



**Общество с ограниченной ответственностью
«Производственное объединение
«ОРИОН-АКВА»**

Лицензия ФСТЭК №3313 от 20.06.2017 на деятельность по технической защите
конфиденциальной информации

Заказчик: ООО «Строительные решения. Специализированный застройщик»

Объект: Канализационная насосная станция для водоотведения объекта:
«Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами
обслуживания жилой застройки во встроенных помещениях по ул. Бронная в
Кировском районе г. Новосибирска»

РАБОЧАЯ ДОКУМЕНТАЦИЯ

Информационная безопасность

БКИТ.241388.КНС-Бронная-ИБ



**Общество с ограниченной ответственностью
«Производственное объединение
«ОРИОН-АКВА»**

Лицензия ФСТЭК №3313 от 20.06.2017 на деятельность по технической защите
конфиденциальной информации

Заказчик: ООО «Строительные решения. Специализированный застройщик»

Объект: Канализационная насосная станция для водоотведения объекта:
«Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами
обслуживания жилой застройки во встроенных помещениях по ул.
Бронная в Кировском районе г. Новосибирска»

РАБОЧАЯ ДОКУМЕНТАЦИЯ

Информационная безопасность

БКИТ.241388.КНС-Бронная-ИБ

Генеральный директор

_____ А.П. Андриянец

Инженер по защите информации

_____ С.С. Белогубов

Обозначение	Наименование	Примечание
БКИТ.241388.КНС-Бронная-ИБ.	Содержание	
	Текстовая часть	
	1. Общие положения	
	2. Описание АСУ ТП	
	3. Основные организационные решения	
	4. Основные технические решения	
	5. Мероприятия по подготовке к вводу СОИБ в действие	
	6. Перечень принятых сокращений и аббревиатур	
	Графическая часть	
БКИТ.241388.КНС-Бронная-ИБ.ГЧ	Структурная схема СОИБ АСУ ТП КНС "Бронная"	
БКИТ.241388.КНС-Бронная-ИБ.С	Спецификация оборудования СОИБ АСУ ТП КНС "Бронная"	
	Приложения:	
	Акт классификации АСУ ТП КНС "Бронная"	
БКИТ.241388.КНС-Бронная-ИБ.ОО	Обследование объектов управления и режимов работы АСУ ТП КНС "Бронная" с позиции информационной безопасности	
БКИТ.241388.КНС-Бронная-ИБ.ТЗ	Техническое задание на создание АСУ ТП КНС "Бронная"	
БКИТ.241388.КНС-Бронная-ИБ.МУ	Модель угроз АСУ ТП КНС "Бронная"	
	Регламент конфигурирования СЗИ	
	Техническое задание	

Взам.инв. N

Подпись и дата

Инв. N подл.

Изм.	Кол.уч.	Лист	Ледок	Подпись	Дата
Разработал	Белогубов				
Проверил	Скляров				
Н. контроль	Подкопаса				
Должность	Фамилия	Подпись	2023		

БКИТ.241388.КНС-Бронная-ИБ					
Канализационная насосная станция для водоотведения объекта: «Многоквартирные многоквартирные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска»					
Проект на создание СОИБ АСУ ТП			Стадия	Лист	Листов
			Р	1	34
			ООО "ПО "ОРИОН-АКВА"		

Обозначения и сокращения

АРМ Автоматизированное рабочее место

АСУ ТП Автоматизированная система управления технологическим процессом

ИС - Информационная система

КЗ - Контролируемая зона

ЛВС - Локальная вычислительная сеть

НСД - Несанкционированный доступ

ОС - Операционная система

ПО - Программное обеспечение

СВТ - Средство вычислительной техники

СЗИ - Средство защиты информации

УБИ - Угроза безопасности информации

ФСТЭК - Федеральная служба по техническому и экспортному контролю


КВО - Критически важный объект



ПЛК - Программируемый логический контроллер

КИПиА - Контрольно-измерительные приборы и автоматика.

СОИБ - Система обеспечения информационной безопасности

КНС - Канализационно-насосная станция

Согласовано:  Д.И. Токарев Д.С.

Изм.	Кол.уч	Лист	№док	Подпись	Дата	БКИТ.241388.КНС-Бронная-ИБ			
						Канализационная насосная станция для водоотведения объекта: «Множкквартирные многотажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроженных помещениях по ул. Бронная в Кировском районе г. Новосибирска»			
Разработал		Белогубов				Проект на создание СОИБ АСУ ТП	Стадия	Лист	Листов
Проверил		Скляров					Р	2	34
Н. контроль		Подкопаева					ООО "ПО "ОРИОН-АКВА"		
Должность		Фамилия		Подпись	2023				

Термины и определения

Автоматизированная система управления технологическим процессом - группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Защита информации - принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Средство защиты от несанкционированного доступа - программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Инв. N подл.	Подпись и дата	Взам. инв. N							Лист
Изм	Кол.уч.	Лист	NДокум	Подп.	Дата	БКИТ.241388.КНС-Бронная-ИБ			3

Модель угроз (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на технологический процесс в АСУ ТП.

Аутентификация - процедура проверки подлинности

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации в АСУ ТП.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Инв. N подл.	Подпись и дата	Взам. инв. N							БКИТ.241388.КНС-Бронная-ИБ	Лист
										4
			Изм	Кол.уч.	Лист	NДокум	Подп.	Дата		

1. Общие положения

1.1 Наименование проектируемой системы

Система обеспечения информационной безопасности в автоматизированной системе управления технологическим процессом канализационной насосной станции для водоотведения объекта: «Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска»; (далее СОИБ АСУ ТП КНС «Бронная»).

1.2 Цели создания

Канализационно-насосная станция предназначена для перекачивания канализационных стоков.

Целями создания СОИБ АСУ ТП КНС

- Обеспечение безопасности информации, обрабатываемой в АСУ ТП КНС
- Снижение вероятности реализации актуальных угроз безопасности информации в АСУ ТП и снижение вероятного ущерба в случае их реализации;
- Соответствие мер, принятых для обеспечения безопасности информации АСУ ТП, действующему законодательству Российской Федерации в сфере информационной безопасности.

1.3 Сведения о нормативно-правовых актах, использованных при проектировании

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

Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" (с изменениями и дополнениями);

- ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

- ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

Инв. N подл.	Подпись и дата	Взам. инв. N							БКИТ.241388.КНС-Бронная-ИБ	Лист 5
			Изм	Кол.уч.	Лист	NДокум	Подп.	Дата		

- ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
- ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

1.4 Условия производства работ

Производство работ осуществляется в помещениях объекта реконструкции без остановки рабочего процесса по установке и настройке устройств защиты информации. На объекте необходимо учесть, что работы выполняются на действующих объектах с наличием в зоне производства работ загромождающих предметов, вблизи объектов, находящихся под высоким напряжением. Принять необходимые меры для защиты и безопасности персонала.

1.5 Наименование предприятий (объединений) разработчика и заказчика (пользователя) системы и их реквизиты

Заказчик: ООО «Строительные решения. Специализированный застройщик»

Разработчик: Общество с ограниченной ответственностью производственное объединение «ОРИОН-АКВА». Адрес 630005, г. Новосибирск, ул. Писарева д. 53.

2. Описание АСУ ТП

2.1 Краткое описание защищаемой АСУ ТП

Канализационно-насосная станция предназначена для перекачивания канализационных стоков.

Автоматизированная система управления технологическими процессами канализационно-насосной станции предназначена для оперативного мониторинга параметров технологического процесса, автоматизированного контроля и управления технологическим процессом и сопутствующими локальными автоматическими подсистемами АСУ ТП.

Основным технологическим оборудованием КНС служат насосные агрегаты. Алгоритм работы насосов определяется уровнем жидкости в приемном резервуаре: при достижении значения рабочего уровня автоматически происходит запуск агрегата. При снижении количества стоков в ёмкости происходит отключение насоса. Реализована возможность автоматического чередования работы насосных агрегатов для равномерной их наработки

Более детальная информация о структуре АСУ ТП представлена в «Отчет по результатам обследования АСУ ТП КНС «Бронная»».

В соответствии с Актом определения класса защищенности АСУ ТП установлен класс защищённости - 3.

В системе не обрабатывается информация, содержащая сведения, составляющие

Взам. инв. N	
Подпись и дата	
Инв. N подл.	

						БКИТ.241388.КНС-Бронная-ИБ	Лист 6
Изм	Кол.уч.	Лист	NДокум	Подп.	Дата		

государственную тайну.

2.2 Описание информационных связей со смежными системами

Информационный обмен АСУ ТП осуществляется с подсистемой АСУ ТП КНС МУП г. Новосибирска «ГОРВОДОКАНАЛ», включающей в себя более 50-ти канализационно-насосных станций (КНС). Обмен осуществляется при помощи выделенного GPRS-канала связи. Подключение к сети Интернет отсутствует.

2.3 Граница контролируемой зоны

Здания, в границах которых размещаются технические средства АСУ ТП КНС являются контролируемой зоной с охранной сигнализацией объекта.

Сторонние организации на территории объекта не размещаются. Доступ в помещения, в которых находятся технические средства АСУ ТП КНС, имеют сотрудники, обслуживающие станцию, и сотрудники сторонних организаций, в сопровождении сотрудников, обслуживающих станцию.

Неконтролируемый доступ к техническим средствам АСУ ТП КНС затруднен, в связи с обеспечением пропускного режима на территорию объекта, запираемых на замок дверей, и присутствием персонала. Шкафы автоматизации имеют запирающиеся замки. Проектная и эксплуатационная документация на бумажных носителях хранится в запираемых шкафах и ящиках.

2.4 Объект защиты

В рамках АСУ ТП КНС «Бронная» к объектам защиты относятся следующие программно-технические средства:

- Сетевое оборудование;
- Программируемые логические контроллеры
- Исполнительные устройства.

Обеспечение информационной безопасности АСУ ТП КНС осуществляется непосредственно СОИБ.

2.5 Требование к системе

Конкретные типы и версии СЗИ должны выбираться с учетом требований по наличию сертификатов соответствия реализованных в них функций безопасности, которые могут использоваться для выполнения требований защищенности в соответствии с моделями угроз и нарушителя. Исходя из соображений обеспечения наилучшей производительности и возможности создания отказоустойчивого решения, СОИБ АСУ ТП КНС «Бронная» должна представлять собой комплекс программно-технических, организационных и правовых мер, обеспечивающих:

БКИТ.241388.КНС-Бронная-ИБ

Лист

7

Взам.инв. N	
Подпись и дата	
Инв. N подл.	

Изм	Кол.уч.	Лист	NДокум	Подп.	Дата

- идентификацию и аутентификацию (ИАФ);
- управление доступом (УПД);
- защиту машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусную защиту (АВЗ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защиту технических средств и систем (ЗТС);
- защиту информационной (автоматизированной) системы и ее компонентов (ЗИС);
- реагирование на компьютерные инциденты (ИНЦ)
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- планирование мероприятий по обеспечению безопасности (ПЛН);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО).

2.6 Определение набора мер

Так как АСУ ТП КНС «Бронная» присвоен класс защищенности 3, то базовым набором мер принимается набор мер, соответствующий классу защищенности 3, из Приложения Приказа ФСТЭК от 14 марта 2014 г. №31 к «Требованиям 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». В результате адаптации данного набора мер с учетом структурных особенностей АСУ ТП КНС «Бронная» исключаются следующие меры:

- Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления (АУД.3). Данная мера исключается из адаптированного набора мер в связи с реализацией данной мере в рамках штатного функционирования АСУ ТП КНС «Бронная».
- Антивирусная защита электронной почты и иных сервисов (АВЗ.2). Данная мера исключается из адаптированного набора мер, так как данная технология не применяется в АСУ ТП КНС «Бронная».

Инв. N подл.	Подпись и дата	Взам. инв. N	БКИТ.241388.КНС-Бронная-ИБ						Лист 8
Изм.	Кол.уч.	Лист	NДокум	Подп.	Дата				

- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4). Данная мера исключается из адаптированного набора мер, так как к информации, обрабатываемой в АСУ ТП КНС «Бронная», не предъявляются требования по сохранению ее конфиденциальности.

- Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) (ЗТС.5). Данная мера исключается из адаптированного набора мер в связи с реализацией данной мере в рамках штатного функционирования АСУ ТП КНС «Бронная».

- Организация демилитаризованной зоны (ЗИС.5). Реализация данной меры не требуется в данной АСУ ТП в связи с её архитектурными особенностями.

- Соккрытие архитектуры и конфигурации информационной (автоматизированной) системы (ЗИС.8). Данная мера реализуется при проектировании АСУ ТП объекта.

- Защита информации при использовании мобильных устройств (ЗИС.38). Данная мера исключается из адаптированного набора мер, так как данная технология не применяется в АСУ ТП КНС «Бронная».

- Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных (ЗИС.39). Данная мера исключается из адаптированного набора мер, так как данная технология не применяется в АСУ ТП КНС «Бронная».

- Контроль целостности программного обеспечения (ОЦЛ.1). Данная мера реализуется в рамках штатного функционирования АСУ ТП КНС «Бронная».

Адаптивный набор мер и актуальные угрозы, нейтрализующиеся данным набором мер представлены в таблице 1.

