

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность систем
и технологий»

Специальность 10.05.03 —

Специализация — 6

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

АТТЕСТАЦИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА БАЗЕ
СЕРВЕРНОГО ПАРКА КОРПОРАТИВНОЙ СЕТИ АО «ФНПЦ «ПО «СТАРТ»
ИМ. М.В. ПРОЦЕНКО»

Студент

Носова Анастасия Андреевна

Руководитель

Мартынов Александр Евгеньевич

Нормоконтролёр

Фатеев Алексей Григорьевич

Рецензент инженер по защите

Шпагин Денис Юрьевич

информации АО «ФНПЦ «ПО

«Старт» им. М.В. Проценко»

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой

Зефиоров Сергей Львович

Работа защищена с отметкой

хорошо

(протокол заседания

ГЭК от 26.06.20 № 14)

Секретарь ГЭК

Иванов Алексей Петрович

Пенза 2020

Оглавление

Введение.....	5
1 Предпроектная стадия	8
1.1 Описание предпроектной стадии	8
1.2 Описание структуры автоматизированной системы на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В.Проценко» в текущем состоянии.....	8
1.3 Создание экспертной комиссии	14
1.4 Разработка модели угроз безопасности информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»	15
1.5 Классификация АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»	94
1.6 Определение требований к системе защиты АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко».....	95
2 Стадия проектирования	111
2.1 Описание стадии проектирования.....	111
2.2 Создание проекта системы защиты информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»	112
3 Стадия реализации	114
3.1 Описание стадии реализации.....	114
3.2 Инструкция системному администратору АС.....	114
3.3 Инструкция пользователю АС.....	115
3.4 Инструкция администратору безопасности АС.....	116
3.5 Инструкция по антивирусному контролю в АС.....	117
3.6 Разрешительная система доступа АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».....	118
3.7 Разработка технического паспорта АС.....	118

4 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	122
Заключение	124
Список использованных источников.....	126
Приложение А. Приказ о создании экспертной комиссии.....	128
Приложение Б. Акт экспертизы информации.....	130
Приложение В. Акт определения уровня защищенности АС.....	133
Приложение Г. Модель угроз безопасности информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко».....	137
Приложение Д. Акт классификации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»	212
Приложение Е. Техническое задание на разработку системы защиты информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко».....	215
Приложение Ж. Технический проект на создание системы защиты информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко».....	234
Приложение И. Разрешительная система доступа к ресурсам АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»	263
Приложение К. Инструкция системному администратору.....	266
Приложение Л. Инструкция пользователю АС	276
Приложение М. Инструкция администратору безопасности АС.....	284
Приложение Н. Журнал учета работ в АС	292
Приложение П. Инструкция по использованию средств антивирусной защиты.....	294
Приложение Р. Технический паспорт АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко».....	301
Приложение С. Приказ о назначении администраторов безопасности и	

системных администраторов АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко».....	310
Приложение Т. Протокол проверки на оригинальность.....	312

Введение

Характерной чертой современного общества является его информатизация – активная разработка и внедрение во все сферы человеческой деятельности информационных технологий и средств. Информация и информационные ресурсы становятся одним из решающих факторов развития личности, общества и государства. Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам, участвующим в процессах автоматизированного информационного взаимодействия, что угрожает безопасности организации.

Жизненно важные интересы организаций, как правило, заключаются в том, чтобы определенная часть информации, например, коммерческая информация или ПДн, была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования, блокирования или уничтожения.

В современных условиях наиболее перспективным способом проверки достигнутого качества функционирования и уровня защищенности автоматизированных систем является процедура аттестации по требованиям безопасности информации.

Цель выпускной квалификационной работы – подготовка автоматизированной системы на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» к аттестации по требованиям безопасности информации.

Исходя из того, что предприятие входит в состав ГосКорпорации «Росатом», то оно должно руководствоваться не только общеизвестными документами в области защиты информации, но ещё и внутренними Едиными

отраслевыми методическими указаниями по информационной безопасности, которые предполагают разбиение процедуры аттестации на несколько этапов:

- предпроектная стадия, включающая предпроектное обследование автоматизированной системы (далее – АС), разработку технического (частного технического) задания на создание системы защиты информации;

- стадия проектирования (разработки проектов), включающая разработку системы защиты информации;

- стадия реализации, включающая разработку опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию АС на соответствие требованиям по безопасности информации.

На основе этого, на каждой стадии необходимо разработать соответствующие технические документы.

На предпроектной стадии:

- приказ о создании экспертной комиссии;
- акт экспертизы информации;
- модель угроз безопасности;
- акт определения защищенности АС;
- акт классификации АС;
- техническое задание.

Стадия проектирования включает в себя разработку технического проекта.

На стадии реализации должны быть разработаны:

- разрешительная система доступа к ресурсам АС;
- инструкция пользователю АС;
- инструкция системному администратору АС;
- инструкция администратору безопасности АС;

- инструкция по антивирусному контролю в АС;
- журнал учета работ в АС;
- технический паспорт АС;
- приказ о назначении администраторов безопасности и системных администраторов АС.

1 Предпроектная стадия

1.1 Описание предпроектной стадии

При необходимости аттестации автоматизированной системы на базе серверного парка корпоративной сети (КС) АО «ФНПЦ «ПО «Старт» им. М.В.Проценко» (далее – АС) по требованиям безопасности информации, необходимо на предпроектной стадии определить какая информация обрабатывается на АС. Для этого назначается экспертная комиссия, которая определяет наличие сведений ограниченного доступа в информации. По результатам проведения экспертизы информации, оформляется «Акт экспертизы информации». Также на этой стадии определяются угрозы безопасности информации, разрабатывается модель угроз, включающая в себя, в том числе, модель нарушителя информации. В целях разработки и применения обоснованных и эффективных мер защиты информации с учетом конфиденциальности информации – проводится классификация АС. После чего по результатам предпроектного обследования на основании действующих нормативных документов по защите информации, с учетом результатов классификации АС задаются конкретные требования к системе защиты информации, включаемые в техническое (частное техническое) задание на разработку системы защиты информации.

1.2 Описание структуры автоматизированной системы на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В.Проценко» в текущем состоянии

Целью автоматизированной системы на базе серверного парка корпоративной сети (КС) АО «ФНПЦ «ПО «Старт» им. М.В.Проценко» (далее – АС) является - обработка, хранение и передача по каналам связи информации степени конфиденциальности – для служебного пользования,

коммерческая тайна, персональные данные, а также несекретной информации

Функциями, реализация которых позволит АС добиться поставленной цели, являются:

- предотвращение НСД, уничтожения, искажения, копирования, блокирования защищаемой информации;
- резервирование элементов системы;
- регулирование доступа к элементам системы и защищаемой информации;
- защита от информационного воздействия на технические средства обработки;
- обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности;
- фиксация всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем обработки информации, относящихся к защите информации;
- предотвращение утечки и утраты информации;
- сохранение конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Объектами защиты являются:

- защищаемая информация (для служебного пользования, персональные данные, коммерческая тайна);
- технологическая информация:
 - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
 - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

- информация на съемных носителях информации (съемные жесткие магнитные диски), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации;
- программно-технические средства обработки:
 - общесистемное и специальное программное обеспечение (операционные системы и другие);
 - резервные копии общесистемного программного обеспечения;
 - инструментальные средства и утилиты систем управления ресурсами АС;
 - аппаратные средства обработки информации;
- средства защиты информации:
 - средства управления и разграничения доступа пользователей;
 - средства обеспечения регистрации и учета действий с информацией;
 - средства, обеспечивающие целостность данных;
 - средства антивирусной защиты;
- объекты и помещения, в которых размещены компоненты АС.

Перечень оборудования, серверов представлены в таблице 1 и 2, соответственно.

Таблица 1 — Перечень оборудования

№ п/п	Оборудование	Примечание
1	СХД резервного копирования StoreOnce (HP Storeonce 4500)	Система хранения данных для резервного копирования
2	СХД 3PAR 7200(HP StoreServ 7200 (M6710/7000 Encl))	Система хранения данных
3	AltellNeo Master	МЭ
4	ME5200	Маршрутизатор
5	Blade-система HP c7000	Блейд-система

Таблица 2 — Перечень серверов

№ п/п	Кластер	Сервер	ОС
1	Кластер сервисов серверного парка КС Yanux 4	node01-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node02-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node03-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node04-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node05-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node06-cl(HPE ProLiant DL380 Gen10)	Yanux 4
2	Кластер сервисов серверного парка КС AstraLinux(Blade-система HP c7000)	bnode01(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode02(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode03(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode04(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode05(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode06(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6

Продолжение таблицы 2

№ п/п	Кластер	Сервер	ОС
2		bnode08(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
3	Кластер БД	db-node01(HPE ProLiant DL380 Gen10)	AstrLinux Smolensk 1.6
		db-node02(HPE ProLiant DL380 Gen10)	AstrLinux Smolensk 1.6
4	Сервера Ascon	HPE ProLiant DL380 Gen10	Windows Сервер 2008

Перечень ИТ-сервисов приведен в таблице 3.

Таблица 3 – Перечень ИТ-сервисов

Кластер	Сервис	Назначение
Кластер сервисов серверного парка КС Unix 4	backup_server	Сервис резервного копирования
	conference	Сервис видеоконференций
	dhcp_server	DHCP-сервер
	dns	DNS-сервер
	fs	Файловый сервис
	intuit	Система дистанционного обучения
	mail	Почтовый сервер
	nagios	Сервис мониторинга
	otrs	Система обработки заявок
	replica	Сервис перекачки данных
	sites	Корпоративные сайты
	spd	Сервис подготовки данных
	tomcat	Сервис формирования pdf
	ad1	Контроллер домена
	ad2	Контроллер домена
	alfresco	Электронный документооборот
	backup	Сервис резервного копирования
	ca	Удостоверяющий центр
	cmdb	Система инвентаризации
	consultant	Информационно-правовая система Консультант
	dns	DNS-сервер

Продолжение таблицы 3

Кластер	Сервис	Назначение
	dtc	Сервер разработки
	fa	Файловый сервис
	homes	Сервер пользовательских данных
	jabber	Сервер обмена сообщений
	ksu	Корпоративная система управления
	ldap	Ldap сервер
	pgsqlddb	Сервер БД разработки задач КСУ
	pgsqldts	Сервер приложений
	redmine	Система управления проектами
	sites	Корпоративные сайты
	svn	Система контроля версий
	tally	Сервис печати
Кластер сервисов серверного парка КС AstraLinux	gitlab	Система управления репозиториями кода
	Maildsp	Почтовый сервер ДСП
	pgsqldb	Сервер БД
	pgsqldev	Сервер приложений для разработки задач КСУ
Сервера ASCON на ОС Windows Сервер 2008	AsconAS5	Аскон
	TFLEXAS	T-Flex DOCs

Структура автоматизированной системы показана на рисунке 1. Все технические средства расположены в пределах КЗ.

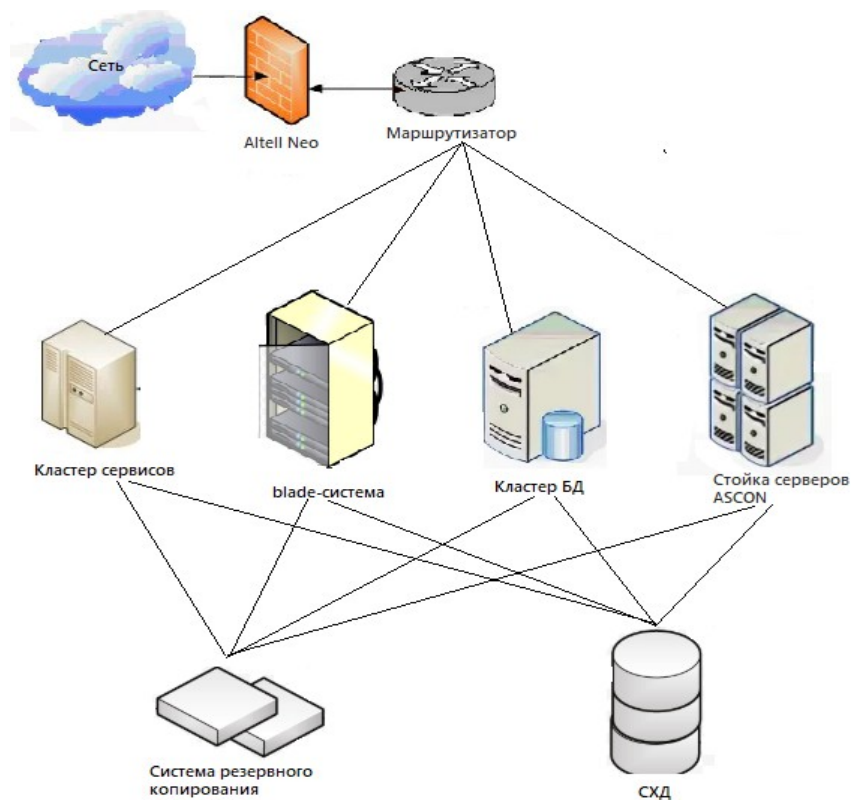


Рисунок 1 — Структура АС

1.3 Создание экспертной комиссии

На первом этапе создается экспертная комиссия для проведения экспертизы информации, предполагаемой к обработке в автоматизированной системе. Экспертная комиссия определяет наличие сведений ограниченного доступа в информации. Экспертная комиссия создается актом который представлен в приложении А.

По результатам проведения экспертизы информации, предполагаемой к обработке в АС, оформляется «Акт экспертизы информации» который приведен в приложении Б.

1.4 Разработка модели угроз безопасности информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

1.4.1 Идентификация источников угроз безопасности.

В качестве источников угроз БИ могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

Источники угроз безопасности информации могут быть следующих типов:

- антропогенные источники (антропогенные угрозы);
- техногенные источники (техногенные угрозы);
- стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В качестве источников антропогенных угроз безопасности информации могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в АС, или нарушения функционирования АС или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);
- лица, имеющие доступ к АС, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации). [1]

1.4.2 Модель нарушителя.

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в АС с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале

этих нарушителей и возможных способах реализации угроз безопасности информации. [1] Результаты оценки возможностей нарушителей отражены в модели нарушителя, которая приведена в таблице 4.

Таблица 4 — Модель нарушителя

№ п/п	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности
1	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
2	Лица, обеспечивающие функционирование АС или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
3	Пользователи АС	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Непреднамеренные, неосторожные или неквалифицированные действия.
4	Администраторы АС и администраторы БД	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.

Был определен потенциал нарушителя, требуемого для реализации угроз безопасности информации. Потенциал нарушителя и их возможности представлены в таблице 5.

Таблица 5 — Потенциалы и возможности нарушителей

№ п/п	Потенциал	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	Лица, обеспечивающие функционирование АС или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики). Пользователи АС. Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ.	Имеют возможность получить информацию об уязвимостях отдельных компонент АС, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации, опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на АС.
2	Нарушители с базовым повышенным (средним) потенциалом	Администраторы АС и администраторы БД.	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах ЗИ, применяемых в ИС данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент АС путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных компонент общесистемного ПО. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования АС.

1.4.3 Описание угроз безопасности информации.

Безопасность конфиденциальной информации при их обработке в информационной системе обеспечивается с помощью системы защиты информации, нейтрализующей актуальные угрозы.

Под угрозами безопасности информации при их обработке в АС понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на неё.[2]

Система защиты информации включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности

информации и информационных технологий, используемых в информационных системах.

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на АС и её элементы объективных физических процессов или стихийных природных явлений, независимых от человека.

Искусственные угрозы – это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АС и её элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
- преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).[3]

Для данного объекта информатизации реально существуют угрозы безопасности информации при обеспечении ее конфиденциальности, доступности, целостности.

1.4.4 Оценка вероятности реализации угроз безопасности информации АС.

Для оценки возможности реализации угрозы были рассчитаны два показателя: уровень исходной защищенности АС и частота (вероятность) реализации рассматриваемой угрозы. Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик.[2] Приказ об утверждении результатов определения уровня защищенности АС, приведен в приложении В.

Определение уровней исходной защищенности АС представлен в таблице 6.

Таблица 6 — Показатель исходной защищенности АС

Технические и эксплуатационные характеристики АС	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: локальная АС, развёрнутая в пределах одного здания	-	+	-
2. По наличию соединения с сетями общего пользования: АС, физически отделённая от сети общего пользования;	+	-	-
3. По встроенным (легальным) операциям с записями баз данных: запись, удаление, сортировка;	-	+	-
4. По разграничению доступа к защищаемой информации: АС, к которой имеют доступ определённые перечнем сотрудники организации, являющейся владельцем АС;	-	+	-
5. По наличию соединений с другими базами АС: АС, в которой используется одна база данных, принадлежащая организации – владельцу данной АС;	+	-	-
6. По уровню обобщения (обезличивания) информации: АС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	-	+
7. По объёму информации, которые предоставляются сторонним пользователям без предварительной обработки: АС, не предоставляющая никакой информации.	-	+	-

Исходная степень защищенности определяется следующим образом.

— АС имеет высокий уровень исходной защищенности, если не менее 70% характеристик АС соответствует уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – по среднему уровню защищенности (положительные решения по второму столбцу);

— АС имеет средний уровень исходной защищенности, если не

выполняются условия по пункту 1 и не менее 70% характеристик АС соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – к низкому уровню защищенности;

— АС имеет низкую степень защищенности, если не выполняются условия по пунктам 1 и 2.

Следовательно, АС АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», имеет средний уровень исходной защищенности.

1.4.5 Определение актуальности угроз безопасности информации.

При составлении перечня актуальных угроз безопасности информации, каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1 , а именно:

- 0 для высокой степени исходной защищенности;
- 5 для средней степени исходной защищенности;
- 10 для низкой степени исходной защищенности.

Числовой коэффициент уровня исходной защищенности АС Y_1 равно 5.

Была определена частота (вероятность) реализации угрозы экспертным путем. Для этого были введены четыре вербальных градации этого показателя:

— маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

— низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

— средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;

— высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты.

При составлении перечня актуальных угроз безопасности каждой градации вероятности возникновения угрозы был поставлен в соответствие числовой коэффициент Y_2 , а именно:

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

Коэффициент реализуемости угрозы Y был определён соотношением :

$$Y = (Y_1 + Y_2) / 20 \quad (1)$$

Исходя из коэффициента реализуемости угрозы Y была сформирована вербальная интерпретация реализуемости угрозы следующим образом:

- если Y больше 0, но меньше 0,3, то возможность реализации угрозы признается низкой;
- если Y больше 0,3, но меньше 0,6, то возможность реализации угрозы признается средней;
- если Y больше 0,6, но меньше 0,8, то возможность реализации угрозы признается высокой;
- если Y больше 0,8, то возможность реализации угрозы признается очень высокой.

Далее была оценена опасность каждой угрозы. При оценке опасности определялся вербальный показатель опасности для АС из следующих значений:

- незначительные негативные последствия (показатель опасности – низкий) – последствия для субъекта малоощутимы (незначительный

финансовый или моральный ущерб, при этом репутация субъекта, его материальное благополучие, жизнь и здоровье не затронуты);

— негативные последствия (показатель опасности – средний) – последствия приводят к ощутимым по объёму или значению финансовым и (или) моральным и (или) репутационным потерям. Основные интересы и права личности, закреплённые Конституцией РФ, не затронуты;

— значительные негативные последствия (показатель опасности – высокий) – последствия приводят к критическим финансовым, моральным, репутационным потерям для субъекта, вплоть до потери средств к существованию, здоровья, жизни.

