
	Device priority	<Уточняется на этапе реализации>

Таблица 1.16 – Настройки сетевых интерфейсов

Параметр	Значение
МДП г. Нижнекамск	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
МДП г. Казань	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ Охранный КУ	
Network Interfaces – <Уточняется на этапе реализации>	

Параметр	Значение
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 18 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 23 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 29 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 31 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>

Параметр	Значение
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 38 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 40 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 42 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 45 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>

Параметр	Значение
БКТМ КУ 60 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 79 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 99 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 119 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 137 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>

Параметр	Значение
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 156 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ УПЗОУ 176 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 194 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 213 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>

Параметр	Значение
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ КУ 232 км	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>
БКТМ Охранной КУ Казанской КС	
Network Interfaces – <Уточняется на этапе реализации>	
Virtual context	<Уточняется на этапе реализации>
Addressing mode	<Уточняется на этапе реализации>
IPv4 address	<Уточняется на этапе реализации>
Subnet mask	<Уточняется на этапе реализации>
Type	<Уточняется на этапе реализации>
Interface Members	<Уточняется на этапе реализации>
Allow access	<Уточняется на этапе реализации>
Comment	<Уточняется на этапе реализации>

Таблица 1.17 – Настройки маршрутизации

Адрес назначения	Шлюз (Gateway)	Примечание
МДП г. Нижнекамск		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
МДП г. Казань		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ Охранный КУ		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 18 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 23 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 29 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 31 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

Адрес назначения	Шлюз (Gateway)	Примечание
БКТМ КУ 38 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 40 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 42 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 45 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 60 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 79 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 99 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 119 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 137 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 156 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ УПЗОУ 176 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 194 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 213 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ КУ 232 км		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
БКТМ Охранный КУ Казанской КС		
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

Таблица 1.18 – Дополнительные параметры

Параметр	Значение
МДП г. Нижнекамск	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
МДП г. Казань	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ Охранный КУ	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 18 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 23 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 29 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>

Параметр	Значение
БКТМ КУ 31 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 38 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 40 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 42 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 45 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 60 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 79 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата

Параметр	Значение
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 99 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 119 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 137 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 156 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ УПЗОУ 176 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 194 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>

Параметр	Значение
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 213 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ КУ 232 км	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>
БКТМ Охранный КУ Казанской КС	
Тип идентификации	identity dn идентификации будет использоваться поле DN сертификата
Параметры для IPsec	esp-gost28147-4m-imit
Пул из которого будет выдан адрес клиенту	<Уточняется на этапе реализации>
Расширенный список доступа	<Уточняется на этапе реализации>

1.5 Подсистема антивирусной защиты

Описание настроек подсистемы антивирусной защиты приведены ниже в Таблица 1.19, Таблица 1.20 – Таблица 1.21.

Таблица 1.19 – Описание аппаратной платформы

Параметр	Значение
Процессор	<Уточняется на этапе реализации>
Оперативная память	<Уточняется на этапе реализации>
Жесткий диск (свободное место)	<Уточняется на этапе реализации>
Операционная система	Windows 11
IP-адрес	<Уточняется на этапе реализации>
Hostname	<Уточняется на этапе реализации>
FQDN	<Уточняется на этапе реализации>
Mask	<Уточняется на этапе реализации>
Default Gateway	<Уточняется на этапе реализации>
DNS-серверы	<Уточняется на этапе реализации>

Таблица 1.20 – Перечень АРМ пользователей и серверов

Тип устройства	IP-адреса
АРМ пользователей	<Уточняется на этапе реализации>
Серверы	<Уточняется на этапе реализации>

Таблица 1.21 – Описание настроек Kaspersky Industrial Cybersecurity for Nodes

Настройки	Значения настроек
Endpoint control	
Enable Device Control	Включено
Endpoint control → Device Control → Types of Device	<Уточняется на этапе реализации>
Endpoint control → Device Control → Connection buses	<Уточняется на этапе реализации>
Endpoint control → Device Control → Trusted devices	<Уточняется на этапе реализации>
Anti-Virus protection	
Start Kaspersky Industrial Cybersecurity for Nodes on computer startup	Включено
Enable Advanced Disinfection technology	Включено
Detection of the following object types is enabled (Settings): Malware: Viruses and worms Trojan programs Malicious tools Adware, auto-dialers, other programs Adware Auto-dialers Other Compressed files Packed files that may cause harm Multi-packed files	 Включено Включено Включено Включено Включено Отключено Включено Включено
Exclusions and trusted applications (Settings - Exclusions)	Значение по умолчанию. *<Дополнительные параметры уточняются на этапе реализации>*
Exclusions and trusted applications (Settings - Trusted applications)	<Уточняется на этапе реализации>
Anti-Virus protection → File Anti-Virus	
Enable File Anti-Virus Select action: Disinfect Delete	Включено Отключено Отключено
Security Level (Settings → General): File types Protection Scope: All removable drives All hard drives All network drives	 All Files Включено Включено Отключено
Security Level (Settings → Performance): Scan methods: Signature Analysis	 Включено