Инв. N подл.	Подпись и дата	Взам. инв. N							Лист
			Изм	Кол.уч.	Лист	NДокум	Подп.	Дата	9

Таблица 1

Условное обозначение и номер меры	Меры по защите информации	Идентификатор актуальной угрозы	Наименование актуальной угрозы, нейтрализуемой мерой по защите информации
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации		
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	УБИ.006	Угроза внедрения кода или данных
		УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
		УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
		УБИ.018	Угроза загрузки нештатной операционной системы
		УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
		УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
		УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
		УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
		УБИ.053	Угроза невозможности управления правами пользователей BIOS
		УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам
		УБИ.086	Угроза несанкционированного изменения аутентификационной информации

Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата
Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата
Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата

Инв. Nподл.	Подпись и дата	Взам.инв. N

Изм	Кол.уч.	Лист	№Докум	Подп.	Дата

		УБИ.089	Угроза несанкционированного редактирования реестра
		УБИ.093	Угроза несанкционированного управления буфером
		УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
		УБИ.107	Угроза отключения контрольных датчиков
		УБИ.152	Угроза удаления аутентификационной информации
		УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
		УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
		УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)
		УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
ИАФ.2	Идентификация и аутентификация устройств	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
		УБИ.152	Угроза удаления аутентификационной информации
		УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
ИАФ.3	Управление идентификаторами	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию

Иив. Nподл.	Подпись и дата	Взам.ив. N

БКИТ.241388.КНС-Бронная-ИБ

		УБИ.089	Угроза несанкционированного редактирования реестра
		УБИ.093	Угроза несанкционированного управления буфером
		УБИ.121	Угроза повреждения системного реестра
		УБИ.158	Угроза форматирования носителей информации
		УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
		УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УПД.5	Назначение минимально необходимых прав и привилегий	УБИ.006	Угроза внедрения кода или данных
		УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
		УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
		УБИ.086	Угроза несанкционированного изменения аутентификационной информации
		УБИ.089	Угроза несанкционированного редактирования реестра
		УБИ.093	Угроза несанкционированного управления буфером
		УБИ.121	Угроза повреждения системного реестра
		УБИ.158	Угроза форматирования носителей информации
		УБИ.178	Угроза несанкционированного использования системных и сетевых утилит

						БКИТ.241388.КНС-Бронная-ИБ	Лист
							14
Изм	Кол.уч.	Лист	№Докум	Подп.	Дата		

		УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
		УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)
		УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
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	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УПД.13	Реализация защищенного удаленного доступа		
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем		
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации		
ЗНИ.1	Учет машинных носителей информации		

Изм.	Кол.уч.	Лист	№Докум	Подп.	Дата

АУД.2	Анализ уязвимостей и их устранение	УБИ.192	Угроза использования уязвимых версий программного обеспечения
АУД.4	Регистрация событий безопасности		
АУД.6	Защита информации о событиях безопасности		
АУД.7	Мониторинг безопасности	УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
		УБИ.192	Угроза использования уязвимых версий программного обеспечения
		УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
АУД.8	Реагирование на сбои при регистрации событий безопасности		
АУД.10	Проведение внутренних аудитов		
АВЗ.0	Регламентация правил и процедур антивирусной защиты		
АВЗ.1	Реализация антивирусной защиты	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
		УБИ.192	Угроза использования уязвимых версий программного обеспечения
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	УБИ.121	Угроза повреждения системного реестра

Изм.	Кол.уч.	Лист	№Докум	Подп.	Дата

ОДТ.0	Регламентация правил и процедур обеспечения доступности	УБИ.121	Угроза повреждения системного реестра
ОДТ.4	Резервное копирование информации	УБИ.152	Угроза удаления аутентификационной информации
ОДТ.5	Обеспечение возможности восстановления информации	УБИ.152	Угроза удаления аутентификационной информации
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	УБИ.018	Угроза загрузки нештатной операционной системы
		УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
		УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
ЗТС.2	Организация контролируемой зоны	УБИ.107	Угроза отключения контрольных датчиков
		УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
ЗТС.3	Управление физическим доступом	УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

Изм.	Кол.уч.	Лист	№Докум	Подп.	Дата

ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам
ЗИС.2	Защита периметра информационной (автоматизированной) системы	УБИ.107	Угроза отключения контрольных датчиков
		УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы		
ЗИС.19	Защита информации при ее передаче по каналам связи	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам
ЗИС.20	Обеспечение доверенных канала, маршрута	УБИ.107	Угроза отключения контрольных датчиков
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	УБИ.152	Угроза удаления аутентификационной информации
ЗИС.32	Защита беспроводных соединений	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам

Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата
Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата
Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата

ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)		
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты		
ИНЦ.1	Выявление компьютерных инцидентов		
ИНЦ.2	Информирование о компьютерных инцидентах		
ИНЦ.3	Анализ компьютерных инцидентов		
ИНЦ.4	Устранение последствий компьютерных инцидентов		
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов		
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы		
УКФ.2	Управление изменениями		
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения		
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS

						БКИТ.241388.КНС-Бронная-ИБ	Лист
							20
Изм.	Кол.уч.	Лист	№Докум	Подп.	Дата		

ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
		УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
ОПО.2	Контроль целостности обновлений программного обеспечения	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
ОПО.3	Тестирование обновлений программного обеспечения	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
ОПО.4	Установка обновлений программного обеспечения		
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации		
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации		
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации		
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях		
ДНС.1	Разработка плана действий в нештатных ситуациях		

Изм.	Кол.уч.	Лист	№Докум	Подп.	Дата

ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
		УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
		УБИ.158	Угроза форматирования носителей информации
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
		УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
		УБИ.158	Угроза форматирования носителей информации
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения		
ИПО.0	Регламентация правил и процедур информирования и обучения персонала		
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы		

Изм	Кол.уч.	Лист	№Докум	Подп.	Дата

ИПО.2	Обучение персонала правилам безопасной работы		
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы		

Все организационные решения, с учётом вновь введенных, должны быть отражены в нормативных актах МУП г. Новосибирска «ГОРВОДОКАНАЛ» и доведены до персонала в части их должностных обязанностей.

В рамках внедрения СОИБ необходимо разработать «Положение о разграничении прав доступа к АСУ ТП КНС «Бронная» и обрабатываемой ею информации», которое будет реализовывать меры по защите информации (ИАФ.0, ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.0, УПД.1, УПД.4, УПД.5, ЗНИ.2, ЗНИ.5, ЗНС.7, ЗИС.0, ЗИС.1) и регламентировать:

- Перечень пользовательских ролей и их полномочий в АСУ ТП КНС «Бронная»;
- Порядок идентификации и аутентификации пользователей, в том числе внешних;
- Правила и порядок создания, изменения, уничтожения идентификаторов и аутентификационной информации;
- Порядок действия в случае утраты и (или) компрометации данной информации;
- Правила разграничения доступа к ресурсам АСУ ТП КНС «Бронная»;

В рамках внедрения в СОИБ необходимо разработать «Положение об управлении конфигурацией и обновлениями АСУ ТП КНС», которое будет реализовывать меры по защите информации (ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4, УКФ.0, УКФ.2, УКФ.3) и определять:

Изм.	Взам.инв. N
Подпись и дата	
Изм.	Подп.

Изм.	Кол.уч.	Лист	№Докум	Подп.	Дата

- Порядок получения, тестирования и установки обновлений программного обеспечения АСУ ТП КНС «Бронная» и СЗИ.
- Порядок проведения контроля целостности обновляемого ПО и СЗИ.
- Порядок информирования об планируемых изменениях конфигурации АСУ ТП КНС «Бронная» сотрудника, ответственного за обеспечение ОБИ АСУ ТП КНС «Бронная»;
- Согласование изменений конфигурации АСУ ТП КНС «Бронная» с сотрудником, ответственным за обеспечение ОБИ АСУ ТП КНС «Бронная»;
- Порядок анализа потенциального воздействия планируемых изменений в конфигурации автоматизированной системы управления и системы защиты на обеспечение защиты информации;

В рамках внедрения в СОИБ необходимо разработать «Положение о работе с машинными носителями информации», которое будет реализовывать меры по защите информации (ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.8) и определять:

- Порядок проведения инвентаризации информационных ресурсов;
- Порядок анализа уязвимостей и их устранение;
- Перечень событий информационной безопасности, подлежащих регистрации;
- Порядок регистрации и хранения событий информационной безопасности;
- Сроки хранения событий информационной безопасности, подлежащих регистрации;
- Порядок защиты информации о событиях безопасности;
- Порядок реагирования на сбои при регистрации событий информационной безопасности;
- Порядок проведения внутренних аудитов;
- Контроль (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления
- Порядок сокрытия архитектуры и конфигурации информационной (автоматизированной) системы.

Изм.	Кол.уч.	Лист	ИД докум.	Подп.	Дата	Взам.инв. №	Подпись и дата	Изм.	Кол.уч.	Лист	ИД докум.	Подп.	Дата	Лист
БКИТ.241388.КНС-Бронная-ИБ														24

В рамках внедрения СОИБ необходимо разработать «Положение об антивирусной защите», которое будет реализовывать меры по защите информации (АВЗ.0, АВЗ.4) и регламентировать:

- Порядок и правила работы со средствами антивирусной защиты;
- Порядок обновления баз данных сигнатур средств антивирусной защиты.

В рамках внедрения СОИБ необходимо разработать «Положение о реагировании на инциденты информационной безопасности», которое будет реализовывать меры по защите информации (ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6) и регламентировать:

- Порядок анализа событий информационной безопасности и выявления инцидентов информационной безопасности;
- Порядок информирования об инцидентах информационной безопасности;
- Порядок реагирования на инциденты информационной безопасности;
- Порядок устранения последствий инцидентов информационной безопасности;
- Порядок принятия мер по предотвращению повторного возникновения инцидентов информационной безопасности.

В рамках внедрения СОИБ необходимо разработать «Положение о резервировании и восстановлении АСУ ТП КНС «Бронная» и её СОИБ», которое будет реализовывать меры по защите информации (ОЦЛ.0, ОДТ.0, ОДТ.1, ОДТ.2, ОДТ.4, ОДТ.5, ОДТ.6) и регламентировать:

- Порядок осуществления контроля целостности программного обеспечения, в том числе средств защиты информации;
- Порядок восстановления ПО, в том числе СЗИ, при возникновении внештатных ситуаций;
- Порядок осуществления резервного копирования информации в АСУ ТП КНС «Бронная» и восстановления её из резервных копий.

Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата	Взам.инв. N	Подпись и дата	Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата	Лист	25
БКИТ.241388.КНС-Бронная-ИБ															

В рамках внедрения СОИБ необходимо разработать «Положение об организации доступа к техническим средствам АСУ ТП КНС «Бронная», которое будет реализовывать меры по защите информации (ЗТС.0, ЗТС.4, ЗТС.6) и определять:

- Границы контролируемой зоны, порядок её формирования и контроля её состояния;
- Порядок контроля и предоставления физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ.

В рамках внедрения СОИБ необходимо разработать «Положение о планировании мероприятий по обеспечению информационной безопасности». Данный документ будет реализовывать меры по защите информации (ПЛН.0, ПЛН.1, ПЛН.2) и устанавливает:

- Порядок пересмотра и переоценки актуальных угроз безопасности информации в АСУ ТП КНС «Бронная»;
- Порядок осуществления планирования мероприятий по обеспечению защиты информации;
- Порядок осуществления контроля выполнения мероприятий по обеспечению информационной безопасности.

В рамках внедрения СОИБ необходимо разработать «Положение об информировании и обучении персонала». Данный документ реализует меры по защите информации (ИПО.0, ИПО.1, ИПО.2) и определяет:

- Процедуру информирование персонала об угрозах информационной безопасности и обучения правилам безопасной работы с АСУ ТП КНС «Бронная» в части их должностных обязанностей;
- Процедуру информирование персонала об угрозах информационной безопасности в части, касающейся их должностных обязанностей.

Инв. №подл.	Подпись и дата	Взам.инв. №							Лист
Изм.	Кол.уч.	Лист	№Докум.	Подп.	Дата	БКИТ.241388.КНС-Бронная-ИБ			26

В рамках внедрения СОИБ необходимо разработать «Регламент обеспечения действий в нештатных ситуациях», которое реализует меры по защите информации (ДНС.0, ДНС.1, ДНС.2, ДНС.5) и регламентирует порядок действий при возникновении нештатных ситуаций, связанных с инцидентами информационной безопасности.

В рамках внедрения СОИБ необходимо разработать «Регламент конфигурирования средств защиты информации», который будет определять конфигурации средств защиты информации», который будет определять конфигурации средств защиты информации, включенные в состав СОИБ АСУ ТП КНС «Бронная».

4. Основные технические решения

4.1 Решения по обеспечению безопасного межсетевого взаимодействия

4.1.1 Решения, применяемые в АСУ ТП КНС «Бронная»

Для обеспечения безопасного межсетевого взаимодействия в СОИБ АСУ ТП КНС «Бронная» проектом предусмотрена установка межсетевых экранов ESR-200, версия программного обеспечения 1.5, РПЛТ.465614.149, имеющий сертификат ФСТЭК №4386 от 14.04.2021, действующий до 14.04.2026 на соответствие (ИТ.МЭ.А4.ПЗ).

Установка предполагается на границе технологических сетей объектов. Устройства Eltex ESR-200 предназначены для применения на сетях передачи данных в качестве оборудования защиты информации от несанкционированного доступа, оборудования коммутации и маршрутизации. Изделие предназначено для выполнения функций контроля и фильтрации проходящих информационных потоков в соответствии с заданными правилами и для использования в целях обеспечения защиты не криптографическими средствами информации ограниченного доступа.

- Порядок реагирования на сбои при регистрации событий информационной безопасности;
- Порядок проведения внутренних аудитов;

Инв. N подл.	Подпись и дата	Взам. инв. N							Лист
Изм.	Кол.уч.	Лист	НДокум	Подп.	Дата	БКИТ.241388.КНС-Бронная-ИБ			27

— Контроль (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления

- Порядок сокрытия архитектуры и конфигурации информационной (автоматизированной) системы.

Функционал данного устройства обеспечивает:

- Маршрутизацию трафика (статическая, динамическая маршрутизация RIP, OSPF, BGP, PIM);

— Межсетевое экранирование, предназначенное для осуществления контроля и фильтрации, проходящих через него сетевых пакетов в соответствии с политиками трафика, которые настраиваются отдельно для каждой категории пользователей и каждого конкретного пользователя;

— Поддержку: VLAN;

- VPN IPsec. Осуществляется поддержка частных частных сетей с использованием протоколов IPsec VPN (LAN-to-LAN)

— Eltex ERS-200 реализует следующие меры по защите информации в АСУ ТП КНС «Бронная»:

— Контроль доступа из внешних информационных (автоматизированных) систем (УПД.14) путем разделения технологической сети АСУ ТП КНС «Бронная» в отдельный сегмент.

Данные правила описаны в регламенте конфигурирования средств защиты информации;

— УПД.2 Реализация политик управления доступа. Ограничения доступа к ресурсам АСУ ТП КНС «Бронная» достигается путем формирования правил межсетевого экранирования, ограничивая адреса и протоколы, по которым осуществляется доступ к ресурсам АСУ ТП КНС «Бронная»;

— «Управление взаимодействием с автоматизированными (информационными) системами сторонних организаций (внешние системы)».

Реализуется мера путем создания VPN-туннеля между системами с обязательной авторизацией сторон. Все правила конфигурации взаимодействия описаны в регламенте конфигурирования средств защиты информации;

Инв. Nподл.	Подпись и дата	Взвешив. N

						БКИТ.241388.КНС-Бронная-ИБ	Лист
							28
Изм	Кол.уч.	Лист	НДокум	Подп.	Дата		

— Идентификация и аутентификация пользователей. Реализуется мера путем создания VPN-туннеля между системами с обязательной авторизацией сторон. Все правила конфигурации взаимодействия описаны в регламенте конфигурирования средств защиты информации;

— «Разбиение автоматизированной системы управления на сегменты (сегментирование) и обеспечение защиты периметров сегментов» (ЗИС.17). Сегментирование технологической сети АСУ ТП КНС «Бронная» производится путем подключения предполагаемых сегментов сети в switch-порты межсетевого экрана и реализацией правил взаимодействия сегментов. Данные правила описаны в регламенте конфигурирования средств защиты информации;

— «Защита периметра (физических и (или) логических границ) автоматизированной системы управления при ее взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями» в части защиты логических границ АСУ ТП КНС «Бронная» путем фильтрации и разграничении информационных потоков АСУ ТП КНС «Бронная».

						БКИТ.241388.КНС-Бронная-ИБ	Лист
							29
Изм	Кол.уч.	Лист	№Докум	Подп.	Дата		

Реализуется данная мера путем использования выделенных GPRS и волоконно-оптического каналов связи. В качестве маршрутизатора используется Eltex ERS-200.

— Реализация защищенного удаленного доступа (УПД.13) Реализуется мера путем создания VPN-туннеля между системами с обязательной авторизацией сторон. Все правила конфигурации взаимодействия описаны в регламенте конфигурирования средств защиты информации;

— Запрет несанкционированной удаленной активации периферийных устройств (ЗИС.21). Реализуется мера путем создания VPN-туннеля между системами с обязательной авторизацией сторон и создания правил межсетевого экранирования информационных потоков системы. Все правила конфигурации взаимодействия описаны в регламенте конфигурирования средств защиты информации;

— Защита от угроз отказа в обслуживании (DOS, DDOS-атак) (ЗИС.34). Реализуется возможностью отключения атакуемого интерфейса и переходом на резервный канал передачи данных, в случае проведения подобной атаки.