Затем был осуществлён выбор из предварительного перечня угроз безопасности тех угроз, которые являются актуальными для АС, в соответствии с критериями, заданными в таблице 7.

Таблица 7 — Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высока
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высока	Актуальная	Актуальная	Актуальная

Результаты определения актуальности угроз представлены в таблице 8.

Разработанная модель угроз безопасности АС представлена в приложении Г.

Таблица 8— Актуальность угроз для АС

УБИ	Число-вой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
		Вероятность (частота) реализации угрозы	Обоснование	Вероятность возникновения угрозы Y2				
Угроза автоматического распространения вредоносного кода в грид-системе УБИ.001								Данная угроза не применяется к рассматриваемой АС
Угроза агрегирования данных, передаваемых в грид-системе УБИ.002								Данная угроза не применяется к рассматриваемой АС
Угроза анализа криптографических алгоритмов и их реализации УБИ. 003	5	маловероятно	На АС отсутствует криптографическое ПО. Отсутствие у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	0	0,25	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза аппаратного сброса пароля BIOS УБИ. 004	5	малове- роятно	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	0	0,25	Низкая	Низкая	Неактуальная
Угроза внедрения вредоносного кода в BIOS УБИ. 005	5	малове- роятно	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	0	0,25	Низкая	Низкая	Неактуальная
Угроза внедрения кода или данных УБИ.006	5	малове- роятно	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	0	0,25	Низкая	Низкая	Неактуальная
Угроза воздействия на программы с высокими привилегиями УБИ. 007	5	малове- роятно	Отсутствие административных привилегий у пользователя Наличие доверенного канала связи посредством СКЗИ. Использование на АП базового проверенного набора ПО.	0	0,25	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фицие нт исход- ной защит енност и (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опаснос- ти угрозы	Актуальность угрозы
Угроза восстановления аутентификационной информации УБИ. 008	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
Угроза восстановления предыдущей уязвимой версии BIOS УБИ. 009	5	низкая	На АС установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
Угроза выхода процесса за пределы виртуальной машины УБИ.010								Данная угроза не применяется к рассматриваемой АС
Угроза деавторизации санкционированного клиента беспроводной сети УБИ.011								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза деструктивного изменения конфигурации/среды окружения программ УБИ.012	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза деструктивного использования декларированного функционала BIOS УБИ.013	5	низкая	На АС установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
Угроза длительного удержания вычислительных ресурсов пользователями УБИ.014	5	низкая	Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
Угроза доступа к защищаемым файлам с использованием обходного пути УБИ.015	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза доступа к локальным файлам сервера при помощи URL УБИ.016	5	малове- роятно	Отсутствие у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	0	0,25	Низкая	Низкая	Неактуальная
Угроза доступа/перехвата/изменения HTTP cookies УБИ.017	5	низкая	Отсутствие у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	2	0,35	Низкая	Низкая	Неактуальная
Угроза загрузки нештатной операционной системы УБИ.018	5	низкая	Возможность подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы.	2	0,35	Низкая	Низкая	Неактуальная
Угроза заражения DNS-кеша УБИ.019	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг УБИ.20								Данная угроза не применяется к рассматриваемой АС
Угроза злоупотребления доверием потребителей облачных услуг УБИ.21								Данная угроза не применяется к рассматриваемой АС
Угроза избыточного выделения оперативной памяти УБИ.022	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АС базового проверенного набора ПО. Возможность выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза изменения компонентов информационной (автоматизированной) системы УБИ.023	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза изменения режимов работы аппаратных элементов компьютера УБИ.024	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза изменения системных и глобальных переменных УБИ.025	5	низкая	Отсутствие возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициен т исход- ной защище нности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальнос- ть угрозы
Угроза искажения XML-схемы УБИ.026	5	средняя	Возможность изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером.	5	0,5	Средняя	Средняя	Актуальная
Угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027	5	средняя	Возможность дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза использования альтернативных путей доступа к ресурсам УБИ.028	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса).	5	0,5	Средняя	Средняя	Актуальная
Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами УБИ.029								Данная угроза не применяется к рассматриваемой АС
Угроза использования информации идентификации/ аутентификации, заданной по умолчанию УБИ.030	5	средняя	Наличие у нарушителя сведений о производителе/модели объекта защиты (ОЗ) и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для ОЗ;	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза использования механизмов авторизации для повышения привилегий УБИ.031	5	низкая	Отсутствие административных привилегий у пользователя.	5	0,25	Низкая	Низкая	Неактуальная
Угроза использования поддельных цифровых подписей BIOS УБИ.032	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
Угроза использования слабостей кодирования входных данных УБИ.033	5	средняя	Возможность осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.).	2	0,35	Средняя	Средняя	Актуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы Y=(Y1+Y2) /20	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034	5	средняя	Возможность осуществления нарушения несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Наличие доверенного канала связи посредством СКЗИ	5	0,5	Средняя	Средняя	Актуальная
Угроза использования слабых криптографических алгоритмов BIOS УБИ.035	5	низкая	Сложность использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI.	2	0,35	Низкая	Низкая	Неактуальная
Угроза исследования механизмов работы программы УБИ.036	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза исследования приложения через отчёты об ошибках УБИ.037	5	низкая	Отсутствие у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	2	0,35	Низкая	Низкая	Неактуальная
Угроза истощения вычислительных ресурсов хранилища больших данных УБИ.038								Данная угроза не применяется к рассматриваемой АС
Угроза истощения запаса ключей, необходимых для обновления BIOS УБИ.039	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя	2	0,35	Низкая	Низкая	Неактуальная
Угроза конфликта юрисдикций различных стран УБИ.40								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализации угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализации угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза межсайтового скриптинга УБИ.041								Данная угроза не применяется к рассматриваемой АС
Угроза межсайтовой подделки запроса УБИ.042								
Угроза нарушения доступности облачного сервера УБИ.043								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины УБИ.044								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения изоляции среды исполнения BIOS УБИ.045	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия УБИ.046								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке УБИ.047								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин УБИ.048								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения целостности данных кеша УБИ.049	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза неверного определения формата входных данных, поступающих в хранилище больших данных УБИ.050								Данная угроза не применяется к рассматриваемой АС
Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания УБИ.051	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения УБИ.052								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза невозможности управления правами пользователей BIOS УБИ.053	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
Угроза недобросовестного исполнения обязательств поставщиками облачных услуг УБИ.054								Данная угроза не применяется к рассматриваемой АС
Угроза незащищённого администрирования облачных услуг УБИ.055								Данная угроза не применяется к рассматриваемой АС
Угроза некачественного переноса инфраструктуры в облако УБИ.056								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза неконтролируемого копирования данных внутри хранилища больших данных УБИ.057								Данная угроза не применяется к рассматриваемой АС
Угроза неконтролируемого роста числа виртуальных машин УБИ.058								Данная угроза не применяется к рассматриваемой АС
Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.059								Данная угроза не применяется к рассматриваемой АС
Угроза неконтролируемого уничтожения информации хранилищем больших данных УБИ.060								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза некорректного задания структуры данных транзакции УБИ.061	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера УБИ.062								Данная угроза не применяется к рассматриваемой АС
Угроза некорректного использования функционала программного и аппаратного обеспечения УБИ.063	5	средняя	возможность использования декларированных возможностей программных и аппаратных средств определенным (нестандартным, некорректным) способом с целью деструктивного воздействия на автоматизированную систему и обрабатываемую ею информацию.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза неопределённости в распределении ответственности между ролями в облаке УБИ.065								Данная угроза не применяется к рассматриваемой АС
Угроза неопределённости ответственности за обеспечение безопасности облака УБИ.066								Данная угроза не применяется к рассматриваемой АС
Угроза неправомерного ознакомления с защищаемой информацией УБИ.067	5	низкая	Возможность неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами деструктивных целей.	2	0,35	Низкая	Низкая	Неактуальная
Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.068	5	низкая		5	0,5	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэф- фициент исходной защищенн ости (Y1)	Частота (вероятность) реализации угрозы			Кoeffи- циент реализуе- мости угрозы Y=(Y1+Y2) /20	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза неправомерных действий в каналах связи УБИ.069	5	низкая	Возможность несанкционированного доступа к сетевому трафику у нарушителя	5	0,25	Низкая	Низкая	Неактуальная
Угроза непрерывной модернизации облачной инфраструктуры УБИ.070								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071	5	средняя	Удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных; Технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных;	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS УБИ.072	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2 0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети УБИ.073							Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к аутентификационной информации УБИ.074	5	средняя	Возможность извлечения паролей, имён пользователей или других учётных данных из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации	2 0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к виртуальным каналам передачи УБИ.075								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети УБИ.076								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение УБИ.077								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети УБИ.078								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин УБИ.079								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети УБИ.080								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы УБИ.081								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к сегментам вычислительного поля УБИ.082								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к системе по беспроводным каналам УБИ.083								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети УБИ.084								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации УБИ.085								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного изменения аутентификационной информации УБИ.086	5	средняя	Возможность осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств.	2	0,5	Средняя	Средняя	Актуальная
Угроза несанкционированного использования привилегированных функций BIOS УБИ.087	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного копирования защищаемой информации УБИ.088	5	средняя	Возможность неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы).	5	0,5	Средняя	Средняя	Актуальная
Угроза несанкционированного редактирования реестра УБИ.089	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализации угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности и угрозы	Актуальность угрозы
Угроза несанкционированного создания учётной записи пользователя УБИ.090	5	низкая	Отсутствие прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного удаления защищаемой информации УБИ.091	5	низкая	Использование на АС базового проверенного набора ПО. Контроль со стороны ответственных за эксплуатацию ТС АС. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам УБИ.092								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного управления буфером УБИ.093	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного управления синхронизацией и состоянием УБИ.094	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации. Возможность изменения нарушителем последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состояния ИС, или в возможности модификации настроек и изменения режимов работы промышленных роботов, приводящих к вмешательству в производственный процесс и хищению хранящейся в памяти роботов информации (исходного кода, параметров продукции и др.).	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза несанкционированного управления указателями УБИ.095	5	низкая	Предоставление прав доступа к информационным ресурсам информационной системы по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несогласованности политик безопасности элементов облачной инфраструктуры УБИ.096								Данная угроза не применяется к рассматри- ваемой АС
Угроза несогласованности правил доступа к большим данным УБИ.097	5	низкая	Использования политик безопасности, согласованных между собой.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098	5	низкая	Возможность определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза обнаружения хостов УБИ.099	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика. Сканирование нарушителем вычислительной сети для выявления работающих сетевых узлов.	2	0,35	Низкая	Низкая	Неактуальная
Угроза обхода некорректно настроенных механизмов аутентификации УБИ.100	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации.	2	0,35	Низкая	Низкая	Неактуальная
Угроза общедоступности облачной инфраструктуры УБИ.101								Данная угроза не применяется к рассматриваемой АС
Угроза опосредованного управления группой программ через совместно используемые данные УБИ.102	5	низкая	Возможность опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные и др.)	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза определения типов объектов защиты УБИ.103	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика.	2	0,35	Низкая	Низкая	Неактуальная
Угроза определения топологии вычислительной сети УБИ.104	5	низкая	Наличие доверенного канала связи посредством СКЗИ Возможность определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз.	2	0,35	Низкая	Низкая	Неактуальная
Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных УБИ.105								Данная угроза не применяется к рассматриваемой АС
Угроза отказа в обслуживании системой хранения данных супер-компьютера УБИ.106								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза отключения контрольных датчиков УБИ.107								Данная угроза не применяется к рассматриваемой АС
Угроза ошибки обновления гипервизора УБИ.108								Данная угроза не применяется к рассматриваемой АС
Угроза перебора всех настроек и параметров приложения УБИ.109	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность получения нарушителем доступа к дополнительному скрытому функционалу или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перегрузки грид-системы вычислительными заданиями УБИ.110								Данная угроза не применяется к рассматриваемой АС
Угроза передачи данных по скрытым каналам УБИ.111								Данная угроза не применяется к рассматриваемой АС
Угроза передачи запрещённых команд на оборудование с числовым программным управлением УБИ.112								Данная угроза не применяется к рассматриваемой АС
Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники УБИ.113	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности и угрозы	Актуальность угрозы
Угроза переполнения целочисленных переменных УБИ.114	5	низкая	Отсутствие у внешнего нарушителя сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных. Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата вводимой и выводимой на периферийные устройства информации УБИ.115	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Отсутствие у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата данных, передаваемых по вычислительной сети УБИ.116	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности и угрозы	Актуальность угрозы
Угроза перехвата привилегированного потока УБИ.117	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата привилегированного процесса УБИ.118	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата управления гипервизором УБИ.119								Технология не применяется в данной АС
Угроза перехвата управления средой виртуализации УБИ.120								Технология не применяется в данной АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза повреждения системного реестра УБИ.121	5	низкая	Возникновение ошибок в работе отдельных процессов или всей операционной системы. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2 0,35	Низкая	Низкая	Неактуальная
Угроза повышения привилегий УБИ.122	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2 0,35	Низкая	Низкая	Неактуальная
Угроза подбора пароля BIOS УБИ.123	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2 0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы Y=(Y1+Y2) /20	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза подделки записей журнала регистрации событий УБИ.124	5	низкая	Технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза подключения к беспроводной сети в обход процедуры аутентификации УБИ.125								Данная угроза не применяется к рассматри- ваемой АС
Угроза подмены беспроводного клиента или точки доступа УБИ.126								Данная угроза не применяется к рассматри- ваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализации угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза подмены действия пользователя путём обмана УБИ.127	5	низкая	Применение методов борьбы с социальной инженерией. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза подмены доверенного пользователя УБИ.128	5	низкая	Возможность нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная
Угроза подмены резервной копии программного обеспечения BIOS УБИ.129	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Отсутствие возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии ПО BIOS/UEFI, предварительно подменённой нарушителем.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербаль-ная интерпретация реализуемости угрозы	Вербаль-ный показатель опасности и угрозы	Актуальность угрозы
Угроза подмены содержимого сетевых ресурсов УБИ.130								Данная угроза не применяется к рассматриваемой АС
Угроза подмены субъекта сетевого доступа УБИ.131								Данная угроза не применяется к рассматриваемой АС
Угроза получения предварительной информации об объекте защиты УБИ.132								Данная угроза не применяется к рассматриваемой АС
Угроза получения сведений о владельце беспроводного устройства УБИ.133								Данная угроза не применяется к рассматриваемой АС
Угроза потери доверия к поставщику облачных услуг УБИ.134								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза потери и утечки данных, обрабатываемых в облаке УБИ.135								Данная угроза не применяется к рассматриваемой АС
Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных УБИ.136								Данная угроза не применяется к рассматриваемой АС
Угроза потери управления облачными ресурсами УБИ.137								Данная угроза не применяется к рассматриваемой АС
Угроза потери управления собственной инфраструктурой при переносе её в облако УБИ.138								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза преодоления физической защиты УБИ.139	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Контроль физического доступа (наличие замков в помещении, обученный проинструктированный персонал и т.п.). Отсутствие возможности любого из методов проникновения на объект	2	0,35	Низкая	Низкая	Неактуальная
Угроза приведения системы в состояние «отказ в обслуживании» УБИ.140	5	низкая	Возможность отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой или при использовании недостатков реализации сетевых протоколов.	2	0,35	Низкая	Низкая	Неактуальная
Угроза привязки к поставщику облачных услуг УБИ.141								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.143	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза программного сброса пароля BIOS УБИ.144	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Отсутствие в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля	2	0,35	Низкая	Низкая	Неактуальная
Угроза пропуска проверки целостности программного обеспечения УБИ.145	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	Низкая	Низкая	Неактуальная
Угроза прямого обращения к памяти вычислительного поля супер-компьютера УБИ.146								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза распространения несанкционированно повышенных прав на всю грид-систему УБИ.147								Данная угроза не применяется к рассматриваемой АС
Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных УБИ.148								Данная угроза не применяется к рассматриваемой АС
Угроза сбоя обработки специальным образом изменённых файлов УБИ.149	5	низкая	Отсутствие у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке;	2	0,35	Низкая	Низкая	Неактуальная
Угроза сбоя процесса обновления BIOS УБИ.150	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL УБИ.151	5	низкая	Наличие доверенного канала связи посредством СКЗИ Возможность получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера.	2	0,35	Низкая	Низкая	Неактуальная
Угроза удаления аутентификационной информации УБИ.152	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов УБИ.153	5	низкая	Отсутствие у нарушителя сведений о сетевом адресе дискредитируемой системы.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза установки уязвимых версий обновления программного обеспечения BIOS УБИ.154	5	низкая	Установка и использование проверенного ПО. Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
Угроза утраты вычислительных ресурсов УБИ.155	5	низкая	Отсутствие у нарушителя сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы	2	0,35	Низкая	Низкая	Неактуальная
Угроза утраты носителей информации УБИ.156	5	низкая	Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опаснос- ти угрозы	Актуальность угрозы
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.157	5	низкая	Отсутствие возможности получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.) Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
Угроза форматирования носителей информации УБИ.158	5	низкая	Создание резервных копий информации, хранящейся на носителях.	2	0,35	Низкая	Низкая	Неактуальная
Угроза «форсированного веб-браузинга» УБИ.159								