Настройки	Значения настроек
Heuristic Analysis	Включено (light scan)
Scan optimization:	
Scan only new and charged files	Включено
Scan of compound files:	
Scan archives	Включено
Scan installation packages	Отключено
Scan embedded OLE objects	Включено
Additional…	
Extract compound files in the background	Включено
Minimum file size	0 MB
Do not unpack large compound files	Включено
Maximum file size	15 MB
Security Level (Settings → Additional):	
Scan mode	Smart mode
Scan technologies	
iSwift Technology	Включено
iChecker Technology	Включено
Pause task	
By schedule	Отключено
At application startup	Отключено
Anti-Virus protection → Firewall	
Enable Firewall	Отключено
Anti-Virus protection → Network Attack Blocker	
Enable Network Attack Blocker	Отключено
Anti-Virus protection → System Watcher	
Enable System Watcher	Включено
Enable Exploit Prevention	Включено
Log application activity for the BSS database	Включено
Do not monitor the activity of applications that have a digital signature	Включено
Rollback malware actions during disinfection	Включено
Use behavior stream signatures (BSS)	Включено
On detecting malware activity	Skip
Anti-Virus protection → Scheduled tasks	
Update	Automatically
Full Scan	Manually
Critical Areas Scan	Every 1 day(s) at 17:00
Custom Scan	Manually
Perform Idle Scan	Отключено
Action on removable drive connection	Quick Scan
Maximum removable drive size	Отключено
Anti-Virus protection → Advanced Settings	
Advanced Protection Settings:	
Enable Self-Defense	Включено
Disable external management of the system service	Включено
Send dump and trace files to Kaspersky Lab for analysis	Отключено
Operating mode:	
Do not start scheduled tasks while running on battery power	
Concede resources to other applications	Включено

Настройки	Значения настроек
	Отключено
Anti-Virus protection → Advanced Settings → Reports and Storages	
Store reports no longer than	Включено (90 days)
Maximum file size	Включено (4096 MB)
Rescan Quarantine after update	Включено
Store objects no longer than	Включено (30 days)
Maximum storage size	Отключено
Anti-Virus protection → Advanced Settings → KSN Settings	
I accept the terms of the KSN Statement and would like to participate in KSN	Включено
Use KSN to scan and categorize files. Used by components: File Antivirus Scan Tasks System Watcher	Включено Включено Включено Отключено
Anti-Virus protection → Advanced Settings → Interface	
Use icon animation while running tasks	Включено
Enable password protection	Включено
Settings…	Значение по умолчанию. *<Дополнительные параметры уточняются на этапе реализации>*

1.6 Подсистема анализа защищенности

Описание настроек подсистемы анализа защищенности приведены в Таблица 1.22, Таблица 1.23, Таблица 1.24, Таблица 1.25, Таблица 1.26.

Таблица 1.22 – Описание аппаратной платформы

Параметр	Значение
Процессор	<Уточняется на этапе реализации>
Оперативная память	<Уточняется на этапе реализации>
Жесткий диск (свободное место)	<Уточняется на этапе реализации>
Операционная система	Windows 11
IP-адрес	<Уточняется на этапе реализации>
Hostname	<Уточняется на этапе реализации>
FQDN	<Уточняется на этапе реализации>
Mask	<Уточняется на этапе реализации>
Default Gateway	<Уточняется на этапе реализации>
DNS-серверы	<Уточняется на этапе реализации>

Таблица 1.23 – Диапазоны IP-адресов для проведения сканирования

Тип устройства	IP-адреса
АРМ пользователей	<Уточняется на этапе реализации>
Серверы	<Уточняется на этапе реализации>
Сетевое оборудование	<Уточняется на этапе реализации>

Таблица 1.24 – Меню «Настройки обновления»

Параметр	Значение
Сервер обновлений	Один из следующих серверов: update.maxpatrol.com update1.maxpatrol.com update3.maxpatrol.com
Порт	tcp/443
Имя пользователя	<Уточняется на этапе реализации>
Пароль авторизации при доступе	<Задается администратором>
Фильтр	Получать только одобренные обновления
Режим обновления	Вручную
Расписание	<Отсутствует>

Таблица 1.25 – Меню «Сканирования → Профили»

Параметр	Значение
Поиск узлов	— Количество потоков для поиска – 50; — Время поиска одного хоста – 2 с; — TCP Ping включен; — ICMP Ping включен — Порты: 21-23/tcp; 25/tcp; 53/tcp; 80/tcp; 110/tcp; 111/tcp; 113/tcp; 135/tcp; 139/tcp; 143/tcp; 389/tcp; 443/tcp; 445/tcp; 563/tcp; 636/tcp; 990/tcp; 993/tcp; 995/tcp; 1521/tcp; 1723/tcp; 1433/tcp; 3128/tcp; 3306/tcp; 3372/tcp; 3389/tcp; 4899/tcp; 5432/tcp; 8080/tcp
Учетные записи	— FTP – использовать анонимный вход — SMB – не использовать.
Настройки сканирования	
Сканер портов	— Не производить сканирование сетевых принтеров –да; — Ограничивать количество одновременных соединений – да; — Количество потоков для поиска – 50; — Список портов: 1-1674/tcp;1698-2028/tcp;2030/tcp;2032-2035/tcp;2038/tcp;2040-2049/tcp;2064-2065/tcp;2067/tcp;2080-2081/tcp;2087/tcp;2089-2112/tcp;2115/tcp;2120/tcp;2140/tcp;2189/tcp;2199-2202/tcp;2205/tcp;2211/tcp;2220/tcp;2222-2223/tcp;2230/tcp;2232/tcp;2241/tcp;2300-2302/tcp;2305/tcp;2307/tcp;2345/tcp;2381/tcp;2400-2402/tcp;2405/tcp;2407/tcp;2430-2433/tcp;2500-2502/tcp;2505/tcp;2525/tcp;2538/tcp;2543/tcp;2550/tcp;2564-2565/tcp;2583/tcp;2600-2605/tcp;2627/tcp;2638-2642/tcp;2700-2702/tcp;2705/tcp;2766/tcp;2773-2774/tcp;2784/tcp;2800-2802/tcp;2805/tcp;2869/tcp;2900-2902/tcp;2905/tcp;2967/tcp;2984-2985/tcp;2998-3025/tcp;3049-3055/tcp;3064/tcp;3067/tcp;3086/tcp;3100-3119/tcp;3121-3123/tcp;3125-3160/tcp;3180/tcp;3200-3211/tcp;3227/tcp;3233/tcp;3264/tcp;3268-3269/tcp;3300-3302/tcp;3305-3310/tcp;3323/tcp;3264/tcp;3268-3269/tcp;3300-3302/tcp;3305-3310/tcp;3323/tcp;3325/tcp;3333/tcp;3351/tcp;3372/tcp;3389-3393/tcp;3400-3402/tcp;3600-3602/tcp;3666/tcp;3679/tcp;3685/tcp;3700-3702/tcp;3800-3802/tcp;3900-3902/tcp;3984-3986/tcp;4000-4004/tcp;4008/tcp;4045/tcp;4080-4081/tcp;4092/tcp;4100-4102/tcp;4128/tcp;4132-4133/tcp;4144/tcp;4200-4202/tcp;4421/tcp;4444/tcp;4453/tcp;4469/tcp;4478/tcp;4480/tcp;4500-4502/tcp;4557/tcp;4559/tcp;4567/tcp;4589-4590/tcp;4600-4602/tcp;4661-4663/tcp;4672/tcp;4700-4702/tcp;4800-4802/tcp;4898-4902/tcp;5000-5005/tcp;5010-5011/tcp;5044-5045/tcp;5050/tcp;5060/tcp;5100-5102/tcp;5145/tcp;5190-