— Обеспечение доверенных канала, маршрута (ЗИС.20). Реализуется мера путем создания VPN-туннеля между системами с обязательной авторизацией сторон, конфигурированием правил маршрутизации трафика. Все правила конфигурации взаимодействия описаны в регламенте конфигурирования средств;

— Защита беспроводных соединений (ЗИС.32). Реализуется мера путем создания VPN-туннеля между системами с обязательной авторизацией сторон. Все правила конфигурации взаимодействия описаны в регламенте конфигурирования средств защиты информации;

4.2 Решение по обеспечению анализа защищенности

Для обеспечения анализа защищенности используется САЗ XSpider производства Positive Technologies, установленный APM1, расположенного в МДП «Комета».

Сведения о САЗ XSpider:

— Используемая версия – 7.8.25;

Инв. №подл.	Подпись и дата	Взам. инв. №	правила конфигурации взаимодействия описаны в регламенте конфигурирования средств защиты информации;						
			4.2 Решение по обеспечению анализа защищенности						
			Для обеспечения анализа защищенности используется САЗ XSpider производства Positive Technologies, установленный АРМ1, расположенного в МДП «Комета».						
Сведения о САЗ XSpider:									
– Используемая версия – 7.8.25;									
						БКИТ.241388.КНС-Бронная-ИБ			Лист
									30
Изм.	Кол.уч.	Лист	№Докум	Подп.	Дата				

5.1 Мероприятия по созданию необходимых подразделений и рабочих мест

МУП г. Новосибирска «ГОРВОДОКАНАЛ» необходимо выделить структурную единицу – Администратор информационной безопасности, который должен обладать квалификацией, достаточной для эксплуатации всех применяемых в СОИБ средств защиты информации.

Администратор информационной безопасности должен знать и выполнять требования, как действующего законодательства Российской Федерации в области защиты информации, так и локальных нормативных актов МУП г. Новосибирска «ГОРВОДОКАНАЛ».

5.2 Мероприятия по вводу СОИБ в действие

При подготовке ввода СОИБ в действие необходимо провести комплекс организационно-технических мероприятий:

— Разработать и ввести в эксплуатацию набор организационно-распорядительной документации, структура которой описана в данном документе; Необходимо установить все доступные обновления операционных систем и программного обеспечения, применяющегося в проектируемой системе. В тех случаях, когда поддержка программного продукта не осуществляется производителем на момент внедрения СОИБ в действие, необходимо заменить данные программные продукты на версии, поддерживаемые их производителями и модернизировать аппаратное обеспечение, если это необходимо;

— Процесс настройки средств защиты информации и наладки СОИБ должен производиться в соответствии с регламентом конфигурирования средств защиты информации и не должен оказывать влияния на работу АСУ ТП;

— Объем пусконаладочных работ для системы обеспечения информационной безопасности приведен в прилагаемых документах проекта;

Взам.инв. №	
Подпись и дата	
Изм. №подл.	

Изм	Кол.уч.	Лист	№Докум	Подп.	Дата

- После настройки средств защиты информации необходимо произвести предварительные испытания и опытную эксплуатацию СОИБ АСУ ТП КНС «Бронная»;
- В случае обнаружения уязвимостей и недостатков провести их анализ и принять меры по их устранению;
- Провести приемочные испытания СОИБ АСУ ТП КНС «Бронная».

Изм.	Кол.уч.	Лист	NДокум	Подп.	Дата	Инв. Nподл.	Подпись и дата	Взам.инв. N		
БКИТ.241388.КНС-Бронная-ИБ									Лист	
									33	

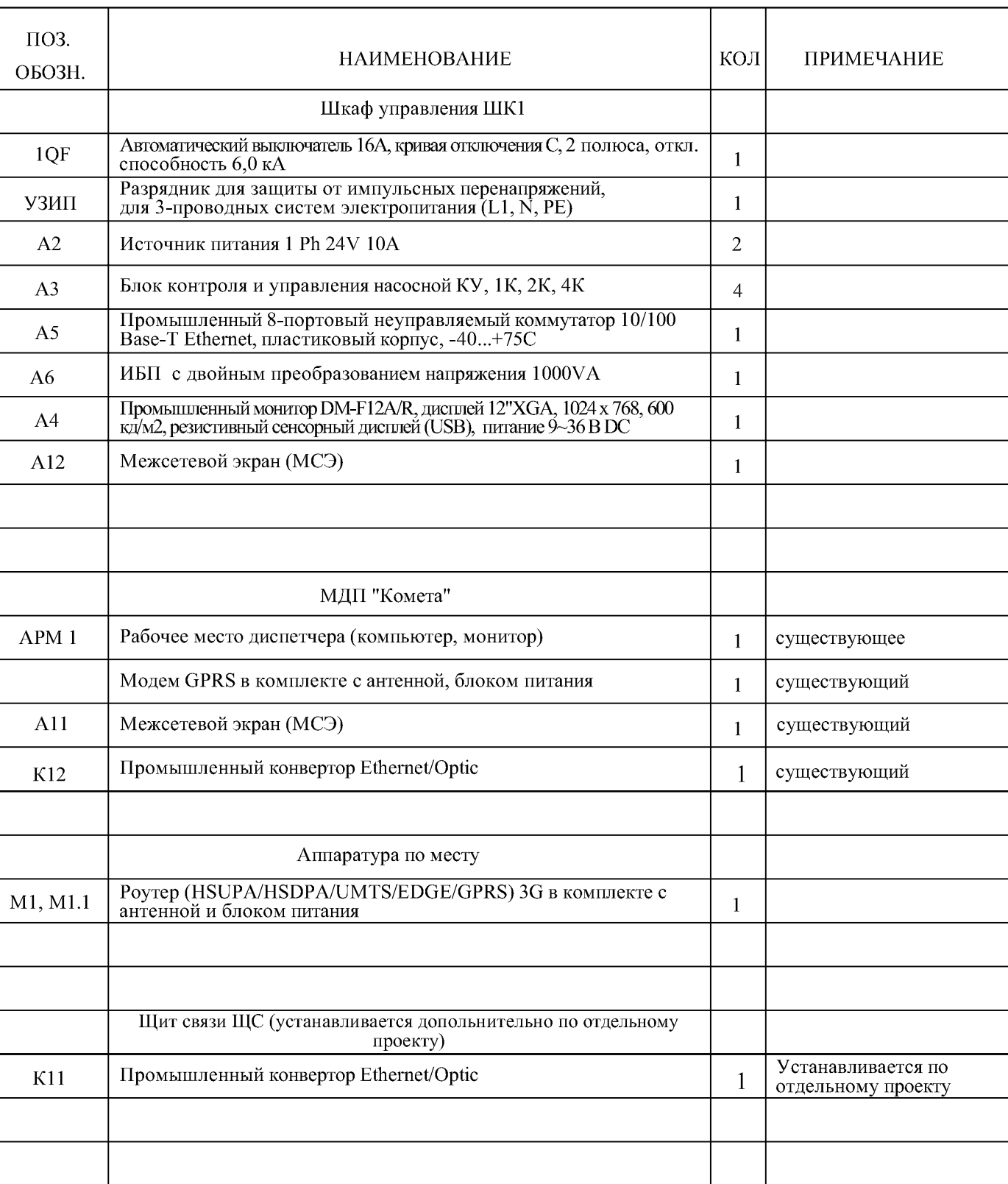
6. Перечень принятых сокращений и аббревиатур

Сокращение	Расшифровка
КСДУВ	Комплексная система диспетчерского управления водо-снабжением
ПЛК	Программируемый логический контроллер
СЗИ	Средство защиты информации
СОИБ	Система обеспечения информационной безопасности
АСУ ТП	Автоматизированная система управления технологическим процессом
ОБИ	Обеспечение безопасности информации
ОС	Операционная система
АРМ	Автоматизированное рабочее место
НДВ	Недекларированные возможности
ФСТЭК	Федеральная служба по техническому и экспортному контролю
НСД	Несанкционированный доступ
МЭ	Межсетевой экран
СОВ	Система обнаружения вторжений
СКН	Средство контроля носителей
ПРД	Правила разграничения доступа
УПД	Управление доступом
ПО	Программное обеспечение
ОДТ	Обеспечение доступности
АС	Автоматизированная система
ИБ	Информационная безопасность

Изм.	Кол.уч.	Лист	NДокум	Подп.	Дата	Изм.	Кол.уч.	Лист	NДокум	Подп.	Дата	Взам.инв. N	Подпись и дата	Изм.	Кол.уч.	Лист	NДокум	Подп.	Дата	Лист
БКИТ.241388.КНС-Бронная-ИБ																				34

ГРАФИЧЕСКАЯ ЧАСТЬ




Инв. N подл.	Подпись и дата	Взам. инв. N							Лист	
										1
			Изм	Кол.уч.	Лист	NДокум	Подп.	Дата		



Формат A2

Инв. № подл.	Подпись и дата	Взам инв. N

[illegible]

						БКИТ.241388.КНС-Бронная-ИБ				
						Канализационная насосная станция для водоотведения объекта: «Многоквартирные многоквартирные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска»				
Изм.	Кол.уч.	Лист	Индок.	Подпись	Дата	Информационная безопасность		Статья	Лист	Листов
Выполнил	Белогубов							Р	1	1
Н.контр.	Скляров									
Проверил	Подкопашева					Спецификация оборудования		ООО ПО "ОРИОН-АКВА"		
Должн.	Фамилия	Подп.	2023							

ПРИЛОЖЕНИЕ

Инв. N подл.	Подпись и дата	Взам. инв. N					
Изм	Кол.уч.	Лист	NДокум	Подп.	Дата	БКИТ.241388.КНС-Бронная-ИБ	Лист
							1

УТВЕРЖДАЮ

Директор МУП г. Новосибирска
«ГОРВОДОКАНАЛ»

_____/_____
«__» _____ 20__ г.

АКТ

определения класса защищенности автоматизированной системы

АСУ ТП КНС объекта: «Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска».

Комиссия в составе:

Председатель

- Иванов И.И.

Начальник службы автоматизации

члены комиссии

- Петров В.В.

- Степанов А.А.

(должность)

Начальник отдела информационной безопасности

(должность)

Инженер отдела по обеспечению безопасности информации

(должность)

рассмотрев исходные данные на автоматизированную систему управления технологическим процессом объекта «Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска», условия ее эксплуатации (многопользовательская система), с учетом характера обрабатываемой информации (критически важная) и в соответствии с Приложением N 1 к Требованиям 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

РЕШИЛА:

Установить АСУ ТП КНС «Бронная» ООО «Строительные решения. Специализированный застройщик» класс защищенности – 3 (КЗ).

Председатель комиссии

_____/ Иванов И.И.

Члены комиссии

_____/ Петров В.В.

_____/ Степанов А.А.

Информационная безопасность
Отчет об Обследовании
БКИТ.241388.КНС-Бронная-ИБ.ОО
На 13 листах

Перечень обозначений и сокращений

АРМ	Автоматизированное рабочее место
АСУ ТП	Автоматизированная система управления технологическим процессом
ИС	Информационная система
КЗ	Контролируемая зона
НСД	Несанкционированный доступ
НФС	Насосно-фильтровая станция
ОС	Операционная система
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
УБИ	Угроза безопасности информации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
КНС	Канализационная насосная станция

1. Общие сведения

Настоящий Отчет подготовлен ООО ПО «ОРИОН-АКВА». Данный отчет используется для разработки рабочей документации по созданию СОИБ АСУ ТП.

1.1 Общие сведения об АСУ ТП

Канализационная насосная станция предназначена для перекачивания канализационных стоков.

Автоматизированная система управления технологическими процессами канализационно-насосной станции предназначена для оперативного мониторинга параметров технологического процесса, автоматизированного контроля и управления технологическим процессом и сопутствующими локальными автоматическими подсистемами АСУ ТП.

2. Описание работы АСУ ТП

Действующая в настоящий момент подсистема АСУ ТП КНС МУП г. Новосибирска "ГОРВОДОКАНАЛ" включает в себя более 50-ти канализационно-насосных станций (КНС). Разрабатываемая КНС осуществляет взаимодействие с существующей корпоративной системой диспетчерского контроля и управления посредством выделенных каналов связи. На КНС «Бронная» реализуется локальная система автоматического управления КНС по требованиям МУП г. Новосибирска "ГОРВОДОКАНАЛ" и на базе принятого действующей системой АСУ ТП КНС аппаратно-программного обеспечения.

Разрабатываемая система АСУ КНС ТП «Бронная» обеспечивает:

- автоматическое управление канализационной насосной станцией «Бронная»;
- сбор, обработку и анализ информации о состоянии объекта управления;
- выработку управляющих воздействий;
- передачу управляющих воздействий на исполнение и её контроль;

- реализацию и контроль выполнения управляющих воздействий;
- визуализацию технологических параметров работы станции;
- архивация технологических параметров;
- светозвуковое оповещение о внештатных ситуациях;
- обмен информацией с взаимосвязанными автоматизированными системами.

Разрабатываемая АСУ ТП является сложной трехуровневой системой, состоящей из:

1. Нижнего уровня, включающий датчики (уровня жидкости в резервуаре, температур, газового анализа), счетчик электроэнергии и исполнительные механизмы (насосные агрегаты, вентиляторы, измельчитель).

2. Среднего уровня, состоящего из программируемых логических контроллеров (управления главными насосами, дренажной системой, мониторинга работы станции, управления системой вентиляции, измельчителем. Обработка информации на этом уровне происходит по единому алгоритму: прием сведений, их анализ и обработка и выдача команд на нижний уровень.

3. Верхнего уровня, построенного на базе серверного оборудования и АРМов операторов, обеспечивающих сбор и хранение данных, а также архивацию информации, полученной от контроллеров, и представление ее в виде визуальных средств. Таким образом, оператор системы может ознакомиться с параметрами процесса, протекающего на объекте.

Компоненты нижнего и среднего уровней связаны между собой проводными линиями связи в единую распределенную систему управления, работающую в режиме реального времени. Средний и верхний уровни объединены в сеть посредством организации GSM- канала передачи данных с возможностью подключения канала ВОЛС. Канал связи является выделенными, отсутствует подключение к сети Интернет. Таким образом,

можно дистанционно и оперативно контролировать работу объекта и избегать аварийных ситуаций, обеспечивая наибольшую производительность и безопасность.

В качестве верхнего уровня АСУ ТП КНС выступает подсистема АСУ ТП КНС КСДУВ созданная на базе WonderWare SystemPlatform, Scada Intouch for WonderWare SystemPlatform, с разработанными приложениями АРМ «Охрана. Связь», АРМ Диспетчера КНС, ПО «Монитора тревог», ПО представления графиков «монитор трендов»

Взаимодействие верхнего и среднего уровня АСУ ТП КНС понимается как взаимодействие сторонних систем. В рамках данного проекта рассматривается только нижний и средний уровень АСУ ТП КНС «Бронная». АСУ ТП КНС «Бронная» по своей структуре, являются локальными системами, так как все устройства, к ней относящиеся находятся в пределах контролируемой зоны объекта.

Структура аппаратных средств уровня канализационно-насосных станций:

1. Программируемые логические контроллеры (ПЛК) управления технологическим процессом;
2. Устройства контроля технологического процесса;
3. Связные контроллеры сбора и передачи данных на верхний уровень;
4. Охранная сигнализация;
5. Средства коммуникации.

В случае возникновения неисправности возможен переход на ручное управление станцией персоналом.