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.160	5	низкая	Отсутствие у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации. Контроль со стороны ответственных за эксплуатацию ТС ИС.	2 0,35	Низкая	Низкая	Неактуальная
Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями УБИ.161							Данная угроза не применяется к рассматриваемой АС
Угроза эксплуатации цифровой подписи программного кода УБИ.162	5	низкая	В системах не используются цифровые подписи кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма прописывания программного кода	2 0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перехвата исключения/сигнала из привилегированного блока функций УБИ.163	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре УБИ.164								Данная угроза не применяется к рассматриваемой АС
Угроза включения в проект не достоверно испытанных компонентов УБИ.165	5	низкая	Для применения в системе выбираются компоненты в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Использование сертифицированного ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза внедрения системной избыточности УБИ.166	5	низкая	Отсутствие избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект) программного обеспечения (или системы в целом).	2	0,35	Низкая	Низкая	Неактуальная
Угроза заражения компьютера при посещении неблагонадёжных сайтов УБИ.167								Данная угроза не применяется к рассматриваемой АС
Угроза «кражи» учётной записи доступа к сетевым сервисам УБИ.168								Данная угроза не применяется к рассматриваемой АС
Угроза наличия механизмов разработчика УБИ.169	5	низкая	Использование проверенного ПО, не подразумевающего использования отладочных механизмов	2	0,35	Низкая	Низкая	Неактуальная
Угроза неправомерного шифрования информации	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза скрытного включения вычислительного устройства в состав бот-сети УБИ.171								Данная угроза не применяется к рассматриваемой АС
Угроза распространения «почтовых червей» УБИ.172								Данная угроза не применяется к рассматриваемой АС
Угроза «спама» веб-сервера УБИ.173								Данная угроза не применяется к рассматриваемой АС
Угроза «фарминга» УБИ.174								Данная угроза не применяется к рассматриваемой АС
Угроза «фишинга» УБИ.175								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты УБИ.176	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная
Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью УБИ.177	5	низкая	Отсутствие (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора»	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного использования системных и сетевых утилит УБИ.178	5	низкая	Предоставление прав пользователю в минимально достаточном объеме. Отсутствие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему, предназначенных для использования администратором для диагностики и обслуживания системы	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированной модификации защищаемой информации УБИ.179	5	низкая	Предоставление прав пользователю в минимально достаточном объеме. Контроль со стороны ответственных за эксплуатацию ТС ИС. Использование доверенного канала связи СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
Угроза отказа подсистемы обеспечения температурного режима УБИ.180	5	низкая	Реализация угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение/вывод из строя компонентов подсистемы.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перехвата одноразовых паролей в режиме реального времени УБИ.181	5	низкая	Отсутствие у нарушителя сведений об информации идентификации/аутентификации дискредитируемого пользователя условно-постоянного действия Невозможность осуществления нарушителем перехвата трафика между системой и пользователем, ввиду использования доверенного канала связи СКЗИ	2	0,35	Низкая	Низкая	Неактуальная
Угроза физического устаревания аппаратных компонентов УБИ.182	5	низкая	Возможность нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды .	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.183								Данная угроза не применяется к рассматриваемой АС
Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства УБИ.184								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного изменения параметров настройки средств защиты информации УБИ.185	5	низкая	Отсутствие СЗИ, вследствие этого отсутствие у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	2	0,35	Низкая	Низкая	Неактуальная
Угроза внедрения вредоносного кода через рекламу, сервисы и контент УБИ.186								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного воздействия на средство защиты информации УБИ.187	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза подмены программного обеспечения УБИ.188								Данная угроза не применяется к рассматриваемой АС
Угроза маскирования действий вредоносного кода УБИ.189	5	низкая		2	0,35	Низкая	Низкая	Неактуальная
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет УБИ.190								Данная угроза не применяется к рассматриваемой АС
Угроза внедрения вредоносного кода в дистрибутив программного обеспечения УБИ.191	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объеме	2	0,35	Низкая	Низкая	Неактуальная
Угроза использования уязвимых версий программного обеспечения УБИ.192	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объеме	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика УБИ.193	5	низкая	Использование на АС базового проверенного набора ПО. Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного использования привилегированных функций мобильного устройства УБИ.194								Данная угроза не применяется к рассматриваемой АС
Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.195								Данная угроза не применяется к рассматриваемой АС
Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве УБИ.196								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза хищения аутентификационной информации из временных файлов cookie УБИ.197	5	низкая	Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Неактуальная
Угроза скрытой регистрации вредоносной программой учетных записей администраторов УБИ.198	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объеме	2	0,35	Низкая	Неактуальная
Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.199							Данная угроза не применяется к рассматриваемой АС
Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.200							Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере УБИ.201								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированной установки приложений на мобильные устройства УБИ.202								Данная угроза не применяется к рассматриваемой АС
Угроза утечки информации с не подключенных к сети Интернет компьютеров УБИ.203								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров УБИ.204								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы Y=(Y1+Y2)/20	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты УБИ.205	5	низкая	Возможность нарушения работы компьютера и отказа в доступе к его данным за счет ошибочного блокирования средством защиты информации файлов.	2	0,35	Низкая	Низкая	Неактуальная
Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем УБИ.206								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей) УБИ.207								Данная угроза не применяется к рассматриваемой АС
Угроза не целевого использования вычислительных ресурсов средства вычислительной техники УБИ.208								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к защищаемой памяти ядра процессора УБИ.209								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения УБИ.210								Данная угроза не применяется к рассматриваемой АС
Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем УБИ.211								Данная угроза не применяется к рассматриваемой АС
Угроза перехвата управления информационной системой УБИ.212								Данная угроза не применяется к рассматриваемой

Продолжение таблицы 8

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза обхода многофакторной аутентификации УБИ.213								Данная угроза не применяется к рассматриваемой АС
Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации УБИ.214								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к системе при помощи сторонних сервисов УБИ.215								Данная угроза не применяется к рассматриваемой АС
Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах УБИ.216								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы 8

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опаснос- ти угрозы	Актуальность угрозы
Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения УБИ.217								Данная угроза не применяется к рассматриваемой АС

Исходя из результатов таблицы 8, в АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», возможна реализация следующих угроз безопасности информации:

- УБИ.026. Угроза искажения XML-схемы;
- УБИ.027. Угроза искажения вводимой и выводимой на периферийные устройства информации;
- УБИ.028. Угроза использования альтернативных путей доступа к ресурсам;
- УБИ.030. Угроза использования информации идентификации/аутентификации, заданной по умолчанию;
- УБИ.033. Угроза использования слабостей кодирования входных данных;
- УБИ.034. Угроза использования слабостей протоколов сетевого/локального обмена данными;
- УБИ.063. Угроза некорректного использования функционала программного и аппаратного обеспечения;
- УБИ.071. Угроза несанкционированного восстановления удалённой защищаемой информации;
- УБИ.074. Угроза несанкционированного доступа к аутентификационной информации;
- УБИ.086. Угроза несанкционированного изменения аутентификационной информации;
- УБИ.088. Угроза несанкционированного копирования защищаемой информации;
- УБИ.182. Угроза физического устаревания аппаратных компонентов.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходом ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

Для анализа угроз безопасности информации должен использоваться банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России.[4]

Описание актуальных угроз безопасности информации представлено в таблице 9.

Таблица 9 — Описание актуальных угроз безопасности информации

№ п/п	Угроза безопасности информации	Нарушитель	Уязвимость	Способы реализации	Объекты воздействия	Последствия
1	УБИ.026. Угроза искажения XML-схемы	Внутренний нарушитель со средним потенциалом	BDU:2018-00868: Уязвимость браузера Firefox, связанная с ошибками реализации хранилища файлов cookies, позволяющая нарушителю получить доступ к файлам cookies httpOnly	Несанкционированный доступ к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя)	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Нарушение конфиденциальности и доступности
2	УБИ.027. Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель с низким потенциалом	BDU:2020-02177: Уязвимость компонента Microsoft Windows Graphics операционных систем Windows, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации	Дезинформирование пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации; подмена или искажение информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение	Нарушение целостности

Продолжение таблицы 9

№ п/п	Угроза безопасности информации	Нарушитель	Уязвимость	Способы реализации	Объекты воздействия	Последствия
3	УБИ.028. Угроза использования альтернативных путей доступа к ресурсам	Внутренний нарушитель с низким потенциалом	BDU:2020-02199: Уязвимость службы Work Folder Service операционных систем Windows, позволяющая нарушителю повысить свои привилегии	Несанкционированный доступ к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса)	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	Нарушение конфиденциальности
4	УБИ.030. Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	Внутренний нарушитель с низким потенциалом	BDU:2017-02221: Уязвимость микропрограммного обеспечения маршрутизатора Axesstel MU553S, связанная с использованием по умолчанию стандартного пароля для учётной записи администратора, позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность данных	Прохождение нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	Нарушение конфиденциальности, целостности и доступности

Продолжение таблицы 9

№ п/п	Угроза безопасности информации	Нарушитель	Уязвимость	Способы реализации	Объекты воздействия	Последствия
5	УБИ.033. Угроза использования слабостей кодирования входных данных	Внутренний нарушитель со средним потенциалом	BDU:2019-04288: Уязвимость операционной системы, существующая из-за недостаточной проверки входных данных, позволяющая нарушителю вызвать повреждение целостности данных в системе	Возможности осуществления нарушения деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.).	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	Нарушение целостности •Нарушение доступности
6	УБИ.034. Угроза использования слабостей протоколов сетевого/локального обмена данными	Внутренний нарушитель с низким потенциалом	BDU:2019-03486: Уязвимость реализации сетевого протокола Microsoft Server Message Block (SMB) операционных систем Windows, позволяющая нарушителю раскрыть защищаемую информацию	Несанкционированный доступ к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов	Системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Нарушение конфиденциальности, целостности и доступности

Продолжение таблицы 9

№ п/п	Угроза безопасности информации	Нарушитель	Уязвимость	Способы реализации	Объекты воздействия	Последствия
7	УБИ.063. Угроза некорректного использования функционала программного и аппаратного обеспечения	Внутренний нарушитель со средним потенциалом	Несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей	Возможность использования декларированных возможностей программных и аппаратных средств определённым (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию.	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение	Нарушение конфиденциальности, целостности и доступности
8	УБИ.071. Угроза несанкционированного восстановления удалённой защищаемой информации	Внутренний нарушитель с низким потенциалом	BDU:2020-02196: Уязвимость драйвера базы данных Microsoft JET Database Engine операционных систем Windows, позволяющая нарушителю выполнить произвольный код	Осуществление прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации	Машинный носитель информации	Нарушение конфиденциальности

Продолжение таблицы 9

№ п/п	Угроза безопасности информации	Нарушитель	Уязвимость	Способы реализации	Объекты воздействия	Последствия
9	УБИ.074. Угроза несанкционированного доступа к аутентификационной информации	Внутренний нарушитель с низким потенциалом	BDU:2017-02523:Уязвимость технологии Clickto-Run пакета программ Microsoft Office, позволяющая нарушителю выполнять действия в системе с привилегиями текущего пользователя	Возможность извлечения паролей, имён пользователей или других учётных данных из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации	Нарушение конфиденциальности
10	УБИ.086. Угроза несанкционированного изменения аутентификационной информации	Внутренний нарушитель с низким потенциалом	BDU:2017-02523:Уязвимость технологии Clickto-Run пакета программ Microsoft Office, позволяющая нарушителю выполнять действия в системе с привилегиями текущего пользователя	Возможность осуществления неправомерного доступа к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств.	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр	Нарушение целостности •Нарушение доступности

Продолжение таблицы 9

№ п/п	Угроза безопасности информации	Нарушитель	Уязвимость	Способы реализации	Объекты воздействия	Последствия
11	УБИ.088. Угроза несанкционированного копирования защищаемой информации	Внутренний нарушитель с низким потенциалом	BDU:2020-01826: Уязвимость браузера Firefox, связанная с неправильным назначением прав доступа для критического ресурса, позволяющая нарушителю получить несанкционированный доступ к информации	Неправомерное получение копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы)	Объекты файловой системы, машинный носитель информации	Нарушение конфиденциальности
12	УБИ.182. Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель с низким потенциалом	Чувствительность к влажности, пыли, загрязнению	Нарушение функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозионных субстанций).	Аппаратное средство	Нарушение доступности

1.5 Классификация АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

Класс защищенности АС был определен в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) равен [уровень значимости информации; масштаб системы].

Уровень значимости информации определялся степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

УЗ равен [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

— высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

— средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

— низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств. [5]

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Результат представлен в виде акта классификации, который представлен в приложении Д.

1.6 Определение требований к системе защиты АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

В соответствии с ГОСТ Р 51624-2014, общей целью защиты информации в АСЗИ является предотвращение или снижение величины ущерба, наносимого владельцу и/или пользователю этой системы или владельцу информации, вследствие реализации угроз безопасности информации. [6]

Задачами обеспечения защиты информации в АС являются:

- предотвращение НСД, уничтожения, искажения, копирования, блокирования защищаемой информации;
- резервирование элементов системы;
- регулирование доступа к элементам системы и защищаемой информации;
- защита от информационного воздействия на технические средства обработки;
- обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности;
- фиксация всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем обработки информации, относящихся к защите информации;
- предотвращение утечки и утраты информации;
- сохранение конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Был определен перечень объектов защиты:

- защищаемая информация (для служебного пользования, персональные данные);
- технологическая информация:
 - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
 - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
 - информация на съемных носителях информации (съемные жесткие магнитные диски), содержащие защищаемую технологическую

информацию системы управления ресурсами или средств доступа к этим системам управления;

- информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;

- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

- служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации;

- программно-технические средства обработки:

- общесистемное и специальное программное обеспечение (операционные системы и другие);

- резервные копии общесистемного программного обеспечения;

- инструментальные средства и утилиты систем управления ресурсами АС;

- аппаратные средства обработки информации;

- средства защиты информации:

- средства управления и разграничения доступа пользователей;

- средства обеспечения регистрации и учета действий с информацией;

- средства, обеспечивающие целостность данных;

- средства антивирусной защиты;

- объекты и помещения, в которых размещены компоненты АС.

В соответствии с приказом ФСТЭК России от 11.02.2013 N 17, установлен второй класс (K2) защищенности для информации для среднего уровня

функционирования АС.[7] Результат классификации АС оформлен в виде акта классификации.

Меры и средства защиты информации, применяемые в АС, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа (присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности));

- управление доступом субъектов доступа к объектам доступа (управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в АС правил разграничения доступа, обеспечение контроля соблюдения этих правил);

- ограничение программной среды (установка и (или) запуск только разрешенного к использованию в АС ПО или исключение возможности установки и (или) запуска запрещенного к использованию в АС ПО);

- защиту машинных носителей информации (исключение возможности несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированного использования съемных машинных носителей информации);

- регистрацию событий безопасности (сбор, запись, хранение и защита информации о событиях безопасности в АС, а также просмотр и анализ информации о таких событиях и реагирование на них);

- антивирусную защиту (обнаружение в АС компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации,

копирования компьютерной информации или нейтрализации средств защиты информации, и реагирование на обнаружение этих программ и информации);

— обнаружение (предотвращение) вторжений (обнаружение действий в АС, направленных на преднамеренный НСД к информации, специальные воздействия на АС и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, и реагирование на эти действия);

— целостность АС и информации (обнаружение фактов несанкционированного нарушения целостности АС и содержащихся в ней данных, а также возможность восстановления АС);

— защиту технических средств и оборудования (исключение НСД к стационарным техническим средствам, обрабатывающим информацию, исполнительным устройствам, средствам, обеспечивающим функционирование АС и в помещения, в которых они постоянно расположены, обеспечение защиты технических средств от внешних воздействий, а также защиты информации, представленной в виде информативных электрических сигналов и физических полей);

— защиту автоматизированной системы и ее компонентов (защита информации при ее передаче по каналам связи, взаимодействии АС или ее отдельных сегментов с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями посредством применения архитектуры АС и проектных решений по ее системе защиты, направленных на обеспечение защиты информации);

— планирование мероприятий по обеспечению защиты информации (разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в АС, в том числе предусматривающего мероприятия по защите информации в ходе создания, эксплуатации и вывода из эксплуатации

АС, сроки выполнения мероприятий и ответственных за их выполнение, а также контроль его выполнения);

- обеспечение действий в нештатных (непредвиденных) ситуациях (планирование мероприятий, обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций, а также резервирование программного обеспечения, технических средств, каналов передачи данных АС в случае возникновения нештатных (непредвиденных) ситуаций и обеспечение возможности ее восстановления);

- информирование и обучение персонала (информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты АС и отдельных средств защиты информации, а также теоретическое и практическое обучение по эксплуатации системы защиты АС и отдельных средств защиты информации);

- выявление инцидентов и реагирование на них (обнаружение, идентификация, анализ инцидентов в АС, а также принятие мер по устранению и предупреждению инцидентов);

- управление конфигурацией АС и ее системы защиты (управление изменениями конфигурации АС и ее системы защиты информации, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений).

Определены следующие требования к сертифицированным средствам защиты информации для АС третьего класса защищенности:

- средства вычислительной техники не ниже 5 класса;
- межсетевые экраны 6 класса;
- средства контроля съемных машинных носителей информации 6 класса;

Проведена адаптация базового набора мер защиты информации применительно к АС.

На основе приказа ФСТЭК №17 от 11 февраля 2013 г. был рассмотрен базовый набор мер защиты информации для АС с учетом присвоенного третьего уровня защищенности.[7]

При анализе базового набора мер защиты информации, было установлено, что пункт «ХІ. Защита среды виртуализации (ЗСВ)» неактуален для АС, так как в автоматизированной системе управления отсутствует среда визуализации.

Мера защиты «ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)» была исключена, так как в АС исключена авторизация внешних пользователей.

Были исключены меры «УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети», «УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа», «УПД.15 Регламентация и контроль использования в информационной системе мобильных технических средств», так как в данной АС обработка информации происходит без применения беспроводного доступа, мобильных технических средств и внешних информационно-телекоммуникационных сетей.

Мера защиты «ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе» была исключена, так как в данной АС обработка информации происходит без применения беспроводного доступа и мобильных технических средств.

Мера защиты «ОДТ.7 Контроль состояния и качества предоставления поставщиком телекоммуникационных услуг вычислительных ресурсов (мощностей), в том числе по передаче информации» была исключена, так как в АС отсутствуют телекоммуникационные услуги, предоставляемые сторонними поставщиками.

Была исключена мера ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые

могут активироваться удаленно, и оповещение пользователей об активации таких устройств, так как удаленное управление не используется.

ЗИС.8 Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи, так как не используется технология мобильного кода.

ЗИС.9 Контроль санкционированной и исключение несанкционированной передачи видеoinформации, в том числе регистрация событий, связанных с передачей видеoinформации, их анализ и реагирование на нарушения, связанные с передачей видео информации, так как передача видеoinформации не реализуется в данной АС.

Меры защиты информации в АС, приведенные в таблице 10, являются адаптированными базовыми мерами защиты информации для АС с учетом её уровня защищенности.

Таблица 10 — Меры защиты информации в АС

Условное обозначение и номер меры	Меры защиты информации в АС
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в АС
ИАФ.5	Исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых символов (защита обратной связи при вводе аутентификационной информации)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (экранирование, фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование автоматизированной системы управления
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в АС
III. Ограничение программной среды (ОПС)	
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	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
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в АС
СОВ.2	Обновление базы решающих правил
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей
IX. Обеспечение целостности (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
X. Обеспечение доступности (ОДТ)	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, исполнительные устройства и средства защиты информации, а также средства обеспечения функционирования.