Параметр	Значение
	5193/tcp;5200-5202/tcp;5222/tcp;5232/tcp;5236/tcp;5238-5239/tcp;5300-5308/tcp;5321/tcp;5373/tcp;5375/tcp;5400-5402/tcp;5432-5436/tcp;5500-5502/tcp;5510/tcp;5520/tcp;5530/tcp;5550/tcp;5554-5557/tcp;5560/tcp;5569/tcp;5600-5602/tcp;5631-5632/tcp;5678-5680/tcp;5700-5702/tcp;5560/tcp;5569/tcp;5600-5602/tcp;5631-5632/tcp;5678-5680/tcp;5700-5702/tcp;5713-5717/tcp;5729-5732/tcp;5742/tcp;5800-5802/tcp;5882/tcp;5900-5902/tcp;5977-5979/tcp;5997-6009/tcp;6050/tcp;6097/tcp;6100-6102/tcp;6105-6106/tcp;6110-6112/tcp;6129/tcp;6141-6148/tcp;6200-6202/tcp;6300-6302/tcp;6400-6402/tcp;6500-6502/tcp;6558/tcp;6600-6602/tcp;6665-6671/tcp;6676-6677/tcp;6699-6702/tcp;6771/tcp;6778/tcp;6789-6790/tcp;6800-6802/tcp;6900-6902/tcp;6939/tcp;6969-6970/tcp;7000-7010/tcp;7020-7023/tcp;7100-7102/tcp;7200-7202/tcp;7215/tcp;7300-7302/tcp;7306-7308/tcp;7326/tcp;7400-7402/tcp;7500-7502/tcp;7597/tcp;7600-7602/tcp;7643/tcp;7700-7702/tcp;7777/tcp;7786/tcp;7789/tcp;7800-7802/tcp;7900-7902/tcp;7937-7938/tcp;7950-7951/tcp;8000-8010/tcp;8020/tcp;8025/tcp;8053/tcp;8080-8111/tcp;8129-8130/tcp;8195/tcp;8197/tcp;8200-8202/tcp;8220/tcp;8223/tcp;8300-8302/tcp;8383/tcp;8390/tcp;8400-8402/tcp;8470-8480/tcp;8500-8502/tcp;8600-8602/tcp;8646/tcp;8700-8702/tcp;8721/tcp;8765/tcp;8800-8802/tcp;8880/tcp;8888-8890/tcp;8892/tcp;8900-8902/tcp;9000-9004/tcp;9090/tcp;9097/tcp;9100-9102/tcp;9200-9202/tcp;9300-9302/tcp;9400-9402/tcp;9500-9502/tcp;9535/tcp;9600-9602/tcp;9700-9702/tcp;9800-9802/tcp;9872-9876/tcp;9900-9902/tcp;9989-10007/tcp;10080/tcp;10082-10083/tcp;10113-10115/tcp;10128/tcp;10167-10168/tcp;10288/tcp;10520/tcp;10607/tcp;11000-11001/tcp;11067/tcp;11111/tcp;11201/tcp;11223-11224/tcp;11319/tcp;11367/tcp;11371/tcp;11720/tcp;12000-12004/tcp;12076/tcp;12172/tcp;12223/tcp;12345-12346/tcp;12349/tcp;12361-12363/tcp;12631/tcp;12753/tcp;13000-13001/tcp;13160/tcp;13223-13224/tcp;13266/tcp;13579/tcp;13720-13722/tcp;13724/tcp;13782-13783/tcp;13818-13822/tcp;14000-14001/tcp;14936-14937/tcp;15000-15001/tcp;15100-15102/tcp;15345/tcp;16000-16001/tcp;16360-16361/tcp;16367-16368/tcp;16769/tcp;16969/tcp;16991/tcp;17000-17001/tcp;17007/tcp;17185/tcp;17300/tcp;17569/tcp;18000-18001/tcp;18181-18185/tcp;18187/tcp;18463/tcp;18888/tcp;19000-19001/tcp;19191/tcp;19283/tcp;19315/tcp;19398/tcp;19410-19412/tcp;19541/tcp;19638/tcp;20000-20001/tcp;20005/tcp;20034/tcp;20168/tcp;20222/tcp;20670/tcp;20999-21001/tcp;21227/tcp;21234/tcp;21554/tcp;21571/tcp;21590/tcp;21845-21849/tcp;22000-22001/tcp;22222/tcp;22273/tcp;22289/tcp;22305/tcp;22321/tcp;22555/tcp;22800/tcp;22951/tcp;23000-23001/tcp;23430/tcp;23456/tcp;23476-23477/tcp;24000-24006/tcp;24242/tcp;24249/tcp;24386/tcp;24554/tcp;24677/tcp;25000-25001/tcp;25356/tcp;25837-25840/tcp;26000-26001/tcp;26208/tcp;26274/tcp;27000-27001/tcp;27374/tcp;27665/tcp;28000-28001/tcp;29000-29001/tcp;30000-30001/tcp;30100-30102/tcp;30129/tcp;30303/tcp;30999-31001/tcp;31234/tcp;31337-31339/tcp;31666/tcp;31785/tcp;31787-31789/tcp;31791-31792/tcp;32000-32001/tcp;32123/tcp;32556-32557/tcp;32764/tcp;32770-32800/tcp;33000-33001/tcp;33333/tcp;34000-34001/tcp;34010-34020/tcp;34324/tcp;34567/tcp;35000-35001/tcp;36000-36001/tcp;36794/tcp;37000-37001/tcp;37900/tcp;38000-38001/tcp;39000-39001/tcp;40000-40001/tcp;40193/tcp;40412/tcp;40421-40423/tcp;40426/tcp;41000-41001/tcp;41234/tcp;42000-42001/tcp;43000-43001/tcp;43188/tcp;44000-44001/tcp;44333-44337/tcp;44401-44409/tcp;44444/tcp;45000-45001/tcp;45678/tcp;46000-46001/tcp;47000-47001/tcp;47557/tcp;48000-48001/tcp;49000-49001/tcp;50000-50001/tcp;50080/tcp;50443/tcp;50505/tcp;50766/tcp;51000-51001/tcp;51054/tcp;51080/tcp;51234/tcp;51266/tcp;51443/tcp;52000-