АСУ ТП КНС «Бронная» обеспечивает локальное управление технологическим объектом при помощи интеллектуального узла управления, состоящего из шкафа мониторинга и управления насосной станцией в автоматическом режиме (далее ШК1) в комплекте с модулями программного обеспечения (ООО НПО «ОРИОН») на базе связного контроллера,

контроллеров управления насосными агрегатами, датчиками, исполнительными устройствами и снабжает взаимосвязанные с ней системы автоматизированного контроля и управления (диспетчерский пункт цеха, предприятия) достоверной информацией о работе технологического объекта управления (КНС «Бронная»).

Алгоритм работы насосов определяется уровнем жидкости в приемном резервуаре: при достижении значения рабочего уровня, установленного для каждого насоса, автоматически происходит запуск соответствующего агрегата. При снижении количества стоков в ёмкости происходит поочередное отключение насосов. Проектом реализована возможность автоматического чередования работы насосных агрегатов для равномерной их наработки. Управление чередованием производится блоком автоматики КУ.

При нарушении регламента выхода основного насоса в оптимальный рабочий режим система в автоматическом режиме переключается на резервный насос.

Контроль состояния насосных агрегатов производится блоками 1К, 2К, передается на блок КУ и далее в систему диспетчерского контроля. Такая структура обеспечивает надежную работу и быстрое переключение на работоспособные агрегаты в аварийных ситуациях.

Насосы снабжены термовыключателем, в случае перегрева (около 150 °С) термовыключатель через защитный контур шкафа управления насосами ШУН остановит насос размыканием электроцепи. После охлаждения термовыключатель вновь замкнёт цепь.

Контроль сигнала аварийной остановки осуществляется контроллерами 1К, 2К с последующей передачей информации о состоянии агрегатов через связной контроллер в корпоративную систему диспетчерского управления.

При вводе оборудования в эксплуатацию и техническом обслуживании, управление насосными агрегатами переводится в ручной режим с помощью переключателей. В ручном режиме управление производится с кнопочных

постов Н1-SB, Н2-SB расположенных в непосредственной близости от насосных агрегатов или кнопками с лицевой панели шкафа управления ШУН.

Для контроля засорения приемного лотка в нём предусмотрена установка дискретного датчика уровня. Аварийный сигнал о засорении поступает с блока КУ на диспетчерский пункт для дальнейшего принятия решения оператором по оперативному управлению.

Автоматическое управление приточно-вытяжной системой производится комплектным блоком автоматики ШУ Вентиляции, заказанным в разделе ОБ. Система работает в автономном режиме по алгоритму завода-изготовителя.

2.1 Взаимодействие со смежными системами:

Логической границей АСУ ТП «Бронная» является её локальная вычислительная сеть.

АСУ ТП «Бронная» осуществляет информационный обмен с АСУ ТП с существующей корпоративной системой диспетчерского контроля и управления АСУ ТП КНС ООО «Строительные решения. Специализированный застройщик». Взаимодействие осуществляется посредством GSM-канала передачи данных, с возможностью подключения к выделенному каналу с применением технологии волоконно-оптической сети (ВОЛС). Канал связи является выделенным, отсутствует подключение к сети Интернет.

2.2 Контролируемые параметры и управляемые устройства

Под критической важной информацией понимается значение контролируемых параметров станции. На КНС «Бронная» осуществляется контроль следующих параметров:

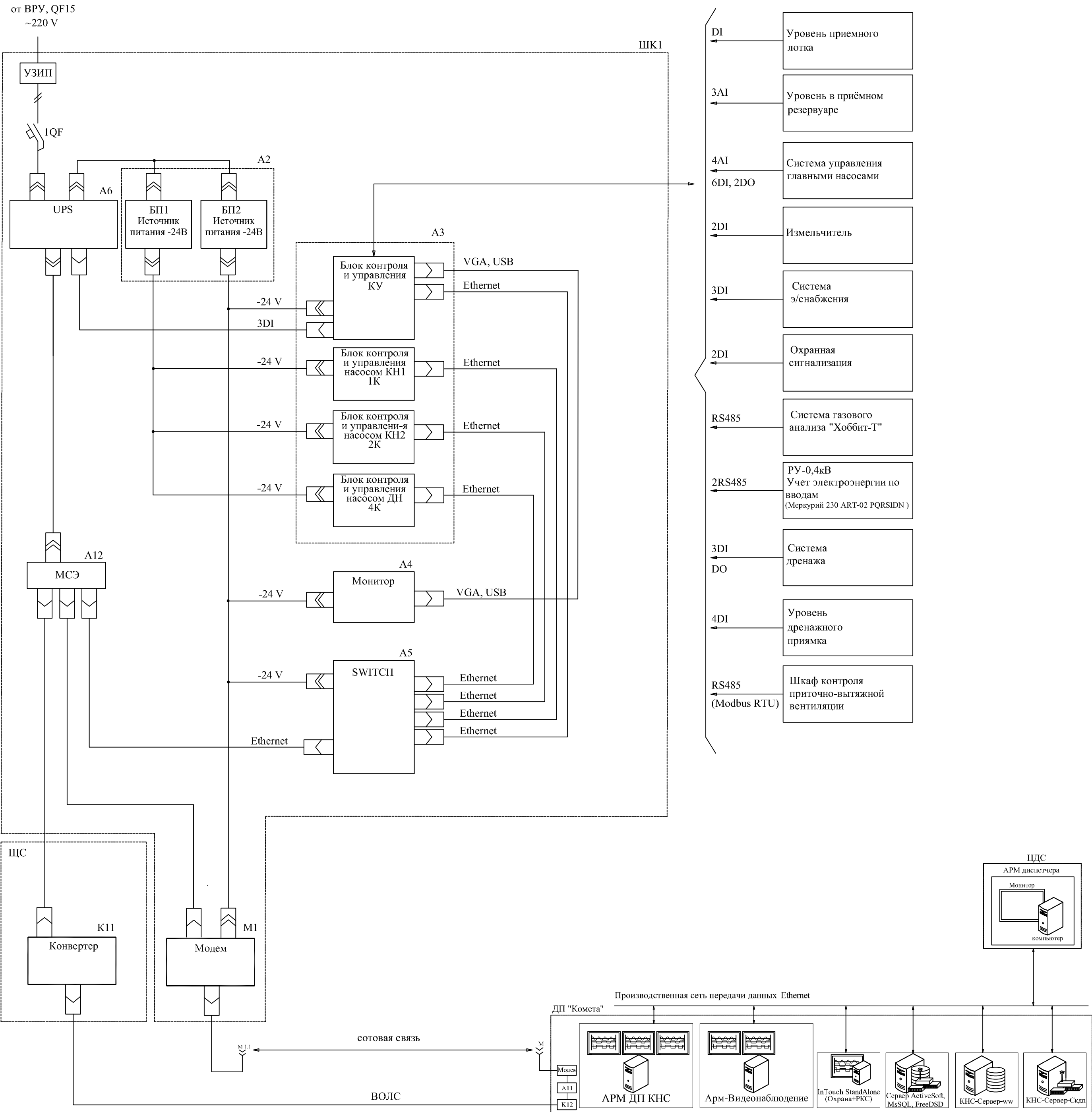
- Параметры работы насосных агрегатов и их состояние
- Параметры работы дренажных насосов и их состояния
- Параметры работы системы приточной вентиляции и ее

состояния

- Параметры работы системы вытяжной вентиляции и ее состояния
- Состояние источников бесперебойного питания
- Потребление электроэнергии оборудованием
- Состояние подачи питания на технологическое оборудование
- Состояние каналов связи
- Состояние охранной сигнализации

На КНС «Бронная» осуществляется управление следующим оборудованием:

- Насосные агрегаты
- Дренажные насосы
- Каналы передачи данных



ПОЗ. ОБОЗН.	НАИМЕНОВАНИЕ	КОЛ	ПРИМЕЧАНИЕ
	Шкаф управления ШК1		
1QF	Автоматический выключатель 16А, кривая отключения С, 2 полюса, откл. способность 6,0 кА	1	
УЗИП	Разрядник для защиты от импульсных перенапряжений, для 3-проводных систем электропитания (L1, N, PE)	1	
A2	Источник питания 1 Ph 24V 10A	2	
A3	Блок контроля и управления насосной КУ, 1К, 2К, 4К	4	
A5	Промышленный 8-портовый неуправляемый коммутатор 10/100 Base-T Ethernet, пластиковый корпус, -40...+75C	1	
A6	ИБП с двойным преобразованием напряжения 1000VA	1	
A4	Промышленный монитор DM-F12A/R, дисплей 12"XGA, 1024 x 768, 600 кд/м2, резистивный сенсорный дисплей (USB), питание 9-36 В DC	1	
A12	Межсетевой экран (МСЭ)	1	
	МДП "Комета"		
АРМ 1	Рабочее место диспетчера (компьютер, монитор)	1	существующее
	Модем GPRS в комплекте с антенной, блоком питания	1	существующий
A11	Межсетевой экран (МСЭ)	1	существующий
K12	Промышленный конвертер Ethernet/Optic	1	существующий
	Аппаратура по месту		
M1, M1.1	Роутер (HSPA/HSDPA/UMTS/EDGE/GPRS) 3G в комплекте с антенной и блоком питания	1	
	Щит связи ИЦС (устанавливается дополнительно по отдельному проекту)		
K11	Промышленный конвертер Ethernet/Optic	1	Устанавливается по отдельному проекту

Примечание:

➤ - питание прибора

➤ - снятие сигнала с прибора

						БКИТ.241388.КНС-Бронная-ИБ			
						Канализационная насосная станция для водоотведения объекта: «Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во ветроновых помещениях по ул. Бронная в Кировском районе г. Новосибирска»			
Изм.	Кол.уч.	Лист	Ндок.	Подпись	Дата	Информационная безопасность	Стадия	Лист	Листов
Выполнил	Архипова						Р	16	
Н.контр.	Левоева								
Проверил	Подкопаева					Структурная схема АСУ	ООО ПО "ОРИОН-АКВА"		
Должн.	Фамилия	Подп.		2023					

Инв. № подл.	Подпись и дата	Взам инв. N

[illegible]




						БКИТ.241388.КНС-Бронная-ИБ				
						Канализационная насосная станция для водоотведения объекта: «Многokвартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска»				
Изм.	Кол.уч.	Лист	Индок.	Подпись	Дата	Информационная безопасность		Статья	Лист	Листов
Выполнил	Белогубов							Р	1	1
Н.контр.	Склярков									
Проверил	Подкопашева									
						Спецификация оборудования		ООО ПО "ОРИОН-АКВА"		
Должн.	Фамилия		Подп.	2023						

Таблица – 1. Перечень процессов, протекающих в АСУ ТП

Наименование автоматизированного процесса/объекта	Наличие персонала на объекте протекания процесса	Возможность перехода на ручное управление	Возможные последствия в случае нарушения/остановки процесса	Уровень критичности информации (процесса) ¹	Примечание
Откачка канализационных стоков	Отсутствует ²	Есть	Остановка откачки канализационных стоков	Низкий	Возникший инцидент не оказывает существенного влияния на технологический процесс. Так как в случае отказа АСУ ТП предусмотрена возможность перехода на ручное управление, а постоянное присутствие персонала позволяет производить

					соответствующие мероприятия по устранению, без существенного влияния на технологический процесс. В соответствии с этим, возникшее в случае сбоя АСУ ТП на объекте ЧС является чрезвычайной ситуацией локального характера, так как распространяется лишь на сам объект
--	--	--	--	--	---

1 – Классификация в соответствии Приложение N 1 к Требованиям 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

2 - Периодичность контроля станции персоналом и возможность перехода на ручное управление позволяет избежать серьезных последствий в случае возникновения инцидента информационной безопасности

Так как в системе обрабатывается информация (процесс) с низким уровнем критичности, то в соответствии с Приложением N 1 к Требованиям 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, АСУ ТП, рекомендуется присвоить третий класс защищенности (К3).

3. Принятые меры по обеспечению информационной безопасности АСУ ТП

3.1 Обеспечение физической безопасности АСУ ТП

Территория, на которой размещаются здания АСУ ТП, является контролируемой зоной. Сторонние организации на территории объекта не размещаются. Представители сторонних организаций допускаются на территорию только по заранее выданным пропускам с регистрацией посещения в соответствующем журнале. Доступ в помещения, в которых находятся технические средства АСУ ТП, имеют сотрудники, обслуживающие станцию, и сотрудники сторонних организаций, допущенные на территорию объекта.

Неконтролируемый доступ к техническим средствам АСУ ТП затруднен, в связи с установкой на КНС «Бронная» специальных технических средств, направленных на исключение неконтролируемого доступа к техническим средствам АСУ ТП. Шкафы автоматизации имеют запирающиеся замки. Проектная и эксплуатационная документация на бумажных носителях хранится в запираемых шкафах и ящиках.

Здание, в границах которого размещаются технические средства АСУ ТП КНС «Бронная» является контролируемой зоной.

Для исключения несанкционированного доступа на объект, проектом предусмотрена охранная сигнализация.

Охранная сигнализация строится на базе интеллектуального шкафа индивидуальной разработки контроля охранной сигнализации ЩОС1 БКИТ.241388.КНС-Бронная-ОС.01ВО (далее - щит охраны ЩОС1).

Запроектированная охранная сигнализация предназначена для:

- Круглосуточного автоматического обнаружения проникновения на станцию;
- Сигнализации о проникновении на станцию на пост диспетчера с круглосуточным пребыванием дежурного персонала;
- Оповещения о проникновении непосредственно на станции.

Информационная безопасность
Техническое задание
БКИТ.241388.КНС-Бронная-ИБ.МУ
На 35 листах

Оглавление

Обозначения и сокращения	5
1. Общие сведения	6
1.1 Полное наименование системы и её условное обозначение:	6
1.2 Перечень документов, на основании которых создаётся СОИБ.....	6
1.3 Плановые сроки начала и окончания работы по созданию СОИБ	6
1.4 Источник и порядок финансирования работ	6
1.5 Порядок оформления и предъявления заказчику результатов работ по созданию системы, по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы.....	7
2. Назначение и цели создания системы	7
2.1 Назначение системы.....	7
2.2 Цели создания системы.....	7
3. Характеристика АСУ ТП.....	8
4. Требования к СОИБ	9
4.1 Требования к СОИБ в целом.....	9
4.1.1 Требования к структуре и функционированию СОИБ.....	9
4.1.2 Требования к численности, квалификации персонала и режиму его работы	12
4.1.3 Показания назначения	13
4.1.4 Требования к надежности	14
4.1.5 Требования по сохранности информации при авариях	14
4.1.6 Требования безопасности	14
4.1.7 Требования по эргономике и технической эстетике.....	15
4.1.8 Требования к транспортабельности	15
4.1.9 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению ...	15
4.2 Требования к функциям СОИБ	15
4.2.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа:	15
4.2.2 Меры по управлению доступом субъектов доступа к объектам доступа	16

4.2.3	Меры по защите машинных носителей	16
4.2.4	Меры по аудиту информационной безопасности	17
4.2.5	Меры по антивирусной защите	17
4.2.6	Меры по обеспечению целостности	18
4.2.7	Меры по обеспечению доступности	18
4.2.8	Меры по защите технических средств и систем	19
4.2.9	Меры по защите АСУ ТП и её компонентов	19
4.2.10	Меры по реагированию на компьютерные инциденты	19
4.2.11	Меры по управлению конфигурацией АСУ ТП	20
4.2.12	Меры по управлению обновлениями АСУ ТП	20
4.2.13	Меры по планированию мероприятий по обеспечению защиты информации	20
4.2.14	Меры по информирование и обучению персонала	21
5.	Состав и содержание работ по созданию СОИБ	21
5.1	Требования к этапу обследования АСУ ТП	22
5.2	Требования к этапу категорирования АСУ ТП	22
5.3	Требования к этапу формирования требований к защите информации	22
5.4	Требования к этапу разработки	24
5.5	Требования к этапу поставки оборудования и ПО	27
5.5.1	Требования к сервисному и гарантийному обслуживанию на поставляемые технические средства	27
5.5.2	Требования к упаковке и маркировке	28
5.5.3	Требования к контролю качества при приёмке товара	28
5.5.4	Требование к сертификации	28
5.5.5	Требования к безопасности	28
5.6	Требования к этапу внедрения	28
6.	Порядок контроля и приёмки системы	29
6.1	Виды испытаний	29
6.1.2	Предварительные испытания	29
6.1.3	Опытная эксплуатация	30

6.1.4 Приёмочные испытания	31
7. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие	32
8. Требования к документированию.....	34
9. Источники разработки	34

Обозначения и сокращения

АРМ	Автоматизированное рабочее место
АСУ ТП	Автоматизированная система управления технологическим процессом
ИС	Информационная система
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
УБИ	Угроза безопасности информации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
КВО	Критически важный объект
ПЛК	Программируемый логический контроллер
КИПиА	Контрольно-измерительные приборы и автоматика.
СОИБ	Система обеспечения информационной безопасности
КНС	Канализационная насосная станция

1. Общие сведения

1.1 Полное наименование системы и её условное обозначение:

Разработка проектной и рабочей документации автоматизации технологических процессов объекта: «Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска».