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в АС
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, исполнительные устройства и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита автоматизированной системы и ее компонентов (ЗИС)	
ЗИС.1	Разделение функций по управлению (администрированию) автоматизированной системой управления, управлению (администрированию) системой защиты, функций по обработке информации и иных функций автоматизированной системы управления
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в АС
ЗИС.17	Разбиение автоматизированной системы управления на сегменты (сегментирование) и обеспечение защиты периметров сегментов
ЗИС.22	Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании
ЗИС.23	Защита периметра (физических и (или) логических границ) автоматизированной системы управления при ее взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями
XIV. Обеспечение безопасной разработки программного обеспечения (ОБР)	
ОБР.0	Разработка правил и процедур (политик) обеспечения безопасной разработки программного обеспечения
ОБР.1	Анализ уязвимостей и угроз безопасности информации в ходе разработки программного обеспечения
ОБР.2	Статический анализ кода программного обеспечения в ходе разработки программного обеспечения
ОБР.4	Тестирование на проникновение в ходе разработки программного обеспечения
ОБР.5	Динамический анализ кода программного обеспечения в ходе разработки программного обеспечения
ОБР.6	Документирование процедур обеспечения безопасной разработки программного обеспечения разработчиком и представление их заказчику (оператору)
XV. Управление обновлениями программного обеспечения (ОПО)	
ОПО.0	Разработка правил и процедур (политик) управления обновлениями программного обеспечения (включая получение, проверку и установку обновлений)
ОПО.1	Получение обновлений программного обеспечения от разработчика или уполномоченного им лица
ОПО.2	Тестирование обновлений программного обеспечения до его установки на макете или в тестовой зоне
XVI. Планирование мероприятий по обеспечению защиты информации (ПЛН)	
ПЛН.0	Разработка правил и процедур (политик) планирования мероприятий по обеспечению защиты информации
ПЛН.1	Определение лиц, ответственных за планирование, реализацию и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в АС
ПЛН.3	Контроль выполнения мероприятий по обеспечению защиты информации в автоматизированных системах управления, предусмотренных утвержденным планом
XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	
ДНС.0	Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденных) ситуациях
ДНС.1	Разработка плана действий на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.2	Обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.4	Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированных систем управления на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.5	Обеспечение возможности восстановления автоматизированной системы управления и (или) ее компонент в случае возникновения нештатных (непредвиденных) ситуаций
XVIII. Информирование и обучение персонала (ИПО)	
ИПО.0	Разработка правил и процедур (политик) информирования и обучения персонала
ИПО.1	Информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
ИПО.2	Обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
ИПО.3	Проведение практических занятий с персоналом по правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
XIX. Анализ угроз безопасности информации и рисков от их реализации (УБИ)	
УБИ.0	Разработка правил и процедур (политик) анализа угроз безопасности информации и рисков от их реализации
УБИ.1	Периодический анализ изменения угроз безопасности информации, возникающих в ходе эксплуатации автоматизированной системы управления
УБИ.2	Периодическая переоценка последствий от реализации угроз безопасности информации (анализ риска)

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в АС
XX. Выявление инцидентов и реагирование на них (ИНЦ)	
ИНЦ.0	Разработка правил и процедур (политик) выявления инцидентов и реагирования на них
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ.5	Принятие мер по устранению последствий инцидентов
ИНЦ.6	Планирование и принятие мер по предотвращению повторных инцидентов
XXI. Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)	
УКФ.0	Разработка правил и процедур (политик) управления конфигурацией автоматизированной системы управления и ее системы защиты
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию автоматизированной системы управления и ее системы защиты
УКФ.2	Управление изменениями конфигурации автоматизированной системы управления и ее системы защиты
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации автоматизированной системы управления и системы защиты на обеспечение защиты информации и согласование изменений в конфигурации автоматизированной системы управления с должностным лицом (работником), ответственным за обеспечение безопасности автоматизированной системы управления
УКФ.4	Документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и ее системы защиты
УКФ.5	Регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления

Сопоставление результатов полученных при определении мер защиты, которые необходимы для нейтрализации угроз безопасности с одной стороны, и при определении угроз безопасности, которые могут быть нейтрализованы

каждой угрозой, с другой стороны, позволяет сделать вывод о том, что все меры защиты адаптированного базового набора должны быть включены в уточненный адаптированный базовый набор мер защиты.

В то же время необходимость включения в базовый набор мер защиты дополнительных мер не требуется, поскольку базового набора мер защиты для УЗЗ достаточно, чтобы нейтрализовать отмеченные актуальные угрозы безопасности и обеспечить выполнение требований нормативно-правовых документов.

Было разработано техническое задание на разработку системы защиты информации АС. Техническое задание предоставлено в приложении Е.

2 Стадия проектирования

2.1 Описание стадии проектирования

На стадии проектирования СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

- разработка раздела технического проекта на объект информатизации в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещением и монтажом технических средств и систем;
- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;
- закупка сертифицированных технических, программных и программно-технических (в т.ч. криптографических) средств защиты информации и их установка;
- разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;
- организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;

- разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;

- определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации.

2.2 Создание проекта системы защиты информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

Разработка технического проекта системы защиты информации в АС является завершающей стадией проектирования системы защиты информации.

В техническом проекте:

- определяются 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);

- определяются 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, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

- выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы;

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

— определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

— осуществляется 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 класса защищенности информационной системы;

— определяются 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;

— определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации;

— определяется реализация подсистем технической защиты системы защиты информации АС.[7]

На основе этого был создан технический проект системы защиты АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В.Проценко». Проект представлен в приложении Ж.

3 Стадия реализации

3.1 Описание стадии реализации

Стадия реализации включает в себя разработку организационно-распорядительной и эксплуатационной документации на АС(технический паспорт АС, инструкции исполнителям АС, журналы и т.д).

При создании системы защиты информации должна быть реализована разрешительная система доступа пользователей и эксплуатационного персонала к информационным ресурсам, программным средствам и ресурсам АС, которые необходимы им для выполнения своих функциональных обязанностей.

3.2 Инструкция системному администратору АС

Инструкция системному администратору определяет функции, права, обязанности и порядок работы в АС на базе серверного парка корпоративной сети.

Системный администратор, является лицом, ответственным за:

— установку, настройку и обновление общесистемного и прикладного ПО в АС;

— установку, настройку и обновление механизмов безопасности в АС.

Функциями Системного администратора являются:

— установка, настройка и обновление общесистемного и прикладного ПО;

— установка и настройка средств защиты информации;

— установка, настройка и обновление антивирусных средств;

— регулярное обновление антивирусных баз в АС;

— управление учетными записями исполнителей АС;

— управление полномочиями доступа исполнителей АС к информации

на накопителях АС;

- периодический контроль за выполнением исполнителями АС требований по защите обрабатываемой информации путем анализа журнала (ов) протоколирования работы в АС;

- настройка и сопровождение подсистемы регистрации и учета действий исполнителей при работе в АС;

- регулярное проведение анализа системного журнала АС для выявления попыток несанкционированного доступа к защищаемым ресурсам;

- архивирование журналов операционной системы и системы ЗИ;

- своевременное информирование Администратора безопасности АС о несанкционированных действиях персонала и участие в проведении расследования попыток НСД;

- периодическое тестирование функций установленной в АС СЗИ, особенно при изменении программной среды и полномочий исполнителей;

- резервирование и восстановление программной среды, программных средств и настроек СЗИ при сбоях.

Системный администратор обязан осуществлять установку, настройку и обновление общесистемного и прикладного ПО в соответствии с руководствами, инструкциями и рекомендациями по установке используемых программных продуктов.[8]

Основываясь на этом, была разработана инструкция системному администратору, которая приведена в приложении К.

3.3 Инструкция пользователю АС

Инструкция пользователю АС регламентирует общие положения и порядок работы Пользователя АС в АС на базе серверного парка корпоративной сети в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Допуск пользователя к работе в АС оформляется документально в виде разрешительной системы доступа к ресурсам АС.

В данной инструкции были описаны права и обязанности пользователя, ответственность и порядок работы в АС. Инструкция пользователя приведена в приложении Л.

3.4 Инструкция администратору безопасности

Инструкция администратору безопасности определяет функции, права, обязанности и порядок работы в АС на базе серверного парка корпоративной сети.

Были выделены функции администратора безопасности:

- контроль доступа лиц к АС в соответствии с «Матрицей доступа к АС...»;
- контроль за целостностью защитных знаков, пломб и печатей в АС;
- контроль за неизменностью конфигурации и состава технических и программных средств АС (объекта информатизации в целом);
- обеспечение функционирования АС в установленном штатном режиме, а также защита АС от несанкционированного доступа к информации;
- контроль за установкой, настройкой и обновлением общесистемного ПО, прикладного ПО и системы защиты информации в АС Системным администратором АС;
- контроль за выполнением пользователями АС требований по защите обрабатываемой информации, контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты КИ, при проведении работ в АС;
- контроль за регулярным обновлением антивирусных баз в АС;
- резервное копирование, уничтожение и восстановление

конфиденциальной информации, а также несекретной информации;

- анализ файла журнала безопасности АС, предоставляемого Системным администратором АС (ежемесячно или по требованию);

- поддержание и контроль соблюдения пользователями установленного порядка и правил антивирусной защиты информации в АС;

- ведение (своевременное создание и изменение) документации на АС в соответствии с требованиями нормативных документов;

- контроль работоспособности и использования средств защиты информации, контроль соблюдения требований по размещению и использованию АС, указанных в предписании на эксплуатацию.

Права, обязанности, контроль за установкой и обновлением общесистемного ПО, а также порядок работы в АС описаны в инструкции администратора безопасности, которая приведена в приложении М.

Пользователи АС, системный администратор и администратор безопасности обязаны зафиксировать в «Журнале учета работы в АС» свои действия, совершаемые в АС: включение – выключение АС; смена пользователя (перезагрузка АС, вход – выход в систему); характер работ (работа с приложениями, создание, редактирование документа, отправка почты). Журнал учета работ показан в приложении Н.

3.5 Инструкция по антивирусному контролю в АС

Перед началом работы с МНИ, пользователь АС, системный администратор, а также администратор безопасности должен осуществлять проверку содержимого МНИ на отсутствие вирусов штатными антивирусными средствами, установленными в АС, в соответствии с «Инструкцией по использованию средств антивирусной защиты».

В данной инструкции был описан порядок использования средств антивирусной защиты исполнителями (администраторами) в АС, которая приведена в приложении П.

3.6 Разрешительная система доступа к ресурсам АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

Разрешительная система доступа к конфиденциальной информации представляет собой совокупность установленных руководством предприятия нормативных положений, обеспечивающих обоснованный и правомерный доступ пользователей к необходимому им для выполнения служебных обязанностей объему конфиденциальной информации. Должно быть определено, кто из руководителей предприятия и структурных подразделений, кому из пользователей и с какими категориями конфиденциальной информации может давать разрешение на ознакомление, а также порядок оформления таких разрешений в зависимости от вида учета или категорий информации. При этом право давать разрешение на ознакомление и право работать с конфиденциальной информацией может быть предоставлено только лицам, имеющим допуск к конфиденциальной информации в целом, оформленный приказом руководителя предприятия или контрактом, а в отдельных случаях, по усмотрению руководителя предприятия, и через органы Федеральной службы безопасности.

Разрешительная система доступа представлена в приложении И.

3.7 Разработка технического паспорта АС

Паспортом на АС называют технический документ, который содержит данные, которые необходимы для осуществления контроля при внедрении автоматизированной системы, а также при ее эксплуатации.

Разработка паспорта на автоматизированную систему осуществляется с целью полного своевременного контроля всех стадий жизненного цикла АС: ее разработки, введения в эксплуатацию, функционирования; анализа системы и оценки ее эффективности; сравнения с аналогами.

Разработка паспорта на АС выполняется как при создании новой, так и при обследовании действующей автоматизированной системы.

На основе этого были составлены перечни ОТСС и ВТСС, представленные в таблицах 11 и 12, соответственно.

Таблица 11 – Перечень ОТСС

№ п/п	Тип ОТСС	Заводской номер	Серийный номер	Примечание
1	СХД резервного копирования StoreOnce (HP Storeonce 4500)	0174590		
2	СХД 3PAR 7200(HP StoreServ 7200 (M6710/7000 Encl))	0174588		
3	AltellNeo Master	0174598	04615/2, з/з E366592	
4	ME5200	0174596		
5	Blade-система HP c7000	0174591	CZJ43304QB	

Таблица 12 – Перечень ВТСС

№ п/п	Тип ВТСС	Заводской номер	Примечание
1	Телефон	-	1 шт.
2	Сервера Ascon	-	-
3	Манипулятор «мышь» Logitech	-	1 шт.
4	Кондиционер 1 STULZ STU000831	-	1 шт.
5	Датчик пожарной сигнализации	-	4 шт.
6	Клавиатура Logitech	-	1 шт.
7	Монитор Samsung	-	1 шт.
8	Пульт автоматического отключения газо-пожаротушения	-	1 шт.

Расстояние от ОТСС до границы контролируемой зоны составляет не менее 90 м. Электропитание ОТСС осуществляется от трансформаторной подстанции, расположенной в пределах КЗ. Схемы электропитания розеточной и осветительной сети объекта представлены на рисунке 2.

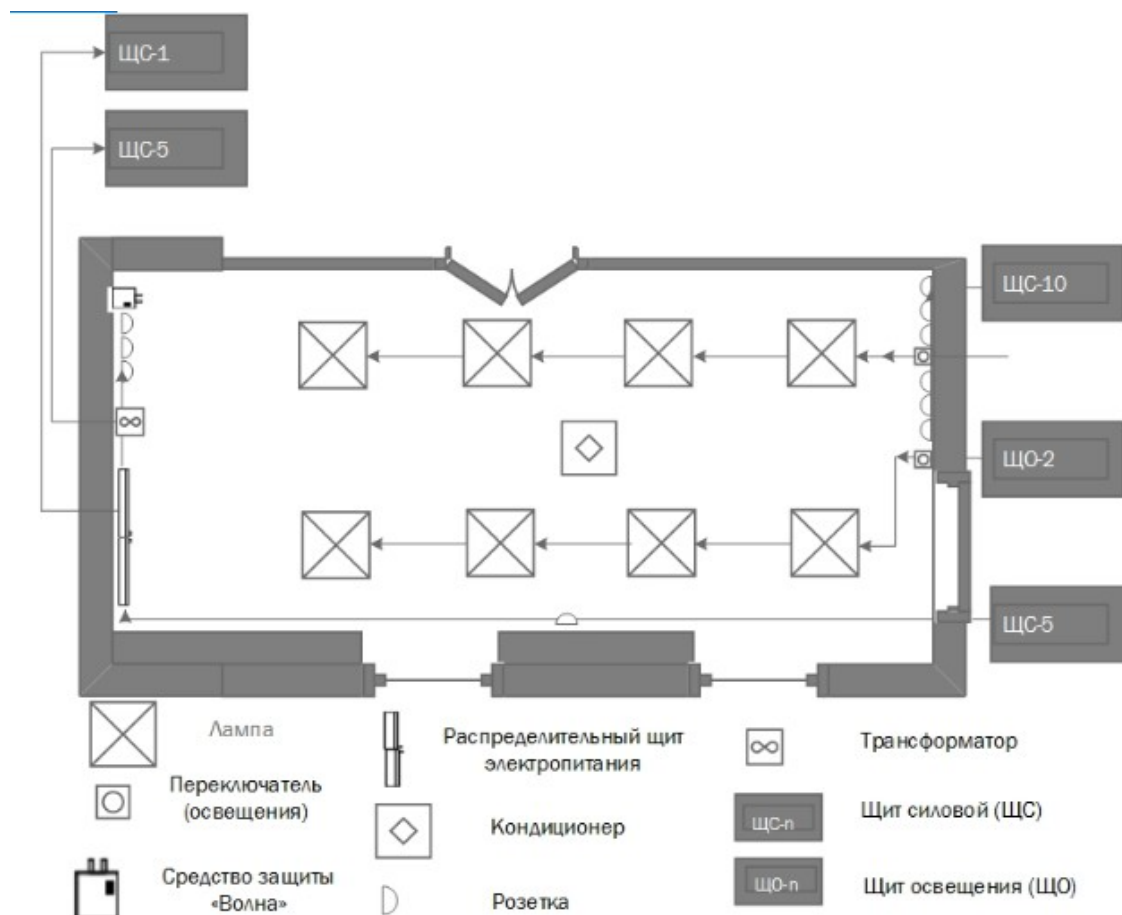


Рисунок 2 – Схема электропитания и освещения

На объекте установлена пожарная сигнализация и система пожаротушения. Была разработана схема, представленная на рисунке 3.

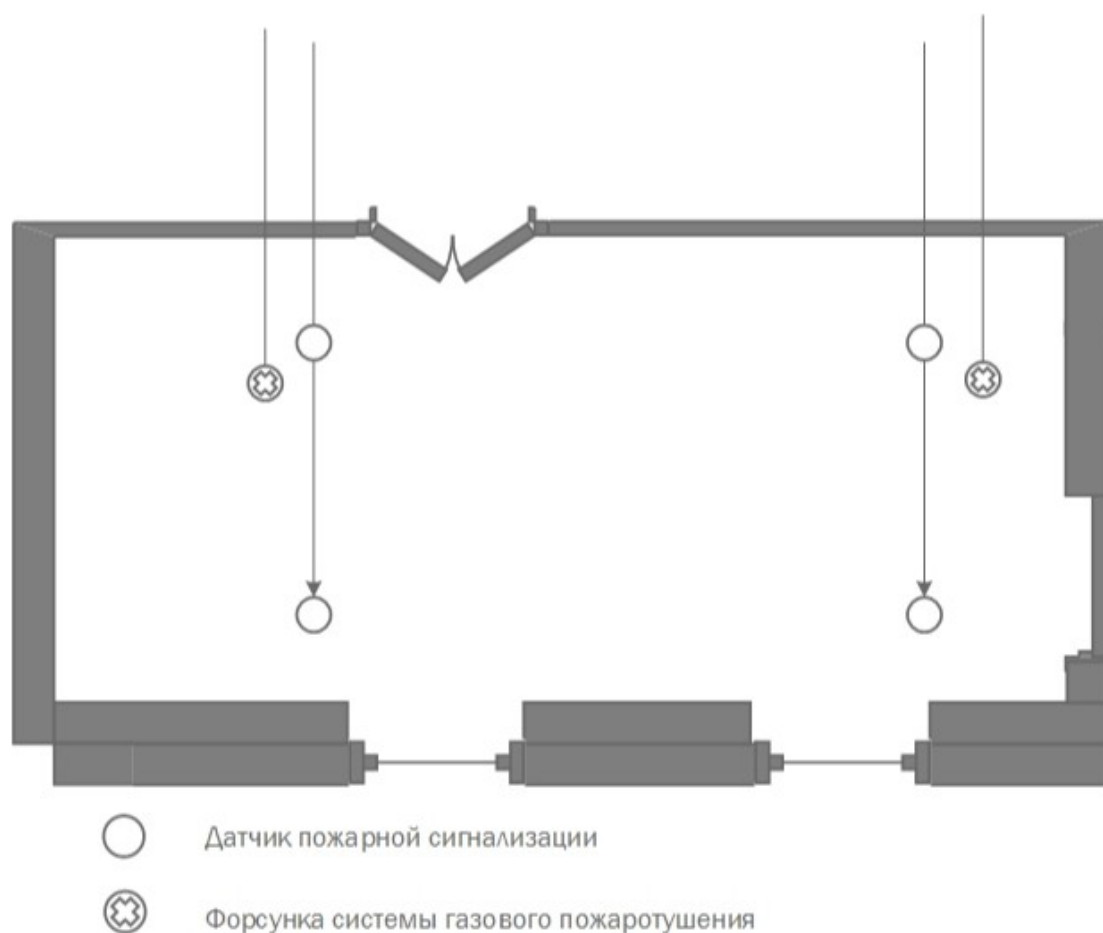


Рисунок 3 – Схема пожарной сигнализации и системы пожаротушения

Был разработан технический паспорт на АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В.Проценко» в соответствии с ГОСТ Р 51583-2014 и со структурой АС, техническими средствами, а также с реализованными средствами защиты. [9] Документ представлен в приложении Р.