Параметр	Значение
	52001/tcp;52080/tcp;52111/tcp;52443/tcp;53000-53001/tcp;54000-54001/tcp;54283/tcp;54320-54321/tcp;55000-55001/tcp;55555/tcp;56000-56001/tcp;56789/tcp;57000-57001/tcp;58000-58001/tcp;59000-59001/tcp;60000-60001/tcp;61000-61001/tcp;61234/tcp;61466/tcp;62000/tcp;62002/tcp;63000-63001/tcp;64000-64001/tcp;65000-65002/tcp;65301/tcp;65363/tcp
Сканер UDP-сервисов	Сканировать UDP-порты – указать все
Идентификация сервисов	— Эвристический метод определения открытых портов – да; — Эвристический метод определения версий служб – да.
Сканер уязвимостей	— Искать уязвимости – да; — Определять уязвимости по баннерам – определять все баннерные уязвимости; — Проверять на известные DoS-атаки – Нет; — Проверять на новые DoS-атаки (эвристический метод) – Нет; — HTTP – указать все; — Анализатор контента: o Использовать словарь при сборе контента – да; o Искать старые файлы – да; o Искать вредоносный код в страницах; o Время ожидания HTTP-пакетов (сек.) – 8; o Максимальное количество применяемых прикладных сценариев – 100; o Количество циклов вложенных проверок – 10; — Анализатор сценариев: o Поиск уязвимостей в GET-запросах – да; o Поиск уязвимостей в POST-запросах – да; o Типы уязвимостей – указать все; o Метод поиска – указать все; — FTP o искать скрытые каталоги; — TFTP: o искать файлы на TFTP-сервере; o имена файлов – tftp-files — LDAP: o Максимальное количество записей RDN первого уровня – 20; o Максимальное количество атрибутов в каждом RDN – 50; — Подбор учетных записей – Нет.

Таблица 1.26 – Меню «Отчет по сканированию»

Параметр	Значение
Тип отчета	Информация
Исходные данные	По задаче / задачам
идентификация узлов	Как в задаче
Тип данных	Уязвимости PenTest
Выбор скана	Последний скан
Выбор задачи	Указать сформированные ранее
Способ предоставления данных	По уязвимостям

1.7 Подсистема регистрации и обработки событий безопасности

Описание настроек подсистемы регистрации и обработки событий безопасности приведены в Таблица 1.27, Таблица 1.28, Таблица 1.29.

Таблица 1.27 – Описание аппаратной платформы

Параметр	Значение
Процессор	<Уточняется на этапе реализации>
Оперативная память	<Уточняется на этапе реализации>
Жесткий диск (свободное место)	<Уточняется на этапе реализации>
Операционная система	Windows 11
IP-адрес	<Уточняется на этапе реализации>
Hostname	<Уточняется на этапе реализации>
FQDN	<Уточняется на этапе реализации>
Mask	<Уточняется на этапе реализации>
Default Gateway	<Уточняется на этапе реализации>
DNS-серверы	<Уточняется на этапе реализации>

Таблица 1.28 – Перечень нормализаторов

Наименование источника в системе	Наименование нормализатора	Порт API
[LIS] Windows_WMI	[LIS] Windows Extended	<Уточняется на этапе реализации>
[LIS] KSC_SQL	[LIS] KSC from SQL	<Уточняется на этапе реализации>
[LIS] InfoWatch ARMA	[LIS] ARMA	<Уточняется на этапе реализации>
[LIS] CyberBackup	[LIS] CyberBackup	<Уточняется на этапе реализации>
[LIS] STerra	[LIS] STerra	<Уточняется на этапе реализации>