Сокращённое наименование системы: СОИБ АСУ ТП КНС «Бронная».

Номер договора: 01/23-Бронная-Пр

Наименование предприятий заказчика и разработки АСУ ТП и их реквизиты:

Заказчик: ООО «Строительные решения. Специализированный застройщик»

Разработчик: Общество с ограниченной ответственностью производственное объединение «ОРИОН-АКВА».

Адрес 630005, г. Новосибирск, ул. Писарева д. 53.

1.2 Перечень документов, на основании которых создаётся СОИБ

ДОГОВОР № 01/23-Бронная-Пр от 27.01.2023 на разработку рабочей документации по информационной безопасности объекта: «Многоквартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска».

1.3 Плановые сроки начала и окончания работы по созданию СОИБ

Начало работ по созданию СОИБ: 27.01.2023

Окончание работ по созданию СОИБ: 05.04.2023

1.4 Источник и порядок финансирования работ

Финансирование осуществляет Заказчик. Порядок и объем финансирования определен в договоре № 01/23-Бронная-Пр.

1.5 Порядок оформления и предъявления заказчику результатов работ по созданию системы, по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы.

После завершения работ Исполнитель предъявляет Заказчику комплект документов, разработанных в рамках данного технического задания, а акты сдачи выполненных работ. Порядок оформления результатов работ определяются на основании действующего законодательства в сфере информационной безопасности АСУ ТП.

2. Назначение и цели создания системы

2.1 Назначение системы

СОИБ АСУ ТП КНС «Бронная» предназначена для защиты ресурсов АСУ ТП от актуальных угроз информационной безопасности.

2.2 Цели создания системы

Цели создания СОИБ являются:

- Создание условий функционирования АСУ ТП, при которых обеспечивается выполнение требований доступности и целостности информации, принадлежащей ей;
- Соответствие мер, принятых для обеспечения безопасности информации АСУ ТП КНС, действующему законодательству Российской Федерации в сфере информационной безопасности.

3. Характеристика АСУ ТП

Действующая в настоящий момент подсистема АСУ ТП КНС МУП г. Новосибирска "ГОРВОДОКАНАЛ" включает в себя более 50-ти канализационно-насосных станций (КНС). Разрабатываемая КНС осуществляет взаимодействие с существующей корпоративной системой диспетчерского контроля и управления посредством выделенных каналов связи. На КНС «Бронная» реализуется локальная система автоматического управления КНС по требованиям МУП г. Новосибирска "ГОРВОДОКАНАЛ" и на базе принятого действующей системой АСУ ТП КНС аппаратно-программного обеспечения.

Разрабатываемая АСУ ТП является сложной трехуровневой системой, состоящей из:

1. Нижнего уровня, включающий датчики (уровня жидкости в резервуаре, температур, газового анализа), счетчик электроэнергии и исполнительные механизмы (насосные агрегаты, вентиляторы, измельчитель).

2. Среднего уровня, состоящего из программируемых логических контроллеров (управления главными насосами, дренажной системой, мониторинга работы станции, управления системой вентиляции, измельчителем. Обработка информации на этом уровне происходит по единому алгоритму: прием сведений, их анализ и обработка и выдача команд на нижний уровень.

3. Верхнего уровня, построенного на базе серверного оборудования и АРМов операторов, обеспечивающих сбор и хранение данных, а также архивацию информации, полученной от контроллеров, и представление ее в виде визуальных средств. Таким образом, оператор системы может ознакомиться с параметрами процесса, протекающего на объекте.

Компоненты нижнего и среднего уровней связаны между собой проводными линиями связи в единую распределенную систему управления, работающую в режиме реального времени. Средний и верхний уровни

объединены в сеть посредством организации GSM-канала передачи данных, с возможностью перехода на канал ВОЛС, при появлении технической возможности. Канал связи является выделенными, отсутствует подключение к сети Интернет. Таким образом, можно дистанционно и оперативно контролировать работу объекта и избегать аварийных ситуаций, обеспечивая наибольшую производительность и безопасность.

Взаимодействие верхнего и среднего уровня АСУ ТП КНС понимается как взаимодействие сторонних систем. В рамках данного проекта рассматривается только нижний и средний уровень АСУ ТП КНС «Бронная». АСУ ТП КНС «Бронная» по своей структуре, является локальной системой, так как все устройства, к ней относящиеся находятся в пределах контролируемой зоны объекта.

В случае возникновения неисправности АСУ ТП КНС «Бронная» возможен переход на ручное управление станцией персоналом.

4. Требования к СОИБ

4.1 Требования к СОИБ в целом

4.1.1 Требования к структуре и функционированию СОИБ

4.1.1.1 Перечень подсистем СОИБ, их назначение и основные характеристики, требования к числу уровней иерархии и степени централизации

СОИБ должна предоставить собой комплекс организационно-технических мер, направленных на противодействие актуальным угрозам безопасности информации в отношении обрабатываемой информации, средства защиты информации и программно-аппаратного обеспечения АСУ ТП.

В состав мер по обеспечению безопасности информации, реализуемых в рамках СОИБ, предварительно должны входить (с учётом набора актуальных угроз):

- а. идентификацию и аутентификацию (ИАФ);

- b. управление доступом (УПД);
- c. ограничение программной среды (ОПС);
- d. защиту машинных носителей информации (ЗНИ);
- e. аудит безопасности (АУД);
- f. антивирусную защиту (АВЗ);
- g. предотвращение вторжений (компьютерных атак) (СОВ);
- h. обеспечение целостности (ОЦЛ);
- i. обеспечение доступности (ОДТ);
- j. защиту технических средств и систем (ЗТС);
- k. защиту информационной (автоматизированной) системы и ее компонентов (ЗИС);
- l. реагирование на компьютерные инциденты (ИНЦ);
- m. управление конфигурацией (УКФ);
- n. управление обновлениями программного обеспечения (ОПО);
- o. планирование мероприятий по обеспечению безопасности (ПЛН);
- p. обеспечение действий в нештатных ситуациях (ДНС);
- q. информирование и обучение персонала (ИПО).

Более детально набор мер должен определяться во время разработки технического проекта таким образом, чтобы не нарушить штатное функционирование АСУ ТП КНС «Бронная». Требования к функционированию определяются действующими нормативно-правовыми актами, регламентирующими вопросы защиты информации в АСУ ТП, и описаны в разделе 4.2 настоящего ТЗ. В случае отсутствия возможности прямой реализации мер по обеспечению информационной безопасности настоящего ТЗ, допускается их замена компенсирующими мерами.

4.1.1.2 Требования к способам и средствам связи для информационного обмена между компонентами СОИБ

Информационный обмен между компонентами СОИБ должен осуществляться с применением существующей в АСУ ТП КНС «Бронная» локальной вычислительной сети.

4.1.1.3 Требования к характеристикам взаимосвязей создаваемой СОИБ со смежными системам, требования к её совместимости, в том числе указания о способах обмена информацией

Должно быть обеспечено взаимодействие компонентов СОИБ с сетевыми средствами с использованием технологий Ethernet (IEEE 802.3), технологии VLAN (IEEE 802.1Q), протоколов TCP (RFC 793), IP (RFC 791) UDP (RFC 768), ICMP (RFC792).

4.1.1.4 Требования к режимам функционирования СОИБ

В СОИБ должны иметься следующие режимы функционирования:

- а. Штатный режим. Все функции СОИБ выполняются в полном объёме в соответствии с проектом.
- б. Сервисный режим. В данном режиме в один или несколько компонентов СОИБ могут быть временно выведены из штатного режима, для проведения обслуживания или обновления. В данном случае допускается неполное выполнение функций СОИБ или снижение производительности на время проведения регламентных работ.
- с. Аварийный режим. Данный режим связан с выходом из строя компонентов СОИБ, должен обеспечивать частичное выполнение функций СОИБ.

4.1.1.5 Требования по диагностированию системы

Компоненты СОИБ должны иметь механизм для диагностики системы. Допускается реализация требований путем ведения журналов событий и последующим их анализом.

4.1.1.6 Перспективы развития, модернизация СОИБ

Необходимость пересмотра структуры и состава может быть продиктована следующими условиями:

- a. Значительное изменение характеристик, структуры, состава защищаемой системы и её компонентов, приводящее к неполноценной работе СОИБ;
- b. Возможное повышение эффективности СОИБ, в случае изменения её структуры, состава;
- c. Возможное снижение затрат на создание или эксплуатацию СОИБ;
- d. Изменения законодательства в сфере обеспечения информационной безопасности;
- e. Изменение условий эксплуатации АСУ ТП КНС.

4.1.2 Требования к численности, квалификации персонала и режиму его работы

4.1.2.1 Требования к численности персонала СОИБ

Необходимо наличие подразделения по защите информации, целью которого будет поддержка работы СОИБ или возложить данную функцию на существующее подразделение, обслуживающее другие АСУ ТП предприятия с привлечением администратора безопасности.

Поддержка функционирования аппаратных и программных средств защиты не должно изменять организационную структуру и численность персонала подразделения по защите информации, если данное подразделение уже создано.

Структурное подразделение ИБ должно состоять как минимум из:

- ответственного за обеспечение безопасности информации – не менее одного человека;
- администраторов информационной безопасности – не менее одного человека.

Данные лица должны выполнять следующие должностные обязанности:

- ответственный за обеспечение безопасности информации – обеспечивает управление отделом ИБ, отвечает за мониторинг за выполнением персоналом ОРД и других нормативно-правовых документов.
- администратор информационной безопасности – отвечает за мониторинг работы СОИБ, выполняет работы по восстановлению работы СОИБ в случае остановки ее работы.

4.1.2.2 Требования к квалификации персонала, порядку его подготовки, контроля его знаний и навыков

Персонал СОИБ должен знать и выполнять требования организационно-распорядительных документов.

В случае создания отдельного подразделения, каждый его сотрудник должен обладать навыками работы с каждым СЗИ, входящим в состав СОИБ. В ином случае, каждый сотрудник должен пройти инструктаж, по определению корректности работы СЗИ, чтобы в случае нештатной работы СОИБ сообщить об этом администратору безопасности.

Назначенный ответственным за работу СОИБ должен обладать профильным образованием или пройти курсы переподготовки.

4.1.2.3 Требуемый режим работы персонала

В штатном или сервисном режиме работы СОИБ работа персонала ведется строго по их штатному режиму работы

В аварийном режиме работы, вводится круглосуточный режим работы, до устранения неисправности.

4.1.3 Показания назначения

Нейтрализация актуальных угроз, описанных в Модели угроз, является параметром, характеризующим степень соответствия СОИБ ее назначению.

4.1.4 Требования к надежности

СЗИ, входящие в состав СОИБ должны обеспечивать круглосуточное функционирование СОИБ, а также иметь инструменты для резервного копирования конфигурации и быстрого восстановления работы, в случае сбоя работы.

Требования к количественным значениям и методам оценки показателей надежности не предъявляется. Надежность обеспечивается производителем СЗИ на условиях гарантии.

4.1.5 Требования по сохранности информации при авариях

Необходимо использовать системы резервного копирования для минимизации объема потерянных данных при сбоях в системе.

4.1.6 Требования безопасности

Применяемые СЗИ должны обеспечивать защиту эксплуатирующего персонала от поражения электрическим током в соответствии ГОСТ 12.2.003 и ГОСТ 12.2.007.

Факторы, оказывающие вредное воздействие на здоровье обслуживающего персонала, не должны превышать действующих норм (СанПин 2.2.2./2.4.1340-03 от 03.06.2003).

Значения эквивалентного уровня акустического шума, создаваемого аппаратурой системы, должно соответствовать ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение», но не превышать следующих величин:

- 50 дБ - при работе технологического оборудования и средств вычислительной техники без печатающего устройства;
- 60 дБ - при работе технологического оборудования и средств вычислительной техники с печатающим устройством.

4.1.7 Требования по эргономике и технической эстетике

Не предъявляются.

4.1.8 Требования к транспортабельности

Не предъявляются.

4.1.9 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению

В СОИБ должны применяться унифицированные средства, для облегчения обслуживания, совместимые с остальными компонентами системы. Данные средства должны предусматривать возможность технического обслуживания, если оно требуется.

4.2 Требования к функциям СОИБ

Защищаемая АСУ ТП, имеет третий класс защищенности, в соответствии с актом определения класса защищенности АСУ ТП КНС «Бронная». К функциям СОИБ третьего класса защищенности, в соответствии с Требования 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, предъявляются ниже описанные требования.

4.2.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа:

Набор мер по идентификации и аутентификации пользователей должен регламентировать работу с идентификаторами и должны обеспечивать:

- a. Регламентация правил и процедур идентификации;
- b. Идентификацию и аутентификацию пользователей и иницилируемых ими процессов
- c. Идентификацию и аутентификацию устройств;

- d. Управление идентификаторами (присвоение, создание, уничтожение, изменение);
- e. Управление средствами аутентификации: выдача, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- f. Защиту обратной связи при вводе аутентификационной информации (исключение отображение вводимого пароля пользователем).

4.2.2 Меры по управлению доступом субъектов доступа к объектам доступа

Данный набор мер, предназначен для защиты от несанкционированного доступа к ресурсам АСУ ТП КНС «Бронная» и должен обеспечивать:

- a. Управление учетными записями пользователей (Создание, модификация, удаление, блокирование);
- b. Реализацию дискреционного метода доступа к ресурсам системы;
- c. Разделение полномочий пользователей АСУ ТП КНС «Бронная» в зависимости от их роли, с назначением минимально необходимых им прав и привилегий;
- d. Ограничение неуспешных попыток входа в АСУ ТП «Бронная» с блокированием учетной записи, с которой совершались попытки входа;
- e. Запрет действий пользователей, разрешенных до идентификации и аутентификации;
- f. Блокирование сеанса доступа к АСУ ТП КНС «Бронная» при неактивности пользователя.