После чего был создан приказ о назначении администраторов безопасности и системных администраторов АС. Он приведен в приложении С.

4 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.

Работа специалиста по защите информации на протяжении всего дня предполагает работу как с бумажными носителями информации, так и за компьютером, что негативно сказывается на работе органов зрения. Чтение оказывает большую нагрузку на глаза, так как восприятие текста связано с чрезвычайно быстрым выполнением зрительным анализатором работы по различению огромного количества крайне мелких деталей и по перемещению вдоль строк и от строки к строке. Работа же на персональном компьютере связана с постоянным напряжением функций зрительного аппарата.

Негативно влияют на зрения следующие факторы:

- отсутствие или недостаток естественного света;
- недостаточная искусственная освещенность рабочей зоны;
- повышенная яркость света;
- повышенная контрастность;
- прямая и отраженная блескость;
- недостаточно высокое напряжение монитора;
- несоблюдение расстояния от глаз до экрана;
- зрительное напряжение.

Существует качественная разница между изображением на мониторе и в реальной жизни. Картинка экрана самосветящаяся, а не отраженная в свете, она менее контрастная, мерцает и не имеет четких контуров. Зрительный анализатор же в процессе эволюции приспособился к восприятию объектов в отраженном свете, которые не имеют вышеописанных характеристик. Фокусировать и удерживать взгляд на таком изображении глазам сложнее, это приводит к перенапряжению мышечного аппарата, спазму аккомодационного

механизма, а также может привести к развитию компьютерного зрительного синдрома(КЗС).

Полностью «обезвредить» работу за компьютером невозможно, но минимизировать негативное влияние монитора на глаза — вполне. Существует несколько рекомендаций:

- правильно организованное рабочее место;
- соблюдать расстояние до монитора;
- контролировать осанку;
- использовать компьютерные очки;
- чаще моргать;
- правильно питаться;
- устраивать перерывы.

А также можно проводить минимальную зарядку для шеи, сделанную во время отдыха. Упражнения очень простые: необходимо покрутить головой в разные стороны, наклонять голову (аккуратно) в разные стороны, тянуть шею. Данный комплекс мер поможет снять усталость, а также улучшит микроциркуляцию крови в органах зрения. [10]

Заключение

В ходе выполнения выпускной квалификационной работы был осуществлен анализ автоматизированной системы на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В.Проценко» в текущем состоянии, а также определены угрозы безопасности информации при ее обработке в АС.

Была выполнена подготовка автоматизированной системы к аттестации по требованиям безопасности информации, соответственно разработаны следующие документы:

- приказ о создании экспертной комиссии;
- акт экспертизы информации;
- модель угроз безопасности;
- акт определения защищенности автоматизированной системы;
- акт классификации автоматизированной системы;
- техническое задание;
- технический проект;
- разрешительная система доступа к ресурсам автоматизированной системы;
- модель нарушителя;
- описание технологического процесса обработки информации;
- инструкция пользователю автоматизированной системы;
- инструкция системному администратору автоматизированной системы;
- инструкция администратору безопасности автоматизированной системы;
- инструкция по антивирусному контролю в

автоматизированной системе;

- технический паспорт автоматизированной системы;
- приказ о назначении администраторов безопасности и системных администраторов автоматизированной системы;
- журнал учета работ в автоматизированной системе.

Изучены вредные психофизиологические факторы влияющие на органы зрения специалиста по защите информации, а также методы и средства физической культуры, которые снижают их воздействие.

Таким образом, задание на выпускную квалификационную работу было выполнено в полном объеме.

Протокол проверки на оригинальность представлен в приложении Т.

Список использованных источников

1 Методика определения угроз безопасности информации в информационных системах(проект) [Электронный ресурс]. — Режим доступа: <http://os.x-pdf.ru/20tehnicheckie/176886-1-utverzhdenn-fstek-rossii-2015-metodicheskij-dokument-metodika-opre.php> (дата обращения 14.04.2020)

2 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Текст] — Утверждена заместителем директора ФСТЭК России от 14 февраля 2008 г. — [Электронный ресурс]. — Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380>

3 Угрозы информационной безопасности в АС [Электронный ресурс]. — Режим доступа: <http://asher.ru/security/book/its/05> (дата обращения 14.04.2020)

4 Банк данных угроз безопасности информации [Электронный ресурс] — Режим доступа: <http://bdu.fstec.ru/ubi/vul> (дата обращения 15.04.2020)

5 Меры защиты информации в государственных информационных системах[Текст] — Утвержден ФСТЭК России от 11 февраля 2014 г. — [Электронный ресурс]. — Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument> (дата обращения 20.04.2020)

6 ГОСТ Р 51624-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования [Текст]. — введ. 01-092014. — М.: Стандартинформ, 2014. — 5 с. — [Электронный ресурс]. — Режим доступа: <http://docs.cntd.ru/document/1200108858> (21.04.2020)

7 Приказ ФСТЭК России от 11 февраля 2013 г. N 17 [Электронный ресурс]. — Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazu/702> (дата обращения 22.04.2020)

9 Обязанности, навыки, задачи системного администратора [Электронный ресурс] — Режим доступа:

<https://linuxtrainingcenter.com/sistemnyj-administrator/> (дата обращения 28.04.2020)

10 Основные вредные факторы, влияющие на состояние здоровья людей, работающих за компьютером [Электронный ресурс] — Режим доступа: <https://lektsii.org/15-84989.html> (дата обращения 30.04.2020)

Приложение А
(обязательное)

Приказ о создании экспертной комиссии

ПРИКАЗ

О создании экспертной комиссии

№ _____

г. Заречный

от «__» _____ 202__ г.

Во исполнение требований «Положения о порядке организации и проведения работ по технической защите конфиденциальной информации на «ПО «Старт»» от 22.03.2005 № 75-10/455дсп, для создания и аттестации объекта информатизации по требованиям безопасности информации.

ПРИКАЗЫВАЮ:

А.1 Создать экспертную комиссию в составе:

Председатель комиссии – должность, ФИО.

Члены комиссии:

- должность, ФИО;
- должность, ФИО;
- должность, ФИО;
- должность, ФИО.

А.2 Экспертной комиссии провести экспертизу информации, предполагаемой к обработке в создаваемой автоматизированной системе (АС) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

А.3 Результаты работы комиссии оформить соответствующим актом.

А.4 Председателю комиссии обеспечить рассмотрение на ПДТК результа-

тов работы экспертной комиссии (акт экспертизы информации) и материалов предпроектного обследования АС (акт классификации ИС, акт определения уровня защищенности ИСПДн) для осуществления контроля в соответствии с приказом ГК «Росатом» от 20.06.2012 года № 1/540-П-дсп «Об оценке видов информации ограниченного доступа при создании, модернизации и эксплуатации автоматизированных систем в защищенном исполнении и прикладных информационных систем».

А.5 Контроль за исполнением приказа возложить на заместителя генерального директора по безопасности — ФИО.

А.6 Приказ вступает в силу со дня его подписания.

Главный инженер

ФИО

С приказом ознакомлены:

ФИО

ФИО

ФИО

ФИО

ФИО

Приложение Б
(обязательное)
Акт экспертизы информации

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

АКТ

экспертизы информации, обрабатываемой в автоматизированной системе
на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт»
им. М.В.Проценко», предназначенной для обработки информации
ограниченного доступа, не содержащей сведений, составляющих
государственную тайну

Комиссия, назначенная Приказом № _____ от _____ г. в составе
Председателя комиссии: должность, ФИО.

Членов комиссии:

- должность, ФИО;
- должность, ФИО;
- должность, ФИО;
- должность, ФИО.

провела экспертизу информации, предполагаемой к обработке на объекте
ВТ – АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО
«Старт» им. М.В.Проценко», предназначенной для обработки информации

ограниченного доступа, не содержащей сведений, составляющих государственную тайну. Перечень сведений приведен в таблице 1.

Таблица Б.1 – Перечень сведений конфиденциального характера

№ п/п	Наименование сведений	Примечание
1	Планы развития предприятия Уровень доходов предприятия Сведения о подрядчиках Сведения о производственных возможностях предприятия Сведения о финансовых операциях Методы изучения рынка сбыта	Коммерческая тайна
2	Фамилия, имя, отчество Паспортные данные (серия/номер/дата/кем выдан) Дата и место рождения Адрес проживания (прописки) Состояние в браке Состав семьи Место работы ИНН Номер страхового свидетельства ПФР Сведения о предыдущих местах работы Общий трудовой стаж Сведения о социальных льготах Сведения о поощрениях и наградах Табельный номер работника Должность работника Структурное подразделение Данные по отпускам Статус военнообязанного Уровень образования Наименование учебного заведения Год окончания Номер диплома Специальность по диплому Квалификация по диплому Данные о повышении квалификации Форма профессионального послевузовского образования Наименование образовательного/научного подразделения Номер и дата выдачи удостоверения о дополнительном образовании Сведения о состоянии здоровья	Персональные данные

Продолжение таблицы Б.1

№ п/п	Наименование сведений	Примечание
3	<p>Организация и состояние системы парольной защиты(значение, порядок генерации, использования, смены и прекращения действия паролей)</p> <p>Организация резервирования конфиденциальной информации, местах хранения резервных копий конфиденциальной, ценной и другой важной информации</p> <p>Содержание переписки, телефонных переговоров, почтовых отправлений, электронных и иных сообщений.</p>	ДСП

Главный инженер

ФИО

С приказом ознакомлены:

ФИО

ФИО

ФИО

ФИО

ФИО

Приложение В

(обязательное)

Акт определения уровня защищенности АС

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

АКТ

определения уровня защищенности информационной системы
персональных данных (автоматизированная система на базе серверного парка
корпоративной сети) АО «ФНПЦ «ПО «Старт» им.М.В. Проценко.

г. Заречный

В.1 Основные положения:

Информационная система, обрабатывающая специальные категории персональных данных — информационная система, в которой обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система, обрабатывающая биометрические персональные данные — информационная система, обрабатывающая сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система, обрабатывающая общедоступные персональные данные — информационная система, в которой обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных.

Информационная система, обрабатывающая иные категории персональных данных — информационная система, в которой не обрабатываются персональные данные, указанные в п.п. 1.1. ÷ 1.3. настоящего документа.

Информационная система, обрабатывающая персональные данные сотрудников оператора — информационная система, в которой обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

Актуальная угроза безопасности персональных данных — это совокупность условий и факторов, создающих актуальную опасность

несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

В.2 Общие данные ИСПДн:

Наименование ИСПДн: ИСПДн (автоматизированная система на базе серверного парка корпоративной сети) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Назначение ИСПДн: обработка, хранение, печать и передача по каналам связи информации следующих степеней конфиденциальности: «несекретно», «персональные данные».

В.3 Исходные данные об ИСПДн

Цели обработки ПДн: осуществление обработки ПДн для обеспечения непрерывности бизнес-процессов предприятия.

Категория субъектов ПДн: ПДн субъектов, являющихся сотрудниками предприятия, а также ПДн субъектов, не являющихся сотрудниками предприятия.

Перечень ПДн: ФИО; год, месяц, дата рождения; место рождения; должность; паспортные данные; номер структурного подразделения предприятия; сведения о доходах; сведения об инвалидности.

Оператор ИСПДн: АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Объем обрабатываемых ПДн: менее чем 100 000 субъектов (в ИСПДн обрабатываются ПДн субъектов, являющихся сотрудниками оператора и не являющихся сотрудниками оператора);

Категории ПДн, обрабатываемые в ИСПДн: информационная система, обрабатывающая специальные категории персональных данных, т.к. в информационной системе обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных.

ИСПДн по типу обработки ПДн: информационная система персональных данных обрабатывающая персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

Актуальные угрозы для ИСПДн (в соответствии с «Моделью угроз...»)

Типы актуальных угроз для ИСПДн (с учетом п. 2.3.8 настоящего документа) – угрозы 3-го типа (т.к. для ИСПДн актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе).

Уровень защищенности ПДн при обработке в ИСПДн: 3 – й уровень защищенности ПДн (т.к. для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора).

Председатель комиссии:

ФИО

Члены комиссии:

ФИО

ФИО

ФИО

ФИО

ФИО

Приложение Г

(обязательное)

Модель угроз безопасности информации АС на базе серверного парка КС

АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА БАЗЕ СЕРВЕРНОГО ПАРКА
КОРПОРАТИВНОЙ СЕТИ АО «ФНПЦ «ПО «СТАРТ» ИМ. М.В. ПРОЦЕНКО».

г. Заречный

Г.1 Общие положения

Настоящая модель угроз разработана в соответствии с Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также с учетом национальных стандартов Российской Федерации в области защиты информации и в области создания автоматизированных систем.

В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, содержащей сведения, составляющие коммерческую тайну (далее — информация), от несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее — защита информации) при обработке указанной информации.

В документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Настоящая модель является обязательной при разработке и ввода в эксплуатацию автоматизированной системы (далее — АС) на базе корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Настоящая модель предназначена для обладателей информации, заказчиков, заключивших контракт на создание АС на базе корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»..

Угрозы безопасности, обрабатываемые в АС, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз в АС.

Г.2 Описание АС и особенностей ее функционирования

Цель и задачи, решаемые АС

Целью автоматизированной системы (АС) на базе серверного парка корпоративной сети (КС) является - обработка, хранение и передача по каналам связи информации степени конфиденциальности – для служебного пользования, коммерческая тайна, персональные данные, а также несекретной информации

Объектами защиты являются:

- защищаемая информация (для служебного пользования, персональные данные);
- технологическая информация:
 - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
 - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
 - информация на съемных носителях информации (съемные жесткие магнитные диски), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
 - информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;
 - информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и

процедурах перехода к управлению в аварийных режимах;

- служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации;
- программно-технические средства обработки:
 - общесистемное и специальное программное обеспечение (операционные системы и другие);
 - резервные копии общесистемного программного обеспечения;
 - инструментальные средства и утилиты систем управления ресурсами АС;
 - аппаратные средства обработки информации;
- средства защиты информации:
 - средства управления и разграничения доступа пользователей;
 - средства обеспечения регистрации и учета действий с информацией;
 - средства, обеспечивающие целостность данных;
 - средства антивирусной защиты;
- объекты и помещения, в которых размещены компоненты АС.

Г.3 Описание структурно-функциональных характеристик

Физические меры защиты объектов, в которых размещены ресурсы АС: серверное помещение, которое оборудовано системой кондиционирования воздуха, вентиляцией воздуха, системой пожаро-охранной сигнализации, так же серверная оборудована автоматической установкой газового пожаротушения и металлической дверью с установленным автономным контроллером-считывателем.

Меры по обеспечению контролируемой зоны — все технические средства расположены в пределах одного здания. Оно оборудовано сигнализацией и системой видео-наблюдения.

Все технические средства расположены в пределах КЗ. Состав и характеристики, а также перечень серверов приведен в таблице Г.1 и таблице Г.2, соответственно. Структурная модель АС представлена на рисунке 1.

Таблица Г.1 — Состав и характеристики АС

№ п/п	Оборудование	Примечание
1	СХД резервного копирования StoreOnce (HP Storeonce 4500)	Система хранения данных для резервного копирования
2	СХД 3PAR 7200(HP StoreServ 7200 (M6710/7000 Encl))	Система хранения данных
3	AltellNeo Master	МЭ
4	ME5200	Маршрутизатор
5	Blade-система HP c7000	Блейд-система

Таблица Г.2 — Перечень серверов

№ п/п	Кластер	Сервер	ОС
1	Кластер сервисов серверного парка КС Yanux 4	node01-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node02-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node03-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node04-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node05-cl(HPE ProLiant DL380 Gen10)	Yanux 4
		node06-cl(HPE ProLiant DL380 Gen10)	Yanux 4
2	Кластер сервисов серверного парка КС AstraLinux(Blade-система HP c7000)	bnode01(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode02(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode03(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6

Продолжение таблицы Г.2

№ п/ п	Кластер	Сервер	ОС
2		bnode04(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode05(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode06(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode07(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
		bnode08(Блейд-сервер HPE Integrity BL860c)	AstrLinux Smolensk 1.6
3	Кластер БД	db-node01(HPE ProLiant DL380 Gen10)	AstrLinux Smolensk 1.6
		db-node02(HPE ProLiant DL380 Gen10)	AstrLinux Smolensk 1.6
4	Сервера Ascon	HPE ProLiant DL380 Gen10	Windows Сервер 2008

Перечень ИТ-сервисов приведен в таблице Г.3.