Таблица 1.29 – Описание правил корреляции

Категория	Имя сценария	Описание условия	Наименование правила
Атака на отказ в обслуживании	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
Вредоносная сетевая активность	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
Заражение вредоносным ПО	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
Нелегитимная административная активность	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
Компрометация узла	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
Компрометация учетной записи	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

Категория	Имя сценария	Описание условия	Наименование правила
Нарушение политик безопасности	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
Несанкционированный доступ к системам	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

1.8 Подсистема резервного копирования

Описание настроек подсистемы резервного копирования приведены в Таблица 1.30, Таблица 1.29, Таблица 1.30, Таблица 1.31 Таблица 1.32.

Таблица 1.30 – Описание аппаратной платформы

Параметр	Значение
Процессор	<Уточняется на этапе реализации>
Оперативная память	<Уточняется на этапе реализации>
Жесткий диск	<Уточняется на этапе реализации>
Операционная система	Astra Linux Special Edition 1.8
IP-адрес	<Уточняется на этапе реализации>
Hostname	<Уточняется на этапе реализации>
FQDN	<Уточняется на этапе реализации>
Mask	<Уточняется на этапе реализации>
Default Gateway	<Уточняется на этапе реализации>
DNS-серверы	<Уточняется на этапе реализации>

Таблица 1.31 – Описание настроек системного программного обеспечения

Параметр	Значение
Системное ПО	
Кибер Бекап	Management Server
	Components for Remote Installation
	Agent for Windows
	Bootable Media Builder
	Command-Line Tool
	Cyber Backup Monitor
	PXE Server
	Storage Node
	Catalog Service
Используемая БД	SQLite (без использования второй БД под malware protection)
Учетная запись служб	Local System
Управляемое хранилище	
Имя хранилища	<Уточняется на этапе реализации>
Тип доступа	Файловый (NFS)
Расположение хранилища	/backup

Параметр	Значение
Объем хранилища	<Уточняется на этапе реализации>
Дедупликация	Включена
Защита паролем	Отключена
Служба каталогизации	<Уточняется на этапе реализации>

Таблица 1.32 – Перечень резервируемых компонент

Наименование	Состав объектов резервирования	Объем	Срок хранения
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>
<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>	<Уточняется на этапе реализации>

Таблица регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в док.	Номер док.	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных				

АО НИП «ИНФОРМЗАЩИТА»

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Реконструкция линейного сооружения - имущественный комплекс «Управление этиленопроводов» на участке Нижнекамск – Казань. Модернизация объектов для транспортировки этилена с учётом дополнительных объемов от ЭП-600»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Предварительная спецификация на СОИБ

НКНХ.5273-ПД-ИБ1-В4

2024

СОДЕРЖАНИЕ

Лист

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	НКНХ.5273-ПД-ИБ1-В4		
Разраб.		Черкасов			11.09.24	Предварительная спецификация на СОИБ	Стадия	Лист	Листов
							П	1	11
Н. контр.		Скиткин			11.09.24		Информзащита Системный интегратор		
ГИП		Черкасов			11.09.24				

1 ОБЩИЕ СВЕДЕНИЯ

Наименование работ: предварительное категорирование объектов критической информационной инфраструктуры (далее – ОКИИ) магистрального этиленопровода «Нижнекамск - Казань» ПАО «Нижнекамскнефтехим».

Генеральный заказчик: ПАО «Нижнекамскнефтехим».

Заказчик: ООО «Прогресс Инжиниринг».

Подрядчик: Акционерное общество НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ «ИНФОРМЗАЩИТА» (АО НИП «ИНФОРМЗАЩИТА»).

Основание для проведения работ: Договор № 0085.2023 от 27.05.2024, заключенному между Заказчиком и Подрядчиком.

Цель работ: сбор информации, на основании которой будет составлен Перечень основных угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры, будет актуализировано категорирование ОКИИ, будут актуализированы проекты Актов категорирования ОКИИ и Сведения о результатах категорирования ОКИИ, которые будет необходимо направить в ФСТЭК России.

Нормативная база: настоящий документ разработан в соответствии с требованиями следующих нормативных документов:

1) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2) Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3) Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Область проведения работ: в область проведения работ включены следующие ОКИИ магистрального этиленопровода «Нижнекамск – Казань» ПАО «Нижнекамскнефтехим» (Таблица 1.1):

Таблица 1.1 – Область проведения работ

№ п/п	Наименование ОКИИ	Тип ОКИИ	Сфера (область) деятельности, в которой функционирует ОКИИ	Критические процессы, в которых используется ОКИИ
1	Автоматизированная система управления технологическим процессом (АСУТП)	АСУ	Химическая промышленность	Транспортировка этилена

№ п/п	Наименование ОКИИ	Тип ОКИИ	Сфера (область) деятельности, в которой функционирует ОКИИ	Критические процессы, в которых используется ОКИИ
2	Автоматизированная система диспетчерского управления энергоснабжением (АСДУЭ)	АСУ	Химическая промышленность	Обеспечение автоматического и автоматизированного управления оборудованием электроснабжения
3	Автоматическая система противопожарной защиты (АСПЗ)	АСУ	Химическая промышленность	–
4	Локальная система оповещения (ЛСО)	АСУ	Химическая промышленность	–
5	Структурированная система мониторинга и управления инженерными системами зданий и сооружений (СМИС)	АСУ	Химическая промышленность	–
6	Система пожарной сигнализации (СПС)	АСУ	Химическая промышленность	–
7	Комплекс инженерно-технических средств охраны (КИТСО)	АСУ	Химическая промышленность	–