4.2.3 Меры по защите машинных носителей

Набор мер по защите машинных носителей регламентирует порядок работы машинных носителей и интерфейсов их взаимодействия в АСУ ТП КНС «Бронная» и реализует:

- a. Учет машинных носителей информации;

- b. Управление физическим доступом к машинным носителям информации;
- c. Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации;
- d. Контроль подключения машинных носителей информации;
- e. Стирание информации на машинных носителях информации при выводе носителя из эксплуатации.

4.2.4 Меры по аудиту информационной безопасности

Данный набор мер определяет состав и содержащуюся информацию о ресурсах АСУ ТП и событиях информационной безопасности, а также порядок сбора, хранения и представления событий, подлежащих регистрации. Данный набор должен реализовывать:

- a. Инвентаризацию информационных ресурсов АСУ ТП;
- b. Анализ уязвимостей и их устранение;
- c. Регистрацию и хранение событий информационной безопасности
- d. Защиту информации о событиях безопасности
- e. Мониторинг (контроль) безопасности;
- f. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
- g. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- h. Порядок проведения внутренних аудитов.

4.2.5 Меры по антивирусной защите

Меры по антивирусной защите предназначены для защиты АСУ ТП КНС «Бронная» от вирусов (вредоносных программ) и реализуется с помощью организационных мер, направленных на антивирусную защиту. Основной функцией, которых является ограничение возможностей

нарушителя по внедрению вредоносного программного кода (вируса) и удаление (по возможности) его из системы.

Меры по антивирусной защите должны реализовывать:

- а. Обнаружение фактов вирусного заражения всеми известными вирусами;
- б. Сигнализация в случае обнаружения фактов заражения вирусом;
- с. Возможность удаления зараженного файла и восстановления работоспособности АСУ ТП КНС «Бронная» в случае заражения вредоносным программным кодом;
- д. Блокирования доступа к отчуждаемым носителям, в случае обнаружения угрозы вирусного заражения;
- е. Возможность обновления баз данных признаков вредоносных компьютерных программ.

4.2.6 Меры по обеспечению целостности

Меры по обеспечению целостности направлены на то, что изменять информацию смогут только легитимные пользователи. Реализуется путем контроля целостности программного обеспечения.

4.2.7 Меры по обеспечению доступности

Данные направлены на обеспечение непрерывного доступа к ресурсам АСУ ТП КНС «Бронная» легитимных пользователей и должны обеспечить:

- а. Наличие работоспособной резервной копии программного обеспечения АСУ ТП КНС «Бронная»;
- б. Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала;
- с. Обеспечения возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

4.2.8 Меры по защите технических средств и систем

Меры по защите технических средств реализуют:

- а. Организацию контролируемой зоны, в пределах которой постоянно размещаются технические средства, обрабатывающие информацию, исполнительные устройства;
- б. Обеспечивают управление физическим доступом к ресурсам АСУ ТП и помещениям, где они расположены.

4.2.9 Меры по защите АСУ ТП и её компонентов

Меры по защите АСУ ТП КНС «Бронная» и её компонентов должны обеспечивать:

- а. Разделение функций по управлению (администрированию) автоматизированной системой управления, управлению (администрированию) системой защиты, функций по обработке информации и иных функций автоматизированной системы управления
- б. Эшелонированную (многослойную) защиту АСУ ТП КНС «Бронная»;
- в. Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании (DOS, DDOS-атак)
- г. Соккрытие архитектуры и конфигурации АСУ ТП КНС «Бронная».

4.2.10 Меры по реагированию на компьютерные инциденты

Для обеспечения выявления инцидентов и реагирование на них необходимо:

- а. Определить правила и порядок выявления (обнаружение, идентификации и регистрации) инцидентов информационной безопасности;
- б. Определить порядок информирования о компьютерных инцидентах;

- с. Определить правила и порядок реагирования на инциденты информационной безопасности;
- d. Определить порядок анализа (определения источников и причин) инцидентов информационной безопасности;
- е. Определить порядок принятия мер по устранению последствий инцидентов информационной безопасности
- f. Определить порядок по предотвращению повторного возникновения инцидентов информационной безопасности.

4.2.11 Меры по управлению конфигурацией АСУ ТП

В рамках реализации данных мер необходимо:

- а. Обеспечить установку только разрешенного программного обеспечения;
- b. Обеспечить процедуру управления изменениями в ресурсах АСУ ТП.

4.2.12 Меры по управлению обновлениями АСУ ТП

Данный набор мер должен:

- а. Определять порядок поиска и получения обновлений программного обеспечения от доверенного источника;
- b. Порядок проведения контроля целостности получаемых обновлений программного обеспечения;
- с. Порядок предварительного тестирования обновлений программного обеспечения;
- d. Порядок установки тестирования обновлений программного обеспечения;

4.2.13 Меры по планированию мероприятий по обеспечению защиты информации

Данный набор мер должен регламентировать:

- а. Разработку, утверждение и актуализацию плана мероприятий по обеспечению защиты информации;
- б. Контроль выполнения мероприятий по обеспечению защиты информации.

4.2.14 Меры по информирование и обучению персонала

Данные меры должны обеспечивать:

- а. Обучение персонала безопасной работе с АСУ ТП КНС «Бронная»;
- б. Информирование персонала о существующих угрозах информационной безопасности, о правилах эксплуатации СОИБ и её отдельных компонентов
- с. Обучение правилам эксплуатации СОИБ и её отдельных компонентов
- д. Осуществление контроля осведомленности персонала об угрозах информационной безопасности и правилах безопасной работы.

5. Состав и содержание работ по созданию СОИБ

Процесс создания СОИБ производится в несколько этапов. Сроки выполнения работ определяются условиями договора с Исполнителями.

Этап 1. Обследование АСУ ТП.

Этап 2. Категорирование АСУ ТП.

Этап 3. Формирование требований к защите информации, обрабатываемой в рамках АСУ ТП.

Этап 3. Разработка СОИБ.

Этап 4. Поставка оборудования и программного обеспечения.

Этап 5. Внедрение СОИБ

5.1 Требования к этапу обследования АСУ ТП

Обследование АСУ ТП заключается в исследовании работы АСУ ТП, определении технического и программного состава АСУ ТП и определении взаимодействий между подсистемами АСУ ТП.

По итогам обследования АСУ ТП формируется отчет об обследовании, содержащий:

- Описание работы АСУ ТП;
- Состав АСУ ТП;
- Взаимодействие АСУ ТП со смежными системами;
- Описание существующих мер по обеспечению безопасности информации.

5.2 Требования к этапу категорирования АСУ ТП

Процесс категорирования АСУ ТП заключается в присвоении класса защищенности на основании анализа критичности технологических процессов, проходящих в АСУ ТП. Присвоение класса защищенности осуществляется в соответствии с Приложением N 1 к «Требованиям 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»

Результатом этапа категорирования АСУ ТП является «Акт определения класса защищенности автоматизированной системы управления технологическим процессом».

5.3 Требования к этапу формирования требований к защите информации

Формирование требований к защите информации, обрабатываемой в составе АСУ ТП, осуществляется с учетом ГОСТ Р 51583 «Защита

информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в АСУ ТП, и разработку на их основе модели угроз безопасности информации;
- определение детальных требований к СОИБ.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России.

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации ФСТЭК (bdu.fstec.ru).

При определении угроз безопасности информации учитываются структурно функциональные характеристики АСУ ТП, включающие структуру и состав АСУ ТП, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными системами и информационно-телекоммуникационными сетями, режимы обработки информации в АСУ ТП и в ее отдельных сегментах, а также иные характеристики АСУ ТП, применяемые информационные технологии и особенности ее функционирования.

Модель угроз безопасности информации должна содержать описание АСУ ТП и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Требования к СОИБ АСУ ТП включаются в частное техническое задание на создание СОИБ, разрабатываемое с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624 и приказом ФСТЭК от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

5.4 Требования к этапу разработки

Разработка СОИБ должна осуществляться в соответствии с частным техническим заданием на создание СОИБ с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624

Разработка СОИБ должна включать следующие стадии:

- Проектирование СОИБ;
- Разработка комплекта эксплуатационной документации на СОИБ;
- Макетирование и тестирование СОИБ (при необходимости).
- СОИБ и ее технические решения не должны влиять на штатный режим работы АСУ ТП КНС «Бронная».

- При проектировании СОИБ должны быть выполнены следующие задачи:

- определены типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

- определены методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, методик безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

- выбраны меры защиты информации, подлежащие реализации в составе СОИБ;

- определены виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

- определена структура СОИБ, включая состав (количество) и места размещения ее элементов;

- осуществлен выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также уровня (класса) защищенности АСУ ТП;

- определены требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также

устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;

- определены меры защиты информации при информационном взаимодействии с иными системами и информационно-телекоммуникационными сетями.

Результаты проектирования системы защиты информации информационной системы отражаются в рабочей документации, разрабатываемой с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее - ГОСТ 34.201).

При отсутствии необходимых средств защиты информации, допускается применение компенсирующих мероприятий по обеспечению информационной безопасности АСУ ТП

Разработка эксплуатационной документации на СОИБ должна осуществляться в соответствии с настоящим техническим заданием.

Эксплуатационная документация на СОИБ разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

- структуры СОИБ;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- правил эксплуатации СОИБ.
- При макетировании и тестировании СОИБ должны осуществляться:

- проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

- проверка выполнения выбранными средствами защиты информации требований к СОИБ;
- корректировка проектных решений, разработанных при создании СОИБ (при необходимости).

5.5 Требования к этапу поставки оборудования и ПО

5.5.1 Требования к сервисному и гарантийному обслуживанию на поставляемые технические средства

Таблица 1 - Требования к поставке, сервисному и гарантийному обслуживанию оборудования и программного обеспечения.

№ п/п	Технические требования
1	Поставляемый товар должен быть новым товаром (товаром, который не был в употреблении, не прошел ремонт, в том числе восстановление, замену составных частей, восстановление потребительских свойств) и официально поддерживаться компанией производителем оборудования.
2	Поставщик должен своими силами доставить товар по адресу Заказчика и обеспечить их разгрузку на склад Заказчика.
3	Оборудование и программное обеспечение должно поставляться с расширенной поддержкой от производителя сроком на 12 месяцев, обеспечивающей: <ul style="list-style-type: none"> •Замену оборудования при выходе его из строя по принципу «следующий рабочий день»; •Круглосуточную поддержку по электронной почте, телефону; •Доступ к регулярным обновлениям программного обеспечения по безопасности, исправлению выявленных ошибок, устранению уязвимостей, расширению функциональности программного обеспечения; •Интерактивный круглосуточный доступ к технической документации, базе знаний и инструментам самодиагностики.

5.5.2 Требования к упаковке и маркировке

Оборудование должно поставляться в упаковке, обеспечивающей безопасность транспортировки и сохранность его качества в течение гарантийного срока хранения.

Серийный номер на коробке и на оборудовании должны совпадать.

5.5.3 Требования к контролю качества при приёмке товара

Заказчик или его представители имеют право провести технический контроль и/или испытания товара для подтверждения их соответствия техническим условиям контракта и при этом не понести каких-либо дополнительных расходов.

5.5.4 Требование к сертификации

Средства защиты информации, предназначенные для использования в составе СОИБ, должны быть сертифицированы на соответствие требованиям по защите информации.

5.5.5 Требования к безопасности

Все оборудование не должно содержать токсичных, радиоактивных и других веществ, угрожающих здоровью человека.

5.6 Требования к этапу внедрения

Работы по внедрению СОИБ должны быть выполнены в рамках, разработанных и согласованных с Заказчиком проектных решений на СОИБ и ее службы (функциональные подсистемы):

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;

- обеспечение целостности АСУ ТП;
- обеспечение доступности информации;
- защита технических средств;
- защита АСУ ТП и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией АСУ ТП и системы обеспечения информационной безопасности;
- управление обновлениями ПО;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала;
- резервирование каналов связи. Работы по внедрению должны включать:
- подготовку объекта Заказчика к внедрению компонентов СОИБ (соответствующие мероприятия по подготовке объектов информатизации к внедрению СОИБ должны быть отражены в разрабатываемой проектной документации на СОИБ);
- пусконаладочные работы;
- предварительные испытания;
- опытную эксплуатацию;
- приемочные испытания.

6. Порядок контроля и приёмки системы

6.1 Виды испытаний

6.1.2 Предварительные испытания

Предварительные испытания проводятся, после установки и отладки СЗИ, с целью проверки работоспособности СОИБ и соответствия создаваемой СОИБ требованиям настоящего Технического задания (ТЗ).

Предварительные производятся испытания СОИБ в соответствии с

«Виды испытаний автоматизированных систем». Результаты испытаний отражают в протоколе. Работу завершают оформлением акта приемки в опытную эксплуатацию.

В программе комплексных испытаний АСУ ТП указывают:

- перечень объектов испытания;
- состав предъявляемой документации;
- описание проверяемых взаимосвязей между объектами испытаний;
- очередность испытаний частей СОИБ;
- порядок и методы испытаний, в том числе состав программных средств и оборудования, необходимых для проведения испытаний, включая специальные стенды и полигоны.

Для проведения комплексных испытаний должны быть представлены:

- программа комплексных испытаний;
- заключение по автономным испытаниям соответствующих частей СОИБ и устранение ошибок и замечаний, выявленных при автономных испытаниях;
- комплексные тесты;
- программные и технические средства и соответствующая им эксплуатационная документация.

6.1.3 Опытная эксплуатация

Перевод СОИБ АСУ ТП в опытную эксплуатацию осуществляется после успешного прохождения предварительных испытаний.

Опытная эксплуатация СЗИ проводится с целью определения характеристик СЗИ и готовности персонала к работе в реальных условиях функционирования СЗИ, совместимости СЗИ с АСУ ТП на продолжительном отрезке времени, а также определения фактической эффективности СЗИ и, при необходимости, корректировки параметров СЗИ и документации.

Опытная эксплуатация проводится в соответствии с документом со штатным режимом работы АСУ ТП

По результатам опытной эксплуатации СЗИ принимается решение о возможности (невозможности) предъявления системы на приемочные испытания.

Опытная эксплуатация завершается оформлением акта о завершении опытной эксплуатации.

6.1.4 Приёмочные испытания

Приемочные испытания СОИБ АСУ ТП проводятся для определения соответствия СОИБ АСУ ТП требованиям Технического задания, оценки качества опытной эксплуатации и решения вопроса о возможности приемки СОИБ АСУ ТП в эксплуатацию.

Приемочные испытания проводятся в соответствии с документом «Программа и методика приемочных испытаний», которая должна содержать:

- перечень объектов испытаний
- критерии приемки системы и ее частей;
- условия и сроки проведения испытаний;
- средства для проведения испытаний;
- фамилии лиц, ответственных за проведение испытаний;
- методику испытаний и обработки их результатов;

Для проведения приемочных испытаний должна быть предъявлена следующая документация:

- техническое задание на создание АС;
- акт приемки в опытную эксплуатацию;
- рабочие журналы опытной эксплуатации;
- акт завершения опытной эксплуатации и допуска АС к приемочным испытаниям;
- программа и методика испытаний.

Приемочные испытания в первую очередь должны включать проверку:

- полноты и качества реализации функций при штатных, предельных, критических значениях параметров объекта автоматизации и в других условиях функционирования АС, указанных в ТЗ;
- средств и методов восстановления работоспособности СОИБ после отказов;
- комплектности и качества эксплуатационной документации.