Таблица Г.3 – Перечень ИТ-сервисов

Кластер	Сервис	Назначение
Кластер сервисов серверного парка КС Unix 4	backup_server	Сервис резервного копирования
	conference	Сервис видеоконференций
	dhcp_server	DHCP-сервер
	dns	DNS-сервер
	fs	Файловый сервис
	intuit	Система дистанционного обучения
	mail	Почтовый сервер
	nagios	Сервис мониторинга
	otrs	Система обработки заявок
	replica	Сервис перекачки данных
	sites	Корпоративные сайты
	spd	Сервис подготовки данных
	tomcat	Сервис формирования pdf
	ad1	Контроллер домена

Продолжение таблицы Г.3

Кластер	Сервис	Назначение
	ad2	Контроллер домена
	alfresco	Электронный документооборот
	backup	Сервис резервного копирования
	ca	Удостоверяющий центр
	cmdb	Система инвентаризации
	consultant	Информационно-правовая система Консультант
	dns	DNS-сервер
	dts	Сервер разработки
	fa	Файловый сервис
	homes	Сервер пользовательских данных
	jabber	Сервер обмена сообщений
	ksu	Корпоративная система управления
	ldap	Ldap сервер
	pgsqlddb	Сервер БД разработки задач КСУ
	pgsqldts	Сервер приложений
	redmine	Система управления проектами
	sites	Корпоративные сайты
	svn	Система контроля версий
	tally	Сервис печати
Кластер сервисов серверного парка КС AstraLinux	gitlab	Система управления репозиториями кода
	Maildsp	Почтовый сервер ДСП
	pgsqldb	Сервер БД
	pgsqldev	Сервер приложений для разработки задач КСУ
Сервера ASCON на ОС Windows Сервер 2008	AsconAS5	Аскон
	TFLEXAS	T-Flex DOCs

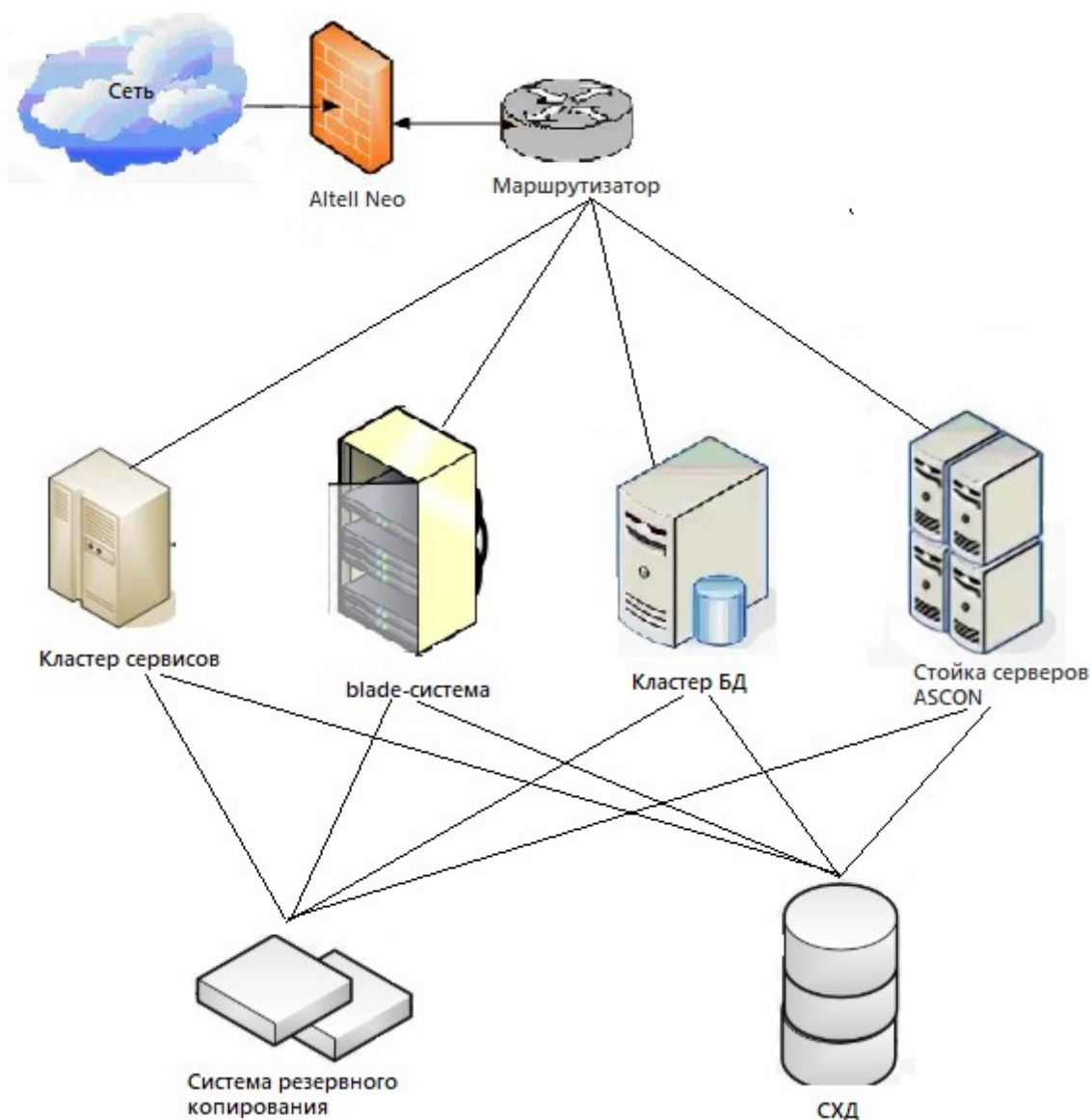


Рисунок Г.1 — Структура АС

Г.4 Возможности нарушителей (модель нарушителя)

Типы и виды нарушителей

В качестве источников угроз БИ могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

Источники угроз безопасности информации могут быть следующих типов:

- антропогенные источники (антропогенные угрозы);

- техногенные источники (техногенные угрозы);
- стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В качестве источников антропогенных угроз безопасности информации могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в АС, или нарушения функционирования АС или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);
- лица, имеющие доступ к АС, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

Таблица Г.4 — Виды и тип нарушителя

№ п/п	Виды нарушителя	Типы нарушителя
1	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний
2	Лица, обеспечивающие функционирование АС или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики)	Внутренний
3	Пользователи ИС	Внутренний
4	Администраторы АС и администраторы БД	Внутренний

Возможные цели и потенциал нарушителей

Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации приведены в таблице Г.5.

Таблица Г.5 — Модель нарушителя

№ п/п	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности
1	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
2	Лица, обеспечивающие функционирование АС или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
3	Пользователи АС	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Непреднамеренные, неосторожные или неквалифицированные действия.
4	Администраторы АС и администраторы БД	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.

Был определен потенциал нарушителя, требуемого для реализации угроз безопасности информации. Потенциал нарушителя и их возможности представлены в таблице Г.6.

Таблица Г.6 — Потенциалы и возможности нарушителей

№ п/п	Потенциал	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица). Лица, обеспечивающие функционирование АС или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики). Пользователи ИС. Бывшие работники (пользователи). Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ.	Имеют возможность получить информацию об уязвимостях отдельных компонент ИС, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации, опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на ИС.

Продолжение таблицы Г.6

№ п/п	Потенциал	Виды нарушителей	Возможности по реализации угроз безопасности информации
2	Нарушители с базовым повышенным (средним) потенциалом	Преступные группы (криминальные структуры). Разработчики, производители, поставщики программных, технических и программно-технических средств. Администраторы АС и администраторы БД.	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах ЗИ, применяемых в АС данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент АС путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных компонент общесистемного ПО. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования

При оценке возможностей нарушителей учитывались условия, что для повышения своих возможностей нарушители 1 вида могут взаимодействовать (вступать в сговор) с нарушителями 2, 3 и 4 видов, поэтому возможности нарушителей объединяются.

Г. 5 Актуальные угрозы безопасности информации

Актуальные угрозы безопасности информации АС представлены в таблице Г.7.

Таблица Г.7 - Актуальные угрозы безопасности информации для АС

УБИ	Число-вой коэф- фициент исходной защищенн ости (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
		Вероят- ность (частота) реализа- ции угрозы	Обоснование	Вероят- ность возникно- вения угрозы Y2				
Угроза автоматического распространения вредоносного кода в грид-системе УБИ.001								Данная угроза не применяется к рассматриваемой АС
Угроза агрегирования данных, передаваемых в грид-системе УБИ.002								Данная угроза не применяется к рассматриваемой АС
Угроза анализа криптографических алгоритмов и их реализации УБИ. 003	5	маловероятно	На АС отсутствует криптографическое ПО. Отсутствие у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	0	0,25	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза аппаратного сброса пароля BIOS УБИ. 004	5	малове- роятно	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	0	0,25	Низкая	Низкая	Неактуальная
Угроза внедрения вредоносного кода в BIOS УБИ. 005	5	малове- роятно	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	0	0,25	Низкая	Низкая	Неактуальная
Угроза внедрения кода или данных УБИ.006	5	малове- роятно	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	0	0,25	Низкая	Низкая	Неактуальная
Угроза воздействия на программы с высокими привилегиями УБИ. 007	5	малове- роятно	Отсутствие административных привилегий у пользователя Наличие доверенного канала связи посредством СКЗИ. Использование на АП базового проверенного набора ПО.	0	0,25	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фицие нт исход- ной защит енност и (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опаснос- ти угрозы	Актуальность угрозы
Угроза восстановления аутентификационной информации УБИ. 008	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
Угроза восстановления предыдущей уязвимой версии BIOS УБИ. 009	5	низкая	На АС установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
Угроза выхода процесса за пределы виртуальной машины УБИ.010								Данная угроза не применяется к рассматриваемой АС
Угроза деавторизации санкционированного клиента беспроводной сети УБИ.011								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза деструктивного изменения конфигурации/среды окружения программ УБИ.012	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза деструктивного использования декларированного функционала BIOS УБИ.013	5	низкая	На АС установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
Угроза длительного удержания вычислительных ресурсов пользователями УБИ.014	5	низкая	Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
Угроза доступа к защищаемым файлам с использованием обходного пути УБИ.015	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза доступа к локальным файлам сервера при помощи URL УБИ.016	5	малове- роятно	Отсутствие у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	0	0,25	Низкая	Низкая	Неактуальная
Угроза доступа/перехвата/изменения HTTP cookies УБИ.017	5	низкая	Отсутствие у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	2	0,35	Низкая	Низкая	Неактуальная
Угроза загрузки нештатной операционной системы УБИ.018	5	низкая	Возможность подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы.	2	0,35	Низкая	Низкая	Неактуальная
Угроза заражения DNS-кеша УБИ.019	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг УБИ.20								Данная угроза не применяется к рассматриваемой АС
Угроза злоупотребления доверием потребителей облачных услуг УБИ.21								Данная угроза не применяется к рассматриваемой АС
Угроза избыточного выделения оперативной памяти УБИ.022	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АС базового проверенного набора ПО. Возможность выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза изменения компонентов информационной (автоматизированной) системы УБИ.023	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза изменения режимов работы аппаратных элементов компьютера УБИ.024	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза изменения системных и глобальных переменных УБИ.025	5	низкая	Отсутствие возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициен т исход- ной защище нности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальнос- ть угрозы
Угроза искажения XML-схемы УБИ.026	5	средняя	Возможность изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером.	5	0,5	Средняя	Средняя	Актуальная
Угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027	5	средняя	Возможность дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза использования альтернативных путей доступа к ресурсам УБИ.028	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса).	5	0,5	Средняя	Средняя	Актуальная
Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами УБИ.029								Данная угроза не применяется к рассматриваемой АС
Угроза использования информации идентификации/ аутентификации, заданной по умолчанию УБИ.030	5	средняя	Наличие у нарушителя сведений о производителе/модели объекта защиты (ОЗ) и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для ОЗ;	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза использования механизмов авторизации для повышения привилегий УБИ.031	5	низкая	Отсутствие административных привилегий у пользователя.	5	0,25	Низкая	Низкая	Неактуальная
Угроза использования поддельных цифровых подписей BIOS УБИ.032	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
Угроза использования слабостей кодирования входных данных УБИ.033	5	средняя	Возможность осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.).	2	0,35	Средняя	Средняя	Актуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы Y=(Y1+Y2) /20	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Наличие доверенного канала связи посредством СКЗИ	5	0,5	Средняя	Средняя	Актуальная
Угроза использования слабых криптографических алгоритмов BIOS УБИ.035	5	низкая	Сложность использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI.	2	0,35	Низкая	Низкая	Неактуальная
Угроза исследования механизмов работы программы УБИ.036	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Число- вой коэф- фициент исход- ной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза исследования приложения через отчёты об ошибках УБИ.037	5	низкая	Отсутствие у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	2	0,35	Низкая	Низкая	Неактуальная
Угроза исчерпания вычислительных ресурсов хранилища больших данных УБИ.038								Данная угроза не применяется к рассматриваемой АС
Угроза исчерпания запаса ключей, необходимых для обновления BIOS УБИ.039	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя	2	0,35	Низкая	Низкая	Неактуальная
Угроза конфликта юрисдикций различных стран УБИ.40								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализации угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза межсайтового скриптинга УБИ.041								Данная угроза не применяется к рассматриваемой АС
Угроза межсайтовой подделки запроса УБИ.042								
Угроза нарушения доступности облачного сервера УБИ.043								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины УБИ.044								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения изоляции среды исполнения BIOS УБИ.045	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия УБИ.046								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке УБИ.047								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин УБИ.048								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения целостности данных кеша УБИ.049	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза неверного определения формата входных данных, поступающих в хранилище больших данных УБИ.050								Данная угроза не применяется к рассматриваемой АС
Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания УБИ.051	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения УБИ.052								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза невозможности управления правами пользователей BIOS УБИ.053	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
Угроза недобросовестного исполнения обязательств поставщиками облачных услуг УБИ.054								Данная угроза не применяется к рассматриваемой АС
Угроза незащищённого администрирования облачных услуг УБИ.055								Данная угроза не применяется к рассматриваемой АС
Угроза некачественного переноса инфраструктуры в облако УБИ.056								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза неконтролируемого копирования данных внутри хранилища больших данных УБИ.057								Данная угроза не применяется к рассматриваемой АС
Угроза неконтролируемого роста числа виртуальных машин УБИ.058								Данная угроза не применяется к рассматриваемой АС
Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.059								Данная угроза не применяется к рассматриваемой АС
Угроза неконтролируемого уничтожения информации хранилищем больших данных УБИ.060								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза некорректного задания структуры данных транзакции УБИ.061	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера УБИ.062								Данная угроза не применяется к рассматриваемой АС
Угроза некорректного использования функционала программного и аппаратного обеспечения УБИ.063	5	средняя	возможность использования декларированных возможностей программных и аппаратных средств определенным (нестандартным, некорректным) способом с целью деструктивного воздействия на автоматизированную систему и обрабатываемую ею информацию.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза неопределённости в распределении ответственности между ролями в облаке УБИ.065								Данная угроза не применяется к рассматриваемой АС
Угроза неопределённости ответственности за обеспечение безопасности облака УБИ.066								Данная угроза не применяется к рассматриваемой АС
Угроза неправомерного ознакомления с защищаемой информацией УБИ.067	5	низкая	Возможность неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами деструктивных целей.	2	0,35	Низкая	Низкая	Неактуальная
Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.068	5	низкая		5	0,5	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэф- фициент исходной защищенн ости (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы Y=(Y1+Y2) /20	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза неправомерных действий в каналах связи УБИ.069	5	низкая	Возможность несанкционированного доступа к сетевому трафику у нарушителя	5	0,25	Низкая	Низкая	Нектуальная
Угроза непрерывной модернизации облачной инфраструктуры УБИ.070								Данная угроза не применяется к рассматри- ваемой АС
Угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071	5	средня я	Удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных; Технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных;	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы Г.7

УБИ	Число-вой коэф- фициент исходной защищенн ости (Y1)	Частота (вероятность) реализации угрозы		Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS УБИ.072	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2 0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети УБИ.073							Данная угроза не применяется к рассматри- ваемой АС
Угроза несанкционированного доступа к аутентификационной информации УБИ.074	5	средня я	Возможность извлечения паролей, имён пользователей или других учётных данных из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации	2 0,5	Средняя	Средняя	Актуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к виртуальным каналам передачи УБИ.075								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети УБИ.076								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение УБИ.077								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети УБИ.078								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин УБИ.079								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети УБИ.080								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы УБИ.081								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к сегментам вычислительного поля УБИ.082								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к системе по беспроводным каналам УБИ.083								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети УБИ.084								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации УБИ.085								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного изменения аутентификационной информации УБИ.086	5	средняя	Возможность осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств.	2	0,5	Средняя	Средняя	Актуальная
Угроза несанкционированного использования привилегированных функций BIOS УБИ.087	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного копирования защищаемой информации УБИ.088	5	средняя	Возможность неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы).	5	0,5	Средняя	Средняя	Актуальная
Угроза несанкционированного редактирования реестра УБИ.089	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализации угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности и угрозы	Актуальность угрозы
Угроза несанкционированного создания учётной записи пользователя УБИ.090	5	низкая	Отсутствие прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного удаления защищаемой информации УБИ.091	5	низкая	Использование на АС базового проверенного набора ПО. Контроль со стороны ответственных за эксплуатацию ТС АС. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам УБИ.092								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного управления буфером УБИ.093	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного управления синхронизацией и состоянием УБИ.094	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации. Возможность изменения нарушителем последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состояния ИС, или в возможности модификации настроек и изменения режимов работы промышленных роботов, приводящих к вмешательству в производственный процесс и хищению хранящейся в памяти роботов информации (исходного кода, параметров продукции и др.).	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза несанкционированного управления указателями УБИ.095	5	низкая	Предоставление прав доступа к информационным ресурсам информационной системы по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несогласованности политик безопасности элементов облачной инфраструктуры УБИ.096								Данная угроза не применяется к рассматри- ваемой АС
Угроза несогласованности правил доступа к большим данным УБИ.097	5	низкая	Использования политик безопасности, согласованных между собой.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числово й коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы Y=(Y1+Y2) /20	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098	5	низкая	Возможность определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза обнаружения хостов УБИ.099	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика. Сканирование нарушителем вычислительной сети для выявления работающих сетевых узлов.	2	0,35	Низкая	Низкая	Неактуальная
Угроза обхода некорректно настроенных механизмов аутентификации УБИ.100	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации.	2	0,35	Низкая	Низкая	Неактуальная
Угроза общедоступности облачной инфраструктуры УБИ.101								Данная угроза не применяется к рассматриваемой АС
Угроза опосредованного управления группой программ через совместно используемые данные УБИ.102	5	низкая	Возможность опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные и др.)	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза определения типов объектов защиты УБИ.103	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика.	2	0,35	Низкая	Низкая	Неактуальная
Угроза определения топологии вычислительной сети УБИ.104	5	низкая	Наличие доверенного канала связи посредством СКЗИ Возможность определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз.	2	0,35	Низкая	Низкая	Неактуальная
Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных УБИ.105								Данная угроза не применяется к рассматриваемой АС
Угроза отказа в обслуживании системой хранения данных супер-компьютера УБИ.106								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза отключения контрольных датчиков УБИ.107								Данная угроза не применяется к рассматриваемой АС
Угроза ошибки обновления гипервизора УБИ.108								Данная угроза не применяется к рассматриваемой АС
Угроза перебора всех настроек и параметров приложения УБИ.109	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность получения нарушителем доступа к дополнительному скрытому функционалу или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перегрузки грид-системы вычислительными заданиями УБИ.110								Данная угроза не применяется к рассматриваемой АС
Угроза передачи данных по скрытым каналам УБИ.111								Данная угроза не применяется к рассматриваемой АС
Угроза передачи запрещённых команд на оборудование с числовым программным управлением УБИ.112								Данная угроза не применяется к рассматриваемой АС
Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники УБИ.113	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности и угрозы	Актуальность угрозы
Угроза переполнения целочисленных переменных УБИ.114	5	низкая	Отсутствие у внешнего нарушителя сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных. Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата вводимой и выводимой на периферийные устройства информации УБИ.115	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Отсутствие у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата данных, передаваемых по вычислительной сети УБИ.116	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности и угрозы	Актуальность угрозы
Угроза перехвата привилегированного потока УБИ.117	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата привилегированного процесса УБИ.118	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза перехвата управления гипервизором УБИ.119								Технология не применяется в данной АС
Угроза перехвата управления средой виртуализации УБИ.120								Технология не применяется в данной АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза повреждения системного реестра УБИ.121	5	низкая	Возникновение ошибок в работе отдельных процессов или всей операционной системы. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2 0,35	Низкая	Низкая	Неактуальная
Угроза повышения привилегий УБИ.122	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2 0,35	Низкая	Низкая	Неактуальная
Угроза подбора пароля BIOS УБИ.123	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2 0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы Y=(Y1+Y2) /20	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опасности угрозы	Актуальность угрозы
Угроза подделки записей журнала регистрации событий УБИ.124	5	низкая	Технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза подключения к беспроводной сети в обход процедуры аутентификации УБИ.125								Данная угроза не применяется к рассматри- ваемой АС
Угроза подмены беспроводного клиента или точки доступа УБИ.126								Данная угроза не применяется к рассматри- ваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализации угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза подмены действия пользователя путём обмана УБИ.127	5	низкая	Применение методов борьбы с социальной инженерией. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза подмены доверенного пользователя УБИ.128	5	низкая	Возможность нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная
Угроза подмены резервной копии программного обеспечения BIOS УБИ.129	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Отсутствие возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии ПО BIOS/UEFI, предварительно подменённой нарушителем.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербаль-ная интерпретация реализуемости угрозы	Вербаль-ный показатель опасности и угрозы	Актуальность угрозы
Угроза подмены содержимого сетевых ресурсов УБИ.130								Данная угроза не применяется к рассматриваемой АС
Угроза подмены субъекта сетевого доступа УБИ.131								Данная угроза не применяется к рассматриваемой АС
Угроза получения предварительной информации об объекте защиты УБИ.132								Данная угроза не применяется к рассматриваемой АС
Угроза получения сведений о владельце беспроводного устройства УБИ.133								Данная угроза не применяется к рассматриваемой АС
Угроза потери доверия к поставщику облачных услуг УБИ.134								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза потери и утечки данных, обрабатываемых в облаке УБИ.135								Данная угроза не применяется к рассматриваемой АС
Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных УБИ.136								Данная угроза не применяется к рассматриваемой АС
Угроза потери управления облачными ресурсами УБИ.137								Данная угроза не применяется к рассматриваемой АС
Угроза потери управления собственной инфраструктурой при переносе её в облако УБИ.138								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза преодоления физической защиты УБИ.139	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Контроль физического доступа (наличие замков в помещении, обученный проинструктированный персонал и т.п.). Отсутствие возможности любого из методов проникновения на объект	2	0,35	Низкая	Низкая	Неактуальная
Угроза приведения системы в состояние «отказ в обслуживании» УБИ.140	5	низкая	Возможность отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой или при использовании недостатков реализации сетевых протоколов.	2	0,35	Низкая	Низкая	Неактуальная
Угроза привязки к поставщику облачных услуг УБИ.141								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.143	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза программного сброса пароля BIOS УБИ.144	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС. Отсутствие в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля	2	0,35	Низкая	Низкая	Неактуальная
Угроза пропуска проверки целостности программного обеспечения УБИ.145	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	Низкая	Низкая	Неактуальная
Угроза прямого обращения к памяти вычислительного поля супер-компьютера УБИ.146								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза распространения несанкционированно повышенных прав на всю грид-систему УБИ.147								Данная угроза не применяется к рассматриваемой АС
Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных УБИ.148								Данная угроза не применяется к рассматриваемой АС
Угроза сбоя обработки специальным образом изменённых файлов УБИ.149	5	низкая	Отсутствие у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке;	2	0,35	Низкая	Низкая	Неактуальная
Угроза сбоя процесса обновления BIOS УБИ.150	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы	
Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL УБИ.151	5	низкая	Наличие доверенного канала связи посредством СКЗИ Возможность получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера.	2	0,35	Низкая	Низкая	Неактуальная
Угроза удаления аутентификационной информации УБИ.152	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов УБИ.153	5	низкая	Отсутствие у нарушителя сведений о сетевом адресе дискредитируемой системы.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза установки уязвимых версий обновления программного обеспечения BIOS УБИ.154	5	низкая	Установка и использование проверенного ПО. Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
Угроза утраты вычислительных ресурсов УБИ.155	5	низкая	Отсутствие у нарушителя сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы	2	0,35	Низкая	Низкая	Неактуальная
Угроза утраты носителей информации УБИ.156	5	низкая	Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.157	5	низкая	Отсутствие возможности получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.) Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
Угроза форматирования носителей информации УБИ.158	5	низкая	Создание резервных копий информации, хранящейся на носителях.	2	0,35	Низкая	Низкая	Неактуальная
Угроза «форсированного веб-браузинга» УБИ.159								