2 СПЕЦИФИКАЦИЯ ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

№ строки	Наименование	Код продукции	Обозначение документа на поставку	Поставщик	Куда входит (обозначение)	Количество				Примечание
						на изделие	в комплекты	на регулир.	Всего	
Подсистема межсетевого экранирования										
1	Программно-аппаратный комплекс "Межсетевой экран ARMAIF-19RACK-K1000"	—	—	InfoWatch	—	8	—	—	8	—
2	Сертификат на техническую поддержку программно-аппаратного комплекса "Межсетевой экран ARMAIF-19RACK-K1000", срок действия 3 года	—	—	InfoWatch	—	8	—	—	8	—
3	Лицензия Enterprise Модуль централизованного управления (по количеству подключаемых источников событий)	—	—	InfoWatch	—	4	—	—	4	—
4	Лицензия Enterprise Модуль сбора и анализа событий	—	—	InfoWatch	—	4	—	—	4	—
5	Лицензия Enterprise Модуль корреляции событий, управления и реакции на инциденты ИБ	—	—	InfoWatch	—	4	—	—	4	—
6	Сервер «Гравитон» 2101ИВ	—	—	Гравитон	—	1	—	—	1	Минимальные требования к аппаратному обеспечению: – Процессор - 2,0 ГГц, четырехъядерный, x64 или Байкал-М (ARMv8) – ОЗУ - 16 ГБ – Жесткий диск - 512 ГБ, SSD
Подсистема антивирусной защиты										
7	Kaspersky Certified Media Pack Customized	KL8069RMZZZ	—	Лаборатория Касперского	—	1	—	—	1	—
8	Kaspersky Industrial CyberSecurity for Nodes, Workstation, Enterprise Russian Edition. 1-25 Node 3 year Base License - Лицензия	KL4941RAPTS	—	Лаборатория Касперского	—	19	—	—	19	Workstation - Только для АРМ Windows, количество уточнить по результатам проектирования
9	Kaspersky Industrial CyberSecurity for Nodes, Server, Enterprise Russian Edition. 1-10 Node 3 year Base License	KL4943RAKTS	—	Лаборатория Касперского	—	10	—	—	10	for Server для всех серверов, а также АРМ на Linux, количество уточнить по результатам проектирования
10	Kaspersky Стандартный Certified Media Pack Russian Edition. Media Pack - Установочный комплект, программное обеспечение	KL8067RMZZZ	—	Лаборатория Касперского	—	1	—	—	1	—
11	Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition. 1-10 Node 3 year Base License	KL4867RAKTS	—	Лаборатория Касперского	—	7	—	—	7	—
12	Сервер «Гравитон» 2101ИВ	—	—	Гравитон	—	1	—	—	1	Рекомендуемые требования к аппаратному обеспечению: – Процессор: 2.4 ГГц четырехъядерный. – Оперативная память: 2 ГБ. – Объем свободного места на диске: 4ГБ.

№ строки	Наименование	Код продукции	Обозначение документа на поставку	Поставщик	Куда входит (обозначение)	Количество				Примечание
						на изделие	в комплекты	на регулир.	Всего	
13	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи диск, серверная до 2 сокетов, на срок действия исключительного права, с включенными обновлениями Тип 1 на 36 мес	OS2101X8617DSKSKTSR01-SO36	—	Astra Linux	—	1	—	—	1	—
Подсистема контроля конфигураций										
14	Неисключительное право на использование "Efros DefOps Integrity Check Compliance"	EDO-ICC-SRV	—	Газинформсервис	—	1	—	—	1	—
15	Расширенная техническая поддержка на "Efros DefOps Integrity Check Compliance" (на три года)	EDO-ICC-SRV-SPE	—	Газинформсервис	—	3	—	—	3	—
16	Неисключительное право на использование "Efros DefOps ICC" (до 100 подключений операционных систем)	EDO-ICC-CLI-OS100	—	Газинформсервис	—	1	—	—	1	—
17	Расширенная техническая поддержка на "Efros DefOps ICC" (до 100 подключений операционных систем; на три года)	EDO-ICC-CLI-OS100-SPE	—	Газинформсервис	—	3	—	—	3	—
18	Сертифицированный установочный комплект "Efros DefOps" (дистрибутив; формуляр; сертификат)	EDO-IK-CERT	—	Газинформсервис	—	1	—	—	1	—
19	Неисключительное право на использование "Efros DefOps NA" (до 100 подключений)	EDO-NA-CLI-100	—	Газинформсервис	—	1	—	—	1	—
20	Сертификат расширенной технической поддержки на "Efros DefOps NA" (до 100 подключений; на три года)	EDO-NA-CLI-100-SPE	—	Газинформсервис	—	3	—	—	3	—
21	Неисключительное право на использование "Efros DefOps Network Assurance"	EDO-NA-SRV	—	Газинформсервис	—	1	—	—	1	—
22	Сертификат расширенной технической поддержки на "Efros DefOps Network Assurance" (на три года)	EDO-NA-SRV-SPE	—	Газинформсервис	—	3	—	—	3	—
23	Сертифицированный установочный комплект "Efros DefOps" (дистрибутив; формуляр; сертификат)	EDO-IK-CERT	—	Газинформсервис	—	1	—	—	1	—
24	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи диск, серверная до 2 сокетов, на срок действия исключительного права, с включенными обновлениями Тип 1 на 36 мес	OS2101X8617DSKSKTSR01-SO36	—	Astra Linux	—	1	—	—	1	—
25	Сервер «Гравитон» 2101ИВ	—	—	Гравитон	—	1	—	—	1	Требования к аппаратному обеспечению: – Процессор 16 ядер (от 2 ГГц) – Оперативная память, не менее Гб 32 Гб – Жесткий диск, Гб + (ПК + СУБД), не менее 600 Гб