Проверку полноты и качества выполнения функций СОИБ рекомендуется проводить в два этапа. На первом этапе проводят испытания отдельных функций (задач, комплексов задач). При этом проверяют выполнение требований ТЗ к функциям (задачам, комплексам задач). На втором этапе проводят проверку взаимодействия задач в системе и выполнение требований ТЗ к системе в целом.

По согласованию с Заказчиком проверка задач в зависимости от их специфики может проводиться автономно или в составе комплекса. Объединение задач при проверке в комплексах целесообразно проводить с учетом общности используемой информации и внутренних связей.

Приемочные испытания СЗИ проводятся Исполнителем в присутствии представителей Заказчика путем выполнения комплексных тестов.

7. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

Таблица 2-Требование к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие.

№ этапа работ	Наименование и состав работ по этапу	Перечень отчётных документов
1	• Обследование АСУ ТП	• Отчёт об обследовании
2	• Категорирование АСУ ТП	• Акт определения класса защищённости АСУ ТП
3	Формирование требований к защите информации, обрабатываемой в рамках	• Модель угроз безопасности информации, обрабатываемой в

	<p>АСУ ТП, в том числе:</p> <ul style="list-style-type: none"> • Определение угроз безопасности информации; • Определение требований к СОИБ. 	<p>составе АСУ ТП</p> <ul style="list-style-type: none"> • Частное техническое задание на создание СОИБ.
4	<p>Разработка СОИБ, в том числе:</p> <ul style="list-style-type: none"> • Проектирование СОИБ; • Разработка комплекта эксплуатационной документации на СОИБ; <p>Макетирование и тестирование СОИБ (при необходимости).</p>	<ul style="list-style-type: none"> • Пояснительная записка к техническому проекту; • Структурная схема комплекса технических средств; • Спецификация оборудования и ПО; • Программа и методика испытаний; • Руководство администратора; • Инструкция пользователя; • Протоколы тестирования (при необходимости); • Акт сдачи приёмки работ.
5	<ul style="list-style-type: none"> • Поставка оборудования и ПО 	<ul style="list-style-type: none"> • Акты приёма-передачи прав на использование ПО; • Техническая документация поставляемая с СЗИ.
6	<p>Внедрение СОИБ, в том числе:</p> <ul style="list-style-type: none"> • Подготовка объекта внедрения и пусконаладочные работы; • Предварительные испытания; • Опытная эксплуатация; • Приемочные испытания; • Ввод в эксплуатацию. 	<ul style="list-style-type: none"> • Акт завершения пусконаладочных работ; • Протокол предварительных испытаний; • Акт перевода системы в опытную эксплуатацию; • Акт завершения опытной эксплуатации системы; • Протокол приемочных испытаний системы. • Акт ввода в эксплуатацию

8. Требования к документированию

Виды, комплектность и содержание документов в части, определенной настоящим ТЗ, должны учитывать требования ГОСТ 34.201-89 «Информационная технология.

Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» и РД 50-34.698-90

«Автоматизированные системы. Требования к содержанию документов».

Вся разрабатываемая документация, а также штатная документация по поставляемому оборудованию и программному обеспечению должна быть выполнена на русском языке.

9. Источники разработки

а. ГОСТ Р 51583-2014. Защита информации. «Порядок создания автоматизированных систем в защищенном исполнении»;

б. ГОСТ 34.602-89 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

с. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" (с изменениями и дополнениями).

СОСТАВИЛИ

<i>Наименование организации, предприятия</i>	<i>Должность исполнителя</i>	<i>Фамилия, имя, отчество</i>	<i>Подпись</i>	<i>Дата</i>

СОГЛАСОВАНО

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата

Информационная безопасность
БКИТ.241388.КНС-Бронная-ИБ.МУ

МОДЕЛЬ УГРОЗ

На 40 листах

Содержание

1. Общие положения	6
2. Описание АСУ ТП	7
4. Возможные объекты воздействия угроз безопасности информации	11
5. Источники угроз безопасности информации	12
6. Способы реализации (возникновения) угроз безопасности информации	22
7. Описание угроз АСУ ТП	26

Обозначения и сокращения

АРМ	Автоматизированное рабочее место
АСУ ТП	Автоматизированная система управления технологическим процессом
ИС	Информационная система
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
УБИ	Угроза безопасности информации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
КВО	Критически важный объект
ПЛК	Программируемый логический контроллер
КИПиА	Контрольно-измерительные приборы и автоматика.
СОИБ	Система обеспечения информационной безопасности
КНС	Канализационная насосная станция

Термины и определения

Автоматизированная система управления технологическим процессом – группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Защита информации – принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Источник угрозы безопасности информации – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Средство защиты от несанкционированного доступа – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на технологический процесс в АСУ ТП.

Аутентификация – процедура проверки подлинности

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации в АСУ ТП.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1. Общие положения

Настоящая модель определяет актуальные угрозы безопасности информации при её обработке в АСУ ТП КНС «Бронная» (далее АСУ ТП) и должна использоваться при задании требований к системе защиты информации указанной АСУ ТП.

Номер договора: 01/23-Бронная-Пр

Наименование предприятий заказчика и разработки АСУ ТП и их реквизиты:

Заказчик: ООО «Строительные решения. Специализированный застройщик»

Разработчик: Общество с ограниченной ответственностью производственное объединение «ОРИОН-АКВА». Адрес 630005, г. Новосибирск, ул. Писарева д. 53.

Для разработки модели угроз АСУ ТП использовались следующие нормативные и методические документы, стандарты:

Приказ от 14 марта 2014 г. N 31. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

- Банк данных угроз ФСТЭК.
- Методика оценки угроз безопасности информации, 2021

Модель угроз формируется и утверждается владельцем АСУ ТП и может быть пересмотрена:

- по решению владельца на основе периодически проводимых им анализа и оценки угроз безопасности информации с учетом особенностей и (или) изменений конкретной АСУ ТП;

- по результатам мероприятий, направленных на осуществление контроля выполнения требований к обеспечению безопасности информации при их обработке в АСУ ТП.

Принципы формирования модели угроз:

- безопасность защищаемой информации в АСУ ТП обеспечивается с помощью СОИБ и мерами промышленной безопасности;
- защищаемая информация обрабатывается и хранится в АСУ ТП с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые и косвенные угрозы защищаемой информации;

В модели угроз представлено описание АСУ ТП и её структурно – функциональных характеристик, состава и режима обработки защищаемой информации, определение класса защищённости АСУ ТП, описание угроз безопасности информации.

Описание угроз безопасности информации включает:

- описание возможностей нарушителя;
- описание возможных уязвимостей АСУ ТП;
- оценку вероятности (возможности) реализации угроз;
- оценку степени и вида ущерба от реализации угроз;
- определение актуальности УБИ.

2. Описание АСУ ТП

Для обеспечения оптимальной работы, высокой устойчивости к отказам и безопасной эксплуатации установок безопасности для объекта: «Многokвартирные многоэтажные дома № 1, 2 (по ГП) с объектами обслуживания жилой застройки во встроенных помещениях по ул. Бронная в Кировском районе г. Новосибирска».

Канализационная насосная станция предназначена для перекачивания канализационных стоков.

Автоматизированная система управления технологическим процессом канализационной насосной станции предназначена для оперативного мониторинга параметров технологического процесса, автоматизированного контроля и управления технологическим процессом и сопутствующими локальными автоматическими подсистемами АСУ ТП.

Действующая в настоящий момент подсистема АСУ ТП КНС МУП г. Новосибирска "ГОРВОДОКАНАЛ" включает в себя более 50-ти канализационных насосных станций (КНС). Разрабатываемая КНС осуществляет взаимодействие с существующей корпоративной системой диспетчерского контроля и управления посредством выделенных каналов связи. На КНС реализуется локальная система автоматического управления по требованиям МУП г. Новосибирска "ГОРВОДОКАНАЛ" и на базе принятого действующей системой АСУ ТП КНС аппаратно-программного обеспечения.

Разрабатываемая АСУ ТП является сложной трехуровневой системой, состоящей из:

1. Нижнего уровня, включающего датчики и исполнительные механизмы.
2. Среднего уровня, состоящего из программируемых логических контроллеров. Обработка информации на этом уровне происходит по единому алгоритму: прием сведений, их анализ и обработка, и выдача команд на нижний уровень.

3. Верхнего уровня, построенного на базе серверного оборудования и АРМов операторов, обеспечивающих сбор и хранение данных, а также архивацию информации, полученной от контроллеров, и представление ее в виде визуальных средств. Таким образом, оператор системы может ознакомиться с параметрами процесса, протекающего на объекте.

Компоненты нижнего и среднего уровней связаны между собой проводными линиями связи в единую распределенную систему управления, работающую в режиме реального времени. Взаимодействие верхнего и среднего уровня АСУ ТП понимается как взаимодействие сторонних систем.

Канал связи является выделенными, отсутствует подключение к сети Интернет. Таким образом, можно дистанционно и оперативно контролировать работу объекта и избегать аварийных ситуаций, обеспечивая наибольшую производительность и безопасность.

Персонал АСУ ТП

Персонал, эксплуатирующий АСУ ТП разбивается на следующие функциональные роли:

- Начальник смены АСУ ТП
- Системный администратор АСУ ТП.
- Сотрудник, обслуживающие помещения АСУ ТП

Персонал АСУ ТП имеет только локальный доступ к средствам управления и мониторинга АСУ ТП в рамках их должностных обязанностей.

В соответствии с должностными обязанностями диспетчер в процессе эксплуатации АСУ ТП выполняет следующие функции:

- мониторинг показателей и текущих параметров технологического процесса;
- реагирование на сигнализацию, уведомление обслуживающего персонала о нештатных ситуациях в рамках их должностных инструкций.

Системный администратор в процессе эксплуатации АСУ ТП выполняет следующие функции:

- конфигурирование, настройка, техническое обслуживание контроллеров АСУ ТП;
- реагирование на уведомления операторов о нештатных ситуациях и устранение причин нештатной ситуации.

Инженер по АСУ ТП выполняет техническое обслуживание шкафов АСУ ТП, датчиков измерительных систем и исполнительных элементов и устройств АСУ ТП.

Принятые меры по обеспечению информационной безопасности АСУ ТП

Технические и программные средства, функционал которых направлен на обеспечение информационной безопасности АСУ ТП

Для идентификации и аутентификации пользователей системы используются штатные механизмы операционных систем, на каждом устройстве существует одна учетная запись с правами администратора, для настройки АРМ и для осуществления работы системы.

Обеспечение физической безопасности АСУ ТП

Здания, в границах которых размещаются технические средства АСУ ТП, является контролируемой зоной.

Сторонние организации на территории объекта не размещаются. Доступ в помещения, в которых находятся технические средства АСУ ТП, имеют сотрудники, обслуживающие станцию, и сотрудники сторонних организаций, в сопровождении сотрудников, обслуживающих станцию.

Неконтролируемый доступ к техническим средствам АСУ ТП затруднен, в связи с наличием охранной сигнализации и запираемых на замок дверей. Шкафы автоматизации имеют запирающиеся замки. Проектная и эксплуатационная документация на бумажных носителях хранится в запираемых шкафах и ящиках.

Для исключения несанкционированного доступа на объект, предусмотрена охранная сигнализация.

Запроектированная охранная сигнализация предназначена для:

- Круглосуточного автоматического обнаружения проникновения на территорию объекта;
- Сигнализации о проникновении на территорию объекта на ДП НФСЗ с круглосуточным пребыванием дежурного персонала.

Определение уровня защищённости АСУ ТП

Таблица 1

Категория	Показатель	Уровень проектной защищённости
По структуре АСУ ТП	Локальная АСУ ТП	Средний
По архитектуре АСУ ТП	Использование разных операционных систем	Средний
	Использование выделенных каналов связи	Средний
По наличию (отсутствию) взаимосвязей с иными	Взаимодействующая с системами	Низкая

информационными системами		
По наличию (отсутствию) взаимосвязей (подключений) к сетям связи	Подключённая	Низкая
По размещению технических средств	Расположенные в пределах одной контролируемой зоны	Высокая
По режимам обработки информации	Многопользовательский	Низкий
По режимам разграничения прав доступа	С разграничением	Средний
По режимам разделения функций по управлению информационной системой	Без разделения	Низкий
По подходам к сегментированию АСУ ТП	Не сегментирована	Низкий

Исходя из приведённых в таблице 1 показателей, проектная защищенность АСУ ТП принимается, как низкая.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

Определение вида ущерба и типовые негативные последствия от реализации угроз безопасности информации:

Таблица 2. Виды рисков (ущерба) и типовые негативные последствия

№	Виды риска (ущерба)	Возможные типовые негативные последствия
1	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Нарушение штатного режима

№	Виды риска (ущерба)	Возможные типовые негативные последствия
		<p>функционирования автоматизированной системы управления и управляемого объекта и/или процесса.</p> <p>Срыв запланированной сделки с партнером.</p> <p>Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.</p> <p>Потеря конкурентного преимущества.</p> <p>Нарушение деловой репутации.</p> <p>Снижение престижа.</p> <p>Дискредитация работников.</p> <p>Утрата доверия.</p> <p>Причинение имущественного ущерба.</p> <p>Неспособность выполнения договорных обязательств.</p> <p>Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).</p> <p>Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).</p> <p>Принятие неправильных решений.</p>

4. Возможные объекты воздействия угроз безопасности информации

Таблица 3. Возможные объекты воздействия угроз

Негативные последствия	Объекты воздействия	Виды воздействия
Некорректная работа АСУ ТП (У1)	ПО АСУ ТП	Нарушение работы ПО
		Внедрение вредоносного ПО
		Утечка идентификационной и аутентификационной информации
		Несанкционированное изменение идентификационной и

Негативные последствия	Объекты воздействия	Виды воздействия
		аутентификационной информации
	Аппаратные средства АСУ ТП	Несанкционированное изменение программной и аппаратной конфигурации
Потеря данных, обрабатываемых АСУ ТП (У2)	Аппаратные средства АСУ ТП	Перезагрузка и/или выведение из строя средств вычислительной техники
	Каналы передачи данных	Выведение из строя каналов передачи данных
Остановка работы АСУ ТП (У3)	Аппаратные средства АСУ ТП	Перезагрузка и/или выведение из строя средств вычислительной техники

5. Источники угроз безопасности информации

Определение состава и источников угроз, актуальных для АСУ ТП:

Таблица 4. Состав и источники угроз

№ вида	Вид нарушителя	Категория нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
1	Отдельные физические лица (хакеры)	Внешний	<p>Идеологические или политические мотивы.</p> <p>Причинение имущественного ущерба путем мошенничества или иным преступным путем.</p> <p>Получение финансовой или иной материальной выгоды.</p> <p>Любопытство или желание самореализации (подтверждение статуса).</p> <p>Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды</p>
2	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана,	Внутренний	<p>Причинение имущественного ущерба путем обмана или злоупотребления доверием.</p> <p>Получение финансовой или иной</p>

№ вида	Вид нарушителя	Категория нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
	уборщики и т.д.)		материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
3	Авторизованные пользователи систем и сетей	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
4	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия
5	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия

Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации:

Таблица 5

Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	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)	+	+	У1, У2, У3
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	+	+	У2, У3
Авторизованные пользователи систем и сетей	+	+	У1, У2, У3
Бывшие работники (пользователи)	+	+	У1, У2, У3
Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	+	+	У2, У3