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.160	5	низкая	Отсутствие у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации. Контроль со стороны ответственных за эксплуатацию ТС ИС.	2 0,35	Низкая	Низкая	Неактуальная
Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями УБИ.161							Данная угроза не применяется к рассматриваемой АС
Угроза эксплуатации цифровой подписи программного кода УБИ.162	5	низкая	В системах не используются цифровые подписи кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма прописывания программного кода	2 0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перехвата исключения/сигнала из привилегированного блока функций УБИ.163	5	низкая	Предоставление прав доступа к информационным ресурсам АС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре УБИ.164								Данная угроза не применяется к рассматриваемой АС
Угроза включения в проект не достоверно испытанных компонентов УБИ.165	5	низкая	Для применения в системе выбираются компоненты в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Использование сертифицированного ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза внедрения системной избыточности УБИ.166	5	низкая	Отсутствие избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект) программного обеспечения (или системы в целом).	2	0,35	Низкая	Низкая	Неактуальная
Угроза заражения компьютера при посещении неблагонадёжных сайтов УБИ.167								Данная угроза не применяется к рассматриваемой АС
Угроза «кражи» учётной записи доступа к сетевым сервисам УБИ.168								Данная угроза не применяется к рассматриваемой АС
Угроза наличия механизмов разработчика УБИ.169	5	низкая	Использование проверенного ПО, не подразумевающего использования отладочных механизмов	2	0,35	Низкая	Низкая	Неактуальная
Угроза неправомерного шифрования информации	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза скрытного включения вычислительного устройства в состав бот-сети УБИ.171								Данная угроза не применяется к рассматриваемой АС
Угроза распространения «почтовых червей» УБИ.172								Данная угроза не применяется к рассматриваемой АС
Угроза «спама» веб-сервера УБИ.173								Данная угроза не применяется к рассматриваемой АС
Угроза «фарминга» УБИ.174								Данная угроза не применяется к рассматриваемой АС
Угроза «фишинга» УБИ.175								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты УБИ.176	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная
Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью УБИ.177	5	низкая	Отсутствие (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора»	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного использования системных и сетевых утилит УБИ.178	5	низкая	Предоставление прав пользователю в минимально достаточном объеме. Отсутствие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему, предназначенных для использования администратором для диагностики и обслуживания системы	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированной модификации защищаемой информации УБИ.179	5	низкая	Предоставление прав пользователю в минимально достаточном объеме. Контроль со стороны ответственных за эксплуатацию ТС ИС. Использование доверенного канала связи СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
Угроза отказа подсистемы обеспечения температурного режима УБИ.180	5	низкая	Реализация угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение/вывод из строя компонентов подсистемы.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перехвата одноразовых паролей в режиме реального времени УБИ.181	5	низкая	Отсутствие у нарушителя сведений об информации идентификации/аутентификации дискредитируемого пользователя условно-постоянного действия	2	0,35	Низкая	Низкая	Неактуальная
Угроза физического устаревания аппаратных компонентов УБИ.182	5	низкая	Невозможность осуществления нарушителем перехвата трафика между системой и пользователем, ввиду использования доверенного канала связи СКЗИ	5	0,5	Средняя	Средняя	Актуальная
			Возможность нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды .					

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза перехвата управления автоматизированной системой управления техно-логическими процессами УБИ.183								Данная угроза не применяется к рассматриваемой АС
Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства УБИ.184								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного изменения параметров настройки средств защиты информации УБИ.185	5	низкая	Отсутствие СЗИ, вследствие этого отсутствие у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	2	0,35	Низкая	Низкая	Неактуальная
Угроза внедрения вредоносного кода через рекламу, сервисы и контент УБИ.186								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного воздействия на средство защиты информации УБИ.187	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза подмены программного обеспечения УБИ.188								Данная угроза не применяется к рассматриваемой АС
Угроза маскирования действий вредоносного кода УБИ.189	5	низкая		2	0,35	Низкая	Низкая	Неактуальная
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет УБИ.190								Данная угроза не применяется к рассматриваемой АС
Угроза внедрения вредоносного кода в дистрибутив программного обеспечения УБИ.191	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объеме	2	0,35	Низкая	Низкая	Неактуальная
Угроза использования уязвимых версий программного обеспечения УБИ.192	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объеме	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика УБИ.193	5	низкая	Использование на АС базового проверенного набора ПО. Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
Угроза несанкционированного использования привилегированных функций мобильного устройства УБИ.194								Данная угроза не применяется к рассматриваемой АС
Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.195								Данная угроза не применяется к рассматриваемой АС
Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве УБИ.196								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы		Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза хищения аутентификационной информации из временных файлов cookie УБИ.197	5	низкая	Использование на АС базового проверенного набора ПО.	2	0,35	Низкая	Неактуальная
Угроза скрытной регистрации вредоносной программой учетных записей администраторов УБИ.198	5	низкая	Использование на АС базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объеме	2	0,35	Низкая	Неактуальная
Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.199							Данная угроза не применяется к рассматриваемой АС
Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.200							Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере УБИ.201								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированной установки приложений на мобильные устройства УБИ.202								Данная угроза не применяется к рассматриваемой АС
Угроза утечки информации с не подключенных к сети Интернет компьютеров УБИ.203								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров УБИ.204								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы Y=(Y1+Y2)/20	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты УБИ.205	5	низкая	Возможность нарушения работы компьютера и отказа в доступе к его данным за счет ошибочного блокирования средством защиты информации файлов.	2	0,35	Низкая	Низкая	Неактуальная
Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем УБИ.206								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей) УБИ.207								Данная угроза не применяется к рассматриваемой АС
Угроза не целевого использования вычислительных ресурсов средства вычислительной техники УБИ.208								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза несанкционированного доступа к защищаемой памяти ядра процессора УБИ.209								Данная угроза не применяется к рассматриваемой АС
Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения УБИ.210								Данная угроза не применяется к рассматриваемой АС
Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем УБИ.211								Данная угроза не применяется к рассматриваемой АС
Угроза перехвата управления информационной системой УБИ.212								Данная угроза не применяется к рассматриваемой

Продолжение таблицы Г.7

УБИ	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы $Y=(Y1+Y2)/20$	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
Угроза обхода многофакторной аутентификации УБИ.213								Данная угроза не применяется к рассматриваемой АС
Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации УБИ.214								Данная угроза не применяется к рассматриваемой АС
Угроза несанкционированного доступа к системе при помощи сторонних сервисов УБИ.215								Данная угроза не применяется к рассматриваемой АС
Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах УБИ.216								Данная угроза не применяется к рассматриваемой АС

Продолжение таблицы Г.7

УБИ	Числовой коэф- фициент исходной защищен- ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи- циент реализуе- мости угрозы $Y=(Y1+Y2)/20$	Вербаль- ная интерпре- тация реализуе- мости угрозы	Вербаль- ный показа- тель опаснос- ти угрозы	Актуальность угрозы
Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения УБИ.217								Данная угроза не применяется к рассматри- ваемой АС

Для нейтрализации (устранения, затруднения реализации) данных угроз необходимо применять организационные и программно – технические меры защиты информации.

В качестве организационных мер должны быть реализованы и исполняться:

- порядок учета машинных носителей;
- правила действующей на предприятии разрешительной системы допуска и доступа и действующие правила работы в информационных системах.

В качестве программно – технических мер защиты информации необходимо применять сертифицированные по требованиям безопасности информации:

- средства защиты информации от НСД;
- межсетевые экраны;
- средства антивирусной защиты;
- средства анализа защищенности;
- средства криптографической защиты информации.

Главный инженер:

_____	ФИО
_____	ФИО
_____	ФИО
_____	ФИО
_____	ФИО
_____	ФИО

Приложение Д

(обязательное)

Акт классификации АС на базе серверного парка КС АО «ФНПЦ «ПО
«Старт» им. М.В.Проценко»

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

АКТ

классификации информационной системы персональных данных
(автоматизированная система на базе серверного парка корпоративной сети) АО
«ФНПЦ «ПО «Старт» им. М.В. Проценко»

г. Заречный

Д.1 Общие положения

Наименование информационной системы: Информационная система (ИС) персональных данных АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» (автоматизированная система на базе серверного парка корпоративной сети).

Назначение ИС: Обработка, хранение, печать и передача по каналам связи информации следующих степеней конфиденциальности: «несекретно», «для служебного пользования», «коммерческая тайна» «персональные данные».

Д.2 Исходные данные об ИС:

Цели обработки защищаемой информации – осуществление обработки информации для обеспечения непрерывности бизнес-процессов предприятия.

Категория субъектов – сотрудники АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», субъекты, не являющихся сотрудниками АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Оператор ИС – АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Д.3 Определение класса защищенности информационной системы:

Определение степени возможного ущерба для обладателя информации (АО «ФНПЦ «ПО «Старт» им. М.В. Проценко») от нарушения конфиденциальности, целостности или доступности информации.

Степень ущерба - [(конфиденциальность) (целостность) (доступность)] = низкая, так как в результате нарушения всех свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Определение уровня значимости информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень

ущерба) (доступность, степень ущерба)] = [(конфиденциальность, степень ущерба = средняя) (целостность, степень ущерба = средняя) (доступность, степень ущерба = средняя)] = УЗ 2 = средний уровень значимости, т.к. для всех свойств безопасности информации (конфиденциальности, целостности, доступности) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» определены средние степени ущерба.

Определение масштаба системы

Информационная система имеет объектовый масштаб, т.к. она функционирует на объектах одной организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Определение класса защищенности информационной системы

Класс защищенности информационной системы определяется в соответствии с таблицей Д.1.

Таблица Д.1. – Определение класса защищенности

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ1	К1	К1	К1
УЗ2	К1	К2	К2
УЗ3	К2	К3	К3
УЗ4	К3	К3	К4

Класс защищенности информационной системы (К) = [уровень значимости информации; масштаб системы] = [УЗ 2; объектовый масштаб] = К2 (второй класс).

Главный инженер:

ФИО

ФИО

ФИО

ФИО

Приложение Е

(обязательное)

Техническое задание на разработку системы защиты информации АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА РАЗРАБОТКУ СИСТЕМЫ ЗАЩИТЫ
ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА БАЗЕ
СЕРВЕРНОГО ПАРКА КОРПОРАТИВНОЙ СЕТИ АО «ФНПЦ «ПО «СТАРТ»
ИМ. М.В. ПРОЦЕНКО»

г. Заречный

Е.1 Общие положения

При создании (модернизации), эксплуатации и выводе из эксплуатации автоматизированной системы (далее — АС) должны выполняться требования законодательства Российской Федерации в области защиты информации. Требования к защите информации задаются в рамках частного технического задания на создание (развитие или модернизацию) системы защиты информации автоматизированной системы, разрабатываемого с учетом ГОСТ 34.602 и ГОСТ Р 51583.

Защита информации в автоматизированной системе достигается путем принятия в рамках системы защиты автоматизированной системы совокупности организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление штатного режима функционирования автоматизированной системы управления в случае реализации угроз безопасности информации.

Формирование требований к защите информации в автоматизированной системе осуществляется с учетом ГОСТ Р 51583 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения", ГОСТ Р 51624 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования" и стандартов организации и в том числе включает:

- принятие решения о необходимости защиты информации в автоматизированной системе; классификацию автоматизированной системы по требованиям защиты информации;

- определение угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы, и разработку на их основе модели угроз безопасности информации;

- определение требований к системе защиты автоматизированной системы управления.

Е.2 Цели и задачи обеспечения защиты информации в АС

Целью обеспечения защиты информации в АС является обеспечение доступности, конфиденциальности и целостности информации, обрабатываемой в АС.

Задачами обеспечения защиты информации в АС являются:

- предотвращение НСД, уничтожения, искажения, копирования, блокирования защищаемой информации;

- резервирование элементов системы;

- регулирование доступа к элементам системы и защищаемой информации;

- защита от информационного воздействия на технические средства обработки;

- обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности;

- фиксация всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем обработки информации, относящихся к защите информации;

- предотвращение утечки и утраты информации;

- сохранение конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Е.3 Класс защищенности АС

В соответствии с положениями приказа ФСТЭК России № 17 от 11 февраля 2013 г. АС присвоен класс защищённости «К2».

Е.4 Перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система АС должна соответствовать следующим документам:

- ГОСТ 34.003-90 Автоматизированные системы. Термины и определения;
- ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы;
- ГОСТ 34.603-92 Виды испытаний автоматизированных систем;
- ГОСТ 34.601-90 Автоматизированные системы. Стадии создания;
- ГОСТ 34.201-89 Виды, комплектность и обозначения документов при создании автоматизированных систем;
- РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов;
- Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21);
- Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).

Е.5 Объекты защиты АС

- защищаемая информация (для служебного пользования, персональные данные);

- технологическая информация:
 - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
 - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
 - информация на съемных носителях информации (съемные жесткие магнитные диски), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
 - информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;
 - информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
 - служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации;
- программно-технические средства обработки:
 - общесистемное и специальное программное обеспечение (операционные системы и другие);
 - резервные копии общесистемного программного обеспечения;
 - инструментальные средства и утилиты систем управления ресурсами АС;
 - аппаратные средства обработки информации;
- средства защиты информации:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- объекты и помещения, в которых размещены компоненты АС.

Е.6 Требования к мерам и средствам защиты информации, применяемым в АС

Меры и средства защиты информации, применяемые в АС, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа (присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности));
- управление доступом субъектов доступа к объектам доступа (управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в АС правил разграничения доступа, обеспечение контроля соблюдения этих правил);
- ограничение программной среды (установка и (или) запуск только разрешенного к использованию в АС ПО или исключение возможности установки и (или) запуска запрещенного к использованию в АС ПО);
- защиту машинных носителей информации (исключение возможности несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированного использования съемных машинных носителей информации);

— регистрацию событий безопасности (сбор, запись, хранение и защита информации о событиях безопасности в АС, а также просмотр и анализ информации о таких событиях и реагирование на них);

— антивирусную защиту (обнаружение в АС компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, и реагирование на обнаружение этих программ и информации);

— обнаружение (предотвращение) вторжений (обнаружение действий в АС, направленных на преднамеренный НСД к информации, специальные воздействия на АС и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, и реагирование на эти действия);

— целостность АС и информации (обнаружение фактов несанкционированного нарушения целостности АС и содержащихся в ней данных, а также возможность восстановления АС);

— защиту технических средств и оборудования (исключение НСД к стационарным техническим средствам, обрабатывающим информацию, исполнительным устройствам, средствам, обеспечивающим функционирование АС и в помещения, в которых они постоянно расположены, обеспечение защиты технических средств от внешних воздействий, а также защиты информации, представленной в виде информативных электрических сигналов и физических полей);

— защиту автоматизированной системы и ее компонентов (защита информации при ее передаче по каналам связи, взаимодействии АС или ее отдельных сегментов с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями посредством

применения архитектуры АС и проектных решений по ее системе защиты, направленных на обеспечение защиты информации);

- планирование мероприятий по обеспечению защиты информации (разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в АС, в том числе предусматривающего мероприятия по защите информации в ходе создания, эксплуатации и вывода из эксплуатации АС, сроки выполнения мероприятий и ответственных за их выполнение, а также контроль его выполнения);

- обеспечение действий в нештатных (непредвиденных) ситуациях (планирование мероприятий, обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций, а также резервирование программного обеспечения, технических средств, каналов передачи данных АС в случае возникновения нештатных (непредвиденных) ситуаций и обеспечение возможности ее восстановления);

- информирование и обучение персонала (информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты АС и отдельных средств защиты информации, а также теоретическое и практическое обучение по эксплуатации системы защиты АС и отдельных средств защиты информации);

- выявление инцидентов и реагирование на них (обнаружение, идентификация, анализ инцидентов в АС, а также принятие мер по устранению и предупреждению инцидентов);

- управление конфигурацией АС и ее системы защиты (управление изменениями конфигурации АС и ее системы защиты информации, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений).