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	№ док.	Подп.	Дата	НКНХ.5273-ПД-ИБ1-В4	Лист 5

№ строки	Наименование	Код продукции	Обозначение документа на поставку	Поставщик	Куда входит (обозначение)	Количество				Примечание
						на изделие	в комплекты	на регулир.	Всего	
Подсистема резервного копирования										
26	Кибер Бэкап Расширенная редакция для рабочей станции Linux	F16PCLANL	—	ООО «Киберпротект»	—	20	—	—	20	Количество уточняется на этапе РД
27	Сертификат на техническую поддержку ПО Кибер Бэкап Расширенная редакция для рабочей станции Linux	F16PCLANL-S	—	ООО «Киберпротект»	—	20	—	—	20	—
28	Сертификат на техническую поддержку ПО Кибер Бэкап Расширенная редакция для рабочей станции Linux Продление на 2 года	F16PCLA2RN	—	ООО «Киберпротект»	—	20	—	—	20	Количество уточняется на этапе РД
29	Базовый пакет для сертифицированной версии программного комплекса Кибер Бэкап 16 Расширенная редакция для рабочей станции Linux ФСТЭК	CB4337workstALinuxCert	—	ООО «Киберпротект»	—	20	—	—	20	Количество уточняется на этапе РД
30	Кибер Бэкап Расширенная редакция для физического сервера	F16PANL	—	ООО «Киберпротект»	—	16	—	—	16	Количество уточняется на этапе РД
31	Сертификат на техническую поддержку ПО Кибер Бэкап Расширенная редакция для физического сервера	F16PANL-S	—	ООО «Киберпротект»	—	16	—	—	16	Количество уточняется на этапе РД
32	Сертификат на техническую поддержку ПО Кибер Бэкап Расширенная редакция для физического сервера Продление на 2 года	F16PA2RN	—	ООО «Киберпротект»	—	16	—	—	16	Количество уточняется на этапе РД
33	Базовый пакет для сертифицированной версии программного комплекса Кибер Бэкап 16 Расширенная редакция для физического сервера ФСТЭК	CB4337servACert	—	ООО «Киберпротект»	—	16	—	—	16	Количество уточняется на этапе РД
34	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи диск, серверная до 2 сокетов, на срок действия исключительного права, с включенными обновлениями Тип 1 на 36 мес	OS2101X8617DSKSKTSR01-SO36	—	Astra Linux	—	1	—	—	1	—
35	Сервер «Гравитон» 2101ИВ	—	—	Гравитон	—	1	—	—	1	Рекомендуемые требования к аппаратному обеспечению: – Процессор - 2,0 ГГц, 12 ядер – ОЗУ – 32 ГБ – Жесткий диск - 2 ТБ, SSD
Подсистема защиты от НСД										
36	Право на использование модуля защиты от НСД и контроля устройств Средства защиты информации Secret N	SNS-8.x-NSD-NS-SP1Y	—	Код безопасности	—	30	—	—	30	Количество уточняется на этапе РД
37	Право на использование модуля защиты диска и шифрование контейнеров Средства защиты информации Secret Net Studio 8	SNS-8.x-DCR-NS-SP1Y	—	Код безопасности	—	30	—	—	30	Количество уточняется на этапе РД
38	Установочный комплект. Сертифицированное Средство защиты информации Secret Net Studio 8	SNS-F-DISC	—	Код безопасности	—	1	—	—	1	—

№ строки	Наименование	Код продукции	Обозначение документа на поставку	Поставщик	Куда входит (обозначение)	Количество				Примечание
						на изделие	в комплекты	на регулир.	Всего	
Подсистема криптографической защиты										
39	Аппаратный комплекс "С-Терра VPN" Версия 4.3 исполнение "3-1" - "С-Терра Шлюз ST КС1"	G-1000-4.3-1030-4-2SFP-ST-KC1	—	S-Terra	—	52	—	—	52	—
40	Лицензия на право использования ПО Программно-аппаратного комплекса "С-Терра VPN" Версия 4.3, исполнение "3-1" - "С-Терра Шлюз ST КС1"	LIC-1000-4.3-50-ST-KC1	—	S-Terra	—	52	—	—	52	—
41	Сертификат активации технической поддержки на 3 года	SCON-4.3-1000-50	—	S-Terra	—	52	—	—	52	—
42	Простая (неисключительная) лицензия на право использования программного продукта «С-Терра КП» Версия 4.3	LIC-KP-100-4.3	—	S-Terra	—	1	—	—	1	—
43	С-Терра КП, Система централизованного управления (сертификат активации технической поддержки на 3 года), Сертификат активации технической поддержки	SCON-4.3-KP-10	—	S-Terra	—	1	—	—	1	—
44	Лицензия КриптоПро CSP	—	—	ООО «КРИПТО-ПРО»	—	1	—	—	1	—
45	Программно-аппаратный комплекс "Соболь"	—	—	Код безопасности	—	1	—	—	1	—
46	Сертификат активации технической поддержки на 3 года Соболь	—	—	Код безопасности	—	1	—	—	1	—
47	ПО Microsoft Windows Server Standard 2019 64Bit English DVD 10 Clt 16 Core	P73-07701	—	Microsoft	—	1	—	—	1	—
48	Сервер «Гравитон» 2101ИВ	—	—	Гравитон	—	1	—	—	1	Рекомендуемые требования к аппаратному обеспечению: – Процессор - 2,0 ГГц, 12 ядер – ОЗУ – 32 ГБ – Жесткий диск - 2 ТБ, SSD
Подсистема анализа защищенности										
49	Гравитон Н17И-Т (Intel Core i7-1165G7, 1 Тб SSD)	Н17И-Т	—	Гравитон	—	1	—	—	1	—
50	XSpider. Лицензия на 512 хостов, обновления в течение 3 (трех) лет	PT-XS-IP512	—	Позитивные Технологии	—	1	—	—	1	—
Подсистема регистрации и обработки событий безопасности										
51	Kaspersky Unified Monitoring and Analysis Platform with Netflow support Russian Edition. 100-149 * 100 events per second 3 year Base Premium License - Лицензия	—	—	Лаборатория Касперского	—	1	—	—	1	—
52	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи диск, серверная до 2 сокетов, на срок действия исключительного права, с включенными обновлениями Тип 1 на 36 мес	OS2101X8617DSKSKTSR01-SO36	—	Astra Linux	—	1	—	—	1	—