Таблица 6. Уровни возможностей нарушителей по реализации угроз безопасности

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н1	Нарушитель, обладающий базовыми возможностями	<p>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 программного обеспечения, эксплойтов.</p> <p>Обладает базовыми компьютерными знаниями и навыками на уровне пользователя.</p> <p>Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним.</p> <p>Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов</p>	<p>Физическое лицо (хакер)</p> <p>Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем</p> <p>Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.)</p> <p>Авторизованные пользователи систем и сетей</p> <p>Бывшие работники (пользователи)</p>

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н2	Нарушитель, обладающий базовыми повышенными возможностями	<p>Обладает всеми возможностями нарушителей с базовыми возможностями.</p> <p>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.</p> <p>Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей.</p> <p>Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации.</p> <p>Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.</p> <p>Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе</p>	<p>Преступные группы (два лица и более, действующие по единому плану)</p> <p>Конкурирующие организации</p> <p>Поставщики вычислительных услуг, услуг связи</p> <p>Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ</p> <p>Системные администраторы и администраторы безопасности</p>

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		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	
НЗ	Нарушитель, обладающий средними возможностями	<p>Обладает всеми возможностями нарушителей с базовыми повышенными возможностями.</p> <p>Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей).</p> <p>Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей).</p> <p>Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств.</p> <p>Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному</p>	<p>Террористические, экстремистские группировки</p> <p>Разработчики программных, программно-аппаратных средств</p>

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		<p>оборудованию и другим программно-аппаратным средствам для проведения их анализа.</p> <p>Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях.</p> <p>Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.</p> <p>Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц.</p> <p>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</p>	
Н4	Нарушитель, обладающий высокими возможностями	<p>Обладает всеми возможностями нарушителей со средними возможностями.</p> <p>Имеет возможность получения доступа к исходному коду</p>	Специальные службы иностранных государств

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		<p>встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня».</p> <p>Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств.</p> <p>Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение.</p> <p>Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности.</p> <p>Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.</p>	

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		<p>Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации.</p> <p>Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей.</p> <p>Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недеklarированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей</p>	

Определение актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности:

Таблица 7

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1: Некорректная работа АСУ ТП	Отдельные физические лица (хакеры)	Внешний	Н1
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Бывшие работники (пользователи)	Внешний	Н1
2	У2: Потеря данных, обрабатываемых АСУ ТП	Отдельные физические лица (хакеры)	Внешний	Н1
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Н1
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Бывшие работники (пользователи)	Внешний	Н1
		Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Н2
3	У3: Остановка работы АСУ ТП	Отдельные физические лица (хакеры)	Внешний	Н1
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Н1
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Бывшие работники (пользователи)	Внешний	Н1
		Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных	Внутренний	Н2

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
		и иных видов работ		

6. Способы реализации (возникновения) угроз безопасности информации

Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности:

Таблица 8

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Отдельные физические лица (хакеры) (Н1)	Внешний	ПО АСУ ТП	Локальная вычислительная сеть	Использование недеklarированных возможностей программного обеспечения телекоммуникационного оборудования
					Внедрение вредоносного ПО
				АРМ оператора АСУ ТП	Использование недеklarированных возможностей и ошибок конфигурации системы разграничения доступа
					Компрометация идентификационной и аутентификационной информации

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			Аппаратные средства АСУ ТП	Система контроля и управления доступом	Использование недеklarированных возможностей и ошибок конфигурации системы контроля и управления доступом
					Компрометация аутентификационной информации
			Каналы передачи данных	Локальная вычислительная сеть	Использование недеklarированных возможностей программного обеспечения телекоммуникационного оборудования
					Внедрение вредоносного ПО
2	Лица, обеспечивающие функционирование АСУ ТП или обслуживающие инфраструктуру владельца системы (администрация, охрана, уборщики и т.д.) (Н1)	Внутренний	Аппаратные средства АСУ ТП	Наличие доступа к нижнему и среднему уровню АСУ ТП	Непреднамеренные, неосторожные или неквалифицированные действия
					Умышленное выведение из строя элементов аппаратного состава АСУ ТП
			Каналы передачи данных	Наличие доступа к нижнему и среднему уровню АСУ ТП	Непреднамеренные, неосторожные или неквалифицированные действия
					Умышленное выведение из строя каналов передачи данных АСУ ТП
3	Авторизованные пользователи систем и сетей (Н1)	Внутренний	ПО АСУ ТП	Наличие доступа к ПО АСУ ТП	Непреднамеренные, неосторожные или неквалифицированные действия

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
					Умышленное выведение из строя ПО АСУ ТП
			Аппаратные средства АСУ ТП	Наличие доступа к нижнему и среднему уровню АСУ ТП	Непреднамеренные, неосторожные или неквалифицированные действия
					Умышленное выведение из строя элементов аппаратного состава АСУ ТП
			Каналы передачи данных	Наличие доступа к локальной вычислительной сети	Использование недекларированных возможностей программного обеспечения телекоммуникационного оборудования
					Внедрение вредоносного ПО
4	Бывшие работники (пользователи) (Н1)	Внешний	ПО АСУ ТП	Локальная вычислительная сеть	Использование недекларированных возможностей программного обеспечения телекоммуникационного оборудования
				АРМ оператора АСУ ТП	Внедрение вредоносного ПО
			Аппаратные средства АСУ ТП	Система контроля и управления доступом	Использование недекларированных возможностей и ошибок конфигурации системы контроля и управления доступом
					Компрометация аутентификационной информации

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
5	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ (Н2)	Внутренний	Каналы передачи данных	Локальная вычислительная сеть	Использование недеklarированных возможностей программного обеспечения телекоммуникационного оборудования
					Внедрение вредоносного ПО
			Аппаратные средства АСУ ТП	Наличие доступа к нижнему и среднему уровню АСУ ТП	Непреднамеренные, неосторожные или неквалифицированные действия
					Умышленное выведение из строя элементов аппаратного состава АСУ ТП
			Каналы передачи данных	Наличие доступа к нижнему и среднему уровню АСУ ТП	Непреднамеренные, неосторожные или неквалифицированные действия
					Умышленное выведение из строя каналов передачи данных АСУ ТП
			ПО АСУ ТП	Наличие доступа к ПО АСУ ТП	Непреднамеренные, неосторожные или неквалифицированные действия
					Внедрение вредоносного ПО

7. Описание угроз АСУ ТП

Оценка возможности реализации и подход к определению актуальности угроз безопасности информации в АСУ ТП.

Таблица 9

Уровень защищенности Потенциал нарушителя	Высокий	Средний	Низкий
Базовый (низкий)	Низкая	Средняя	Высокая
Средний	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

Так как уровень проектной защищенности АСУ ТП оценен, как низкий, а потенциал нарушителя как низкий, то возможность реализации угроз безопасности информации в АСУ ТП принимается, как высокая для всех угроз, которые характерны для АСУ ТП с учетом её структурных особенностей и применяемых технологий.

Решение об актуальности угрозы безопасности информации нарушающей целостность или доступность информации в АСУ ТП, принимается в соответствии со структурными особенностями, применяемыми технологиями и значениями из таблицы 4

Таблица 10

Возможность реализации угрозы	Степень возможного ущерба		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная

Степень возможного ущерба определяется экспертным методом в соответствии с таблицей 11

Таблица 11

Степень ущерба	Характеристика степени ущерба
Низкая	В результате нарушения одного из свойств безопасности информации (целостности, доступности) возможны незначительные негативные последствия. АСУ ТП может выполнять свои функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств
Средняя	В результате нарушения одного из свойств безопасности информации (целостности, доступности) возможны умеренные негативные последствия. АСУ ТП не могут выполнять хотя бы часть своих функций
Высокая	В результате нарушения одного из свойств безопасности

	информации (целостности, доступности) возможны существенные негативные последствия. АСУ ТП не может выполнять свои функции
--	---

Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности в соответствии с таблицей 12. В данной модели угроз учитываются только два свойства безопасности информации (доступность, целостность), так как требования по обеспечению конфиденциальности информации не предъявляется владельцем системы.

Таблица 12

Свойство безопасности информации	Результат реализации угрозы безопасности информации	
	Оказывает воздействие	Не оказывает воздействия
Целостность	В результате реализации угрозы безопасности информации возможно уничтожение или модифицирование информации	В результате реализации угрозы безопасности информации отсутствует возможность уничтожения или модифицирования информации
Доступность	В результате реализации угрозы безопасности информации возможно блокирование информации	В результате реализации угрозы безопасности информации отсутствует возможность блокирования информации

Определение угроз, характерных для АСУ ТП

В качестве потенциально опасных угроз безопасности информации (УБИ) АСУ ТП, рассматривались УБИ из банка данных угроз безопасности(<http://bdu.fstec.ru/threat>) нарушающие целостность и доступность информации в АСУ ТП и характерные для внешних нарушителей с базовым потенциалом.

Результаты анализа потенциально реализуемых угроз для уровня диспетчеризации

Результаты анализа потенциально реализуемых угроз для уровня диспетчеризации АСУ ТП Результаты анализа потенциально реализуемых угроз для уровня диспетчеризации (включающего АРМ операторов, серверы с общесистемным и прикладным ПО, телекоммуникационное оборудование, каналы связи) АСУ ТП приведены в таблице 13.

Таблица 13

Код	Название угрозы	Возможность реализации угрозы	Ущерб от реализации угрозы	Свойство информации, нарушаемое при реализации угрозы	Актуальные угрозы	Способ реализации угрозы	Примечание
УБИ.006	Угроза внедрения кода или данных	Высокая	Высокий	Целостность, доступность	Актуальна	НСД с использованием уязвимостей ПО	Реализацией данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Высокая	Низкий	Целостность, доступность	Актуальна	НСД с использованием уязвимостей ПО	Угроза не приведёт существенного влияния на АСУ ТП
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Высокая	Средний	Целостность, доступность	Актуальна	Угроза обусловлена слабостями мер контроля целостности	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.018	Угроза загрузки нештатной операционной	Высокая	Высокий	Целостность, доступность	Актуальна	НСД с использованием уязвимостей ПО,	Реализация данной угрозы приведёт к

	системы					а также недостатками организации работ по ОБИ в АСУ ТП от НСД	некорректной работе АСУ ТП
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Высокая	Средний	Целостность, доступность	Актуальна	НСД с использованием уязвимостей, вызванными недостатками организации работ по ОБИ в АСУ ТП от НСД	Реализация данной угрозы не приведёт к существенным изменениям, однако может послужить уязвимостью для других угроз
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Высокая	Средний	Целостность, доступность	Актуальна	НСД с использованием уязвимостей, вызванными недостатками организации работ по ОБИ в АСУ ТП от НСД	Реализация угрозы не приведёт к существенным изменениям, однако может послужить уязвимостью для других угроз
УБИ.034	Угроза	Высокая	Высокий	Целостность,	Актуальна	НСД с	Реализация

	использования слабостей протоколов сетевого/локального обмена данными			доступность		использованием уязвимостей данных протоколов	данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.041	Угроза межсайтового скриптинга	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Высокая	Высокий	Целостность, доступность	Актуальна	НСД с использованием уязвимостей ПО	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.049	Угроза нарушения целостности кеша	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП

	несовместимости аппаратного и программного обеспечения						
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Высокая	Высокий	Целостность, доступность	Актуально	НСД с использованием уязвимостей, вызванными недостатками организации работ по ОБИ в АСУ ТП от НСД	Реализация данной меры приведёт к некорректному функционированию АСУ ТП
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.055	Угроза незащищённого администрирования облачных услуг	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.060	Угроза неконтролируемого уничтожения	Отсутствует			Неактуальна		Данная технология не применяется в

	информации хранилищем больших данных						АСУ ТП
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Высокая	Высокий	Целостность, доступность	Актуальна	НСД с использованием уязвимостей ПО, вызванных недостатками организации работ ОБИ в АСУ ТП от НСД	Реализуемая мера не приведёт к существенным изменениям, однако может послужить уязвимостью для других угроз
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП

УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Высокая	Высокий	Целостность, доступность	Актуальна	НСД с использованием уязвимостей беспроводных соединений	Реализация угрозы приведёт к потерям передаваемых сигналов
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Высокая	Средний	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей, вызванных недостатками организации работ по ОБИ в АСУ ТП от НСД, НСД с использованием уязвимостей ПО	Реализация угрозы не приведёт существенным последствиям, однако восстановление аутентификационной информации может потребовать

							существенных трудо­затрат
УБИ.089	Угроза несанкционированно­го редактирования реестра	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с возможностью внесения в реестр ОС	Реализация угрозы приведёт к некорректной работе ОС
УБИ.090	Угроза несанкционированно­го создания учётной записи пользователя	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.093	Угроза несанкционированно­го управления буфером	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей ПО	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей, вызванных недостатками организации работ по ОБИ в АСУ ТП от НСД	Реализация данной угрозы приведёт к некорректной работе АСУ ТП

УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Отсутствует			Неактуальна		Данная угрозы не применяется в АСУ ТП
УБИ.107	Угроза отключения контрольных датчиков	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза заключается в возможности обеспечения нарушителем информационной изоляции системы безопасности путём прерывания канала связи с контрольными датчиками	Реализация данной угрозы приведёт к неисправности работы АСУ ТП и переход на ручное управление до устранения всех проблем
УБИ.108	Угроза ошибки обновления гипервизора	Отсутствует			Неактуальна		Данная угрозы не применяется в АСУ ТП
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей вызванных сбоями и отказами программных и	Реализация данной угрозы приведёт к некорректной работе АСУ ТП

						аппаратных средств	
УБИ.121	Угроза повреждения системного реестра	Высокая	Высокий	Целостность, доступность	Актуальна	Возникновение ошибок в работе отдельных процессов или всей ОС	Реализация данной угрозы может привести к некорректной работе АСУ ТП
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.152	Угроза удаления аутентификационной	Высокая	Средний	Целостность, доступность	Актуальна	Угроза НСД с использованием	Угроза не оказывает

	информации					уязвимостей, вызванных недостатками организации работ по ОБИ в АСУ ТП от НСД	существенного воздействия на АСУ ТП
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза заключается в умышленном выведении из строя средств вычислительной техники	Угроза может привести к некорректному функционированию АСУ ТП
УБИ.158	Угроза форматирования носителей информации	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей, вызванных недостатками организации работ по ОБИ в АСУ ТП от НСД	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей ПО	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП

	облачной инфраструктуре						
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.172	Угроза распространения «почтовых червей»	Отсутствует			Неактуальна		Данная технология не применяется в АСУ ТП
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Отсутствует			Неактуальна		Системой диспетчеризации АСУ ТП осуществляется проверка вводимых данных, что исключает ввод некорректных или не подтверждённых данных
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей межсетевого взаимодействия	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.185	Угроза несанкционированно	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием	Реализация данной угрозы

	го изменения параметров настройки средств защиты информации					уязвимостей, вызванных недостатками организации работ по ОБИ в АСУ ТП от НСД	приведёт к некорректной работе АСУ ТП
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Отсутствует			Неактуальна		Данная угроза не применяется в АСУ ТП
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей ПО	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей ПО	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей ПО	Реализация данной угрозы приведёт к некорректной работе АСУ ТП

УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Высокая	Высокий	Целостность, доступность	Актуальна	Угроза НСД с использованием уязвимостей ПО	Реализация данной угрозы приведёт к некорректной работе АСУ ТП
---------	---	---------	---------	--------------------------	-----------	--	--