Е.7 Требования к защите информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями

Требования к защите информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями включают:

- взаимодействие с иными автоматизированными(информационными) системами и информационно-телекоммуникационными сетями осуществляется с использованием межсетевого экранирования;
- при взаимодействии АС с информационно-телекоммуникационными сетями международного информационного обмена должны использоваться межсетевые экраны не ниже 3 класса и не ниже 4 класса в случае отсутствия такого взаимодействия.

Е.8 Требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации

Требования к поставляемым техническим средствам, программному обеспечению и средствам защиты информации включают:

- программное обеспечение должно быть совместимым с программным обеспечением АС и не должно снижать требуемый уровень защищенности информации на объекте информатизации;
- программно-технические средства и средства защиты информации, должны быть совместимы между собой и не должны снижать уровень защищенности информации на объекте информатизации;
- программно-технические средства и средства защиты информации должны быть сертифицированными ФСТЭК России;
- обновления программного обеспечения должны быть безопасно получены, проверены и установлены на компонентах АС;

- поставляемые технические средства, ПО и средства защиты должны быть укомплектованы инструкциями по установке и эксплуатации;
- технические средства, программное обеспечение и средства защиты информации должны поставляться с комплектами соответствующих лицензий на использование;
- программное обеспечение должно проходить контроль отсутствия недекларированных возможностей и отсутствия влияния на корректность работы средств защиты информации.

Е.9 Функции заказчика и оператора по обеспечению защиты информации в АС

Функции заказчика по обеспечению защиты информации в АС:

- своевременное финансирование работ по обеспечению защиты информации в АС;
- проведение предварительных испытаний АС;
- создание необходимых для функционирования АС подразделений и служб;
- определение подразделений и должностных лиц, ответственных за проведение опытной эксплуатации и постоянной эксплуатации.

Функции оператора по обеспечению защиты информации в АС:

- пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;
- регистрация событий, связанных с действиями от имени привилегированных учетных записей (администраторов) и событий, связанных с изменением привилегий учетных записей;
- обеспечение антивирусной защиты на этапе инициализации микропрограммного обеспечения средства вычислительной техники;

- хранение информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации;

- применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках;

- применение автоматизированных средств для обнаружения в информационной системе неразрешенного программного обеспечения (компонентов программного обеспечения) и уведомления об этом уполномоченных должностных лиц (администратора безопасности);

- анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в информационной системе для нарушения безопасности информации.

Е.10 Стадии (этапы работ) создания системы защиты АС

Система защиты АС находится на этапе разработки технического задания для её дальнейшего проектирования.

Е.11 Требования к сертифицированным средствам защиты информации

С учетом использования в АС сертифицированных по требованиям безопасности информации средств защиты информации, класс средств защиты должен быть следующим:

- средства вычислительной техники не ниже 5 класса;

- межсетевые экраны не ниже 3 класса в случае взаимодействия автоматизированной системы управления с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия такого взаимодействия;

- должны применяться средства защиты информации, программное обеспечение которых прошло проверку не ниже, чем по 4 уровню контроля отсутствия недеklarированных возможностей;

— заказчиком (оператором) в зависимости от потенциала нарушителя может приниматься решение о повышении уровня контроля отсутствия недекларированных возможностей в программном обеспечении средств защиты информации.

Е.12 Необходимые меры защиты информации в АС

Адаптированный базовый набор мер защиты информации АС приведен в таблице Е.1.

Таблица Е.1 — Адаптированный базовый набор мер защиты информации в АС

Условное обозначение и номер меры	Меры защиты информации в АС
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых символов (защита обратной связи при вводе аутентификационной информации)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (экранирование, фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления

Продолжение таблицы Е.1

Условное обозначение и номер меры	Меры защиты информации в АС
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование автоматизированной системы управления
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС)	
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

Продолжение таблицы Е.1

Условное обозначение и номер меры	Меры защиты информации в АС
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	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
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений
СОВ.2	Обновление базы решающих правил
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей

Продолжение таблицы Е.1

Условное обозначение и номер меры	Меры защиты информации в АС
IX. Обеспечение целостности (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
X. Обеспечение доступности (ОДТ)	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, исполнительные устройства и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита автоматизированной системы и ее компонентов (ЗИС)	
ЗИС.1	Разделение функций по управлению (администрированию) автоматизированной системой управления, управлению (администрированию) системой защиты, функций по обработке информации и иных функций автоматизированной системы управления
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

Продолжение таблицы Е.1

Условное обозначение и номер меры	Меры защиты информации в АС
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации
ЗИС.17	Разбиение автоматизированной системы управления на сегменты (сегментирование) и обеспечение защиты периметров сегментов
ЗИС.22	Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании
ЗИС.23	Защита периметра (физических и (или) логических границ) автоматизированной системы управления при ее взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями
XIV. Обеспечение безопасной разработки программного обеспечения (ОБР)	
ОБР.0	Разработка правил и процедур (политик) обеспечения безопасной разработки программного обеспечения
ОБР.1	Анализ уязвимостей и угроз безопасности информации в ходе разработки программного обеспечения
ОБР.2	Статический анализ кода программного обеспечения в ходе разработки программного обеспечения
ОБР.4	Тестирование на проникновение в ходе разработки программного обеспечения
ОБР.5	Динамический анализ кода программного обеспечения в ходе разработки программного обеспечения
ОБР.6	Документирование процедур обеспечения безопасной разработки программного обеспечения разработчиком и представление их заказчику (оператору)

Продолжение таблицы Е.1

Условное обозначение и номер меры	Меры защиты информации в АС
XV. Управление обновлениями программного обеспечения (ОПО)	
ОПО.0	Разработка правил и процедур (политик) управления обновлениями программного обеспечения (включая получение, проверку и установку обновлений)
ОПО.1	Получение обновлений программного обеспечения от разработчика или уполномоченного им лица
ОПО.2	Тестирование обновлений программного обеспечения до его установки на макете или в тестовой зоне
XVI. Планирование мероприятий по обеспечению защиты информации (ПЛН)	
ПЛН.0	Разработка правил и процедур (политик) планирования мероприятий по обеспечению защиты информации
ПЛН.1	Определение лиц, ответственных за планирование, реализацию и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления
ПЛН.2	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в автоматизированных системах управления
ПЛН.3	Контроль выполнения мероприятий по обеспечению защиты информации в автоматизированных системах управления, предусмотренных утвержденным планом
XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	
ДНС.0	Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденных) ситуациях
ДНС.1	Разработка плана действий на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.2	Обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.4	Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированных систем управления на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.5	Обеспечение возможности восстановления автоматизированной системы управления и (или) ее компонент в случае возникновения нештатных (непредвиденных) ситуаций

Продолжение таблицы Е.1

XVIII. Информирование и обучение персонала (ИПО)	
ИПО.0	Разработка правил и процедур (политик) информирования и обучения персонала
ИПО.1	Информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
ИПО.2	Обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
ИПО.3	Проведение практических занятий с персоналом по правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
XIX. Анализ угроз безопасности информации и рисков от их реализации (УБИ)	
УБИ.0	Разработка правил и процедур (политик) анализа угроз безопасности информации и рисков от их реализации
УБИ.1	Периодический анализ изменения угроз безопасности информации, возникающих в ходе эксплуатации автоматизированной системы управления
УБИ.2	Периодическая переоценка последствий от реализации угроз безопасности информации (анализ риска)
XX. Выявление инцидентов и реагирование на них (ИНЦ)	
ИНЦ.0	Разработка правил и процедур (политик) выявления инцидентов и реагирования на них
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ.5	Принятие мер по устранению последствий инцидентов
ИНЦ.6	Планирование и принятие мер по предотвращению повторных инцидентов
XXI. Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)	
УКФ.0	Разработка правил и процедур (политик) управления конфигурацией автоматизированной системы управления и ее системы защиты
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию автоматизированной системы управления и ее системы защиты
УКФ.2	Управление изменениями конфигурации автоматизированной системы управления и ее системы защиты

Продолжение таблицы Е.1

Условное обозначение и номер меры	Меры защиты информации в АС
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации автоматизированной системы управления и системы защиты на обеспечение защиты информации и согласование изменений в конфигурации автоматизированной системы управления с должностным лицом (работником), ответственным за обеспечение безопасности автоматизированной системы управления
УКФ.4	Документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и ее системы защиты
УКФ.5	Регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления

Приложение Ж
(обязательное)

Технический проект на создание системы защиты информации АС на базе
серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

ТЕХНИЧЕСКИЙ ПРОЕКТ НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ
ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА БАЗЕ
СЕРВЕРНОГО ПАРКА КОРПОРАТИВНОЙ СЕТИ АО «ФНПЦ «ПО «СТАРТ»
ИМ. М.В. ПРОЦЕНКО»

г. Заречный

Ж.1 Общие положения

При создании (модернизации), эксплуатации и выводе из эксплуатации автоматизированной системы (далее — АС) должны выполняться требования законодательства Российской Федерации в области защиты информации. Требования к защите информации задаются в рамках частного технического задания на создание (развитие или модернизацию) системы защиты информации автоматизированной системы, разрабатываемого с учетом ГОСТ 34.602 и ГОСТ Р 51583.

Защита информации в автоматизированной системе достигается путем принятия в рамках системы защиты автоматизированной системы совокупности организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление штатного режима функционирования автоматизированной системы управления в случае реализации угроз безопасности информации.

Формирование требований к защите информации в автоматизированной системе осуществляется с учетом ГОСТ Р 51583 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения", ГОСТ Р 51624 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования" и стандартов организации и в том числе включает:

— принятие решения о необходимости защиты информации в автоматизированной системе; классификацию автоматизированной системы по требованиям защиты информации;

- определение угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы, и разработку на их основе модели угроз безопасности информации;

- определение требований к системе защиты автоматизированной системы управления.

Ж.2 Цели и задачи обеспечения защиты информации в АС

Целью обеспечения защиты информации в АС является обеспечение доступности, конфиденциальности и целостности информации, обрабатываемой в АС.

Задачами обеспечения защиты информации в АС являются:

- предотвращение НСД, уничтожения, искажения, копирования, блокирования защищаемой информации;

- резервирование элементов системы;

- регулирование доступа к элементам системы и защищаемой информации;

- защита от информационного воздействия на технические средства обработки;

- обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности;

- фиксация всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем обработки информации, относящихся к защите информации;

- предотвращение утечки и утраты информации;

- сохранение конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Ж.3 Общие сведения об АС

Объект представляет собой АС, расположенную по адресу: город Заречный, Пензенской области, пр. Мира 1.

Сервера АС размещены в помещении предприятия, в пределах КЗ.

АС предназначена для обработки, хранения и передачи информации следующих степеней конфиденциальности: для служебного пользования, коммерческая тайна, персональные данные, а также несекретной информации.

Класс защищённости АС, как ИС– К2.

Уровень защищённости АС, как ИСПДн – 3.

Режим работы в АС – многопользовательский, пользователи имеют различные права доступа к ресурсам АС.

АС включает в себя центр обработки данных предприятия (ЦОД) – серверный парк корпоративной сети предприятия, не имеющий подключений к информационно-телекоммуникационным сетям международного информационного обмена.

ЦОД АС функционируют на блейд-серверах. Сервисы представлены в таблице Ж.1.

Таблица Ж.1 – Перечень сервисов

Сервис	Описание
dns	DNS-сервер
fs	Файловый сервис
intuit	Система дистанционного обучения
mail	Почтовый сервер
nagios	Сервис мониторинга
otrs	Система обработки заявок
replica	Сервис перекачки данных
sites	Корпоративные сайты
spd	Сервис подготовки данных
tomcat	Сервис формирования pdf
ad1	Контроллер домена

Продолжение таблицы Ж.1

Сервис	Описание
ad2	Контроллер домена
alfresco	Электронный документооборот
backup	Сервис резервного копирования
ca	Удостоверяющий центр
cmdb	Система инвентаризации
consultant	Информационно-правовая система Консультант
dns	DNS-сервер
dts	Сервер разработки
fa	Файловый сервис
homes	Сервер пользовательских данных
jabber	Сервер обмена сообщений
ksu	Корпоративная система управления
ldap	Ldap сервер
pgsqlddb	Сервер БД разработки задач КСУ
pgsqldts	Сервер приложений
redmine	Система управления проектами
sites	Корпоративные сайты
svn	Система контроля версий
tally	Сервис печати

Все сервера корпоративной сети предприятия соединены посредством сетевых Blade-коммутаторов третьего уровня для внутренней сети и расположены в одной подсети. Подключение АП корпоративной сети предприятия к сервисам ЦОД осуществляется при помощи сетевых Blade-коммутаторов третьего уровня для внешней сети.

Антивирусная защита реализована как в базовых ОС, так и в гостевых ОС ЦОД, с применением антивирусного ПО, сертифицированного ФСТЭК по требованиям безопасности информации.

АС предназначена для обработки, хранения, передачи информации по каналам связи с целью решения производственных задач на предприятии.

Технологический процесс обработки информации в АС:

— администратор АС проходит процедуру авторизации в системе;

- администратор АС запускает прикладное ПО, СЗИ от НСД;
- администратор АС выполняет необходимые действия по администрированию в рамках производственных задач.

Ж.4 Перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система

АС должна соответствовать следующим документам:

- ГОСТ 34.003-90 Автоматизированные системы. Термины и определения;
- ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы;
- ГОСТ 34.603-92 Виды испытаний автоматизированных систем;
- ГОСТ 34.601-90 Автоматизированные системы. Стадии создания;
- ГОСТ 34.201-89 Виды, комплектность и обозначения документов при создании автоматизированных систем;
- РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов;
- Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21);
- Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).

Ж.5 Объекты защиты АС

- защищаемая информация (для служебного пользования, персональные данные);

- технологическая информация:
 - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
 - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
 - информация на съемных носителях информации (съемные жесткие магнитные диски), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
 - информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;
 - информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
 - служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации;
- программно-технические средства обработки:
 - общесистемное и специальное программное обеспечение (операционные системы и другие);
 - резервные копии общесистемного программного обеспечения;
 - инструментальные средства и утилиты систем управления ресурсами АС;
 - аппаратные средства обработки информации;
- средства защиты информации:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- объекты и помещения, в которых размещены компоненты АС.

Ж.6 Требования к мерам и средствам защиты информации, применяемым в АС

Меры и средства защиты информации, применяемые в АС, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа (присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности));
- управление доступом субъектов доступа к объектам доступа (управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в АС правил разграничения доступа, обеспечение контроля соблюдения этих правил);
- ограничение программной среды (установка и (или) запуск только разрешенного к использованию в АС ПО или исключение возможности установки и (или) запуска запрещенного к использованию в АС ПО);
- защиту машинных носителей информации (исключение возможности несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированного использования съемных машинных носителей информации);

— регистрацию событий безопасности (сбор, запись, хранение и защита информации о событиях безопасности в АС, а также просмотр и анализ информации о таких событиях и реагирование на них);

— антивирусную защиту (обнаружение в АС компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, и реагирование на обнаружение этих программ и информации);

— обнаружение (предотвращение) вторжений (обнаружение действий в АС, направленных на преднамеренный НСД к информации, специальные воздействия на АС и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, и реагирование на эти действия);

— целостность АС и информации (обнаружение фактов несанкционированного нарушения целостности АС и содержащихся в ней данных, а также возможность восстановления АС);

— защиту технических средств и оборудования (исключение НСД к стационарным техническим средствам, обрабатывающим информацию, исполнительным устройствам, средствам, обеспечивающим функционирование АС и в помещения, в которых они постоянно расположены, обеспечение защиты технических средств от внешних воздействий, а также защиты информации, представленной в виде информативных электрических сигналов и физических полей);

— защиту автоматизированной системы и ее компонентов (защита информации при ее передаче по каналам связи, взаимодействии АС или ее отдельных сегментов с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями посредством

применения архитектуры АС и проектных решений по ее системе защиты, направленных на обеспечение защиты информации);

— планирование мероприятий по обеспечению защиты информации (разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в АС, в том числе предусматривающего мероприятия по защите информации в ходе создания, эксплуатации и вывода из эксплуатации АС, сроки выполнения мероприятий и ответственных за их выполнение, а также контроль его выполнения);

— обеспечение действий в нештатных (непредвиденных) ситуациях (планирование мероприятий, обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций, а также резервирование программного обеспечения, технических средств, каналов передачи данных АС в случае возникновения нештатных (непредвиденных) ситуаций и обеспечение возможности ее восстановления);

— информирование и обучение персонала (информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты АС и отдельных средств защиты информации, а также теоретическое и практическое обучение по эксплуатации системы защиты АС и отдельных средств защиты информации);

— выявление инцидентов и реагирование на них (обнаружение, идентификация, анализ инцидентов в АС, а также принятие мер по устранению и предупреждению инцидентов);

— управление конфигурацией АС и ее системы защиты (управление изменениями конфигурации АС и ее системы защиты информации, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений).

Ж.7 Требования к системе защиты информации АС

Система защиты информации предусматривает комплекс

организационных, программных, технических, в том числе, криптографических средств и мер по защите информации при автоматизированной обработке и хранении информации, при ее передаче по линиям связи, учете и обращении накопителей и носителей информации на любой основе.

Создаваемая система защиты информации является дифференцированной:

- использует различные методы и способы обеспечения безопасности информации на всех технологических этапах её обработки и во всех режимах функционирования технических средств и систем;

- представляет собой согласованный комплекс организационных мероприятий, программных, технических и программно-технических мер, направленных на обеспечение информационной безопасности ресурсов АС;

- существенно затрудняет реализацию потенциальных угроз информационной безопасности ресурсов АС. При невозможности использования мер по предотвращению реализации угроз информационной безопасности, СЗИ АС реализует механизмы, позволяющие своевременно обнаружить несанкционированную деятельность и локализовать ее источник (субъект, канал воздействия).

В рамках реализации организационных мер защиты у владельца АС должны быть в наличии следующие документы по обеспечению безопасности информации при автоматизированной обработке в АС:

- приказ о создании экспертной комиссии;
- акт экспертизы информации;
- модель угроз безопасности ИСПДн;
- акт определения уровня защищённости АС, как ИСПДн;
- акт классификации АС, как ИС;
- техническое задание на создание СЗИ АС;

- технический проект на создание СЗИ АС;
- разрешительная система доступа к ресурсам АС;
- инструкция пользователю АС;
- инструкция системному администратору АС;
- инструкция администратору безопасности АС;
- инструкция по антивирусному контролю в АС;
- технический паспорт АС;
- журнал учета работ в АС;
- приказ о назначении администраторов безопасности и системных

администраторов автоматизированной системы.

Реализация подсистемы технической защиты информации АС заключается во внедрении следующих компонентов подсистемы защиты информации:

- межсетевого экранирования;
- защиты информации от НСД;
- антивирусной защиты;
- анализа защищённости.

Ж.8 Требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации

Требования к поставляемым техническим средствам, программному обеспечению и средствам защиты информации включают:

- программное обеспечение должно быть совместимым с программным обеспечением АС и не должно снижать требуемый уровень защищенности информации на объекте информатизации;
- программно-технические средства и средства защиты информации, должны быть совместимы между собой и не должны снижать уровень защищенности информации на объекте информатизации;

- программно