№ строки	Наименование	Код продукции	Обозначение документа на поставку	Поставщик	Куда входит (обозначение)	Количество				Примечание
						на изделие	в комплекты	на регулир.	Всего	
53	Сервер «Гравитон» 2101ИВ		—	Гравитон		1	—	—	1	Серверы для установки коллекторов: Процессор: Intel или AMD от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 8 vCPU (виртуальных процессоров). ОЗУ: 16 ГБ. Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt. Серверы для установки коррелляторов: Процессор: Intel или AMD от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 8 vCPU (виртуальных процессоров). ОЗУ: 16 ГБ. Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt. Серверы для установки Ядра: Процессор: Intel или AMD от 2 ядер (4 потока) с поддержкой набора инструкций SSE 4.2 или 4 vCPU (виртуальных процессоров). ОЗУ: 12 ГБ. Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.
Коммутаторы СОИБ ОКИИ										
54	Ethernet-коммутатор MES2324, 24 порта 10/100/1000 Base-T, 4 комбо-порта 10/100/1000 Base-T/100/1000 Base-X (SFP) 220V AC	MES2324_AC	—	Элтекс	—	88	—	—	88	—
55	Продление гарантийного обслуживания, MES2324_AC, до 3 лет	EW-MES2324_AC-3Y	—	Элтекс	—	88	—	—	88	—
56	SFP модуль 1.25G (40 км), 2 волокна, 1310 нм, DDM, LC	FH-S3112CDL40	—	Элтекс	—	70	—	—	70	—
Серверный шкаф										
57	DYNAmic 19" Телекоммуникационный напольный шкаф 42U, 800x1000x2053, стеклянная двустворчатая передняя дверь, металлическая двустворчатая задняя дверь с кабельными вводами, цвет серый	LN-FS42U8010-LG-131	—	—	—	22	—	—	22	—

№ строки	Наименование	Код продукции	Обозначение документа на поставку	Поставщик	Куда входит (обозначение)	Количество				Примечание
						на изделие	в комплекты	на регулир.	Всего	
58	Кабельный желоб перфорированный оцинкованый, 42U, 100x10x1885 мм	LN-KDG-CMT-42UK-ZN	—	—	—	44	—	—	44	—
59	Кабельный органайзер горизонтальный 19" 1U, с 5 металлическими кольцами, 482x72x44мм, серый	LN-KDG-YKD-1UKN-LG	—	—	—	50	—	—	50	—
60	Электрическая распределительная панель 19" 3U, с DIN-рейкой, 482x123x133мм, универсальная, серая	LN-PRZ-MOD-3U15-LG	—	—	—	6	—	—	6	—
61	Полка стационарная 19" 1U, нагрузка 50 кг, 4 точки крепления, 486x770x30мм, для шкафов глубиной 1000мм, серая	LN-RAF-SBT-D100-LG	—	—	—	50	—	—	50	—
62	Цоколь для напольных шкафов LANDE, 800x1000x100мм, серый	LN-ZMN-BAZ-8010-LG	—	—	—	22	—	—	22	—
63	Модуль вентиляторный, 4 вентилятора, с механическим термостатом, 415x431x44мм, для напольных шкафов LANDE, серый	LN-FAN-THM-4FFS-LG	—	—	—	22	—	—	22	—

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	–	Автоматизированное рабочее место
АСУ	–	Автоматизированная система управления
АСУ ТП	–	Автоматизированная система управления технологического процесса
ВОЛС	–	Волоконно-оптическая линия связи
ДМЗ	–	Демилитаризированная зона
ИС	–	Информационная система
ИТС	–	Информационно-телекоммуникационная сеть
КИИ	–	Критическая информационная инфраструктура
КИП	–	Контрольно-измерительные приборы
ОКИИ	–	Объект критической информационной инфраструктуры
ОС	–	Операционная система
ПАЗ	–	Противоаварийная защита
ПЛК/PLC	–	Программируемый логический контроллер/ Programmable logic controller
ПО	–	Программное обеспечение
ППО	–	Прикладное программное обеспечение
РЗА	–	Релейная защита и автоматика
САО	–	Система аварийного останова
СЗИ	–	Средство защиты информации
СКУД	–	Система контроля и управления доступом
СОИБ	–	Система обеспечения информационной безопасности
СУБД	–	Система управления базами данных
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю
ЧМИ	–	Человеко-машинный интерфейс
MES	–	Manufacturing execution system/ Система управления производственными процессами

Таблица регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в док.	Номер док.	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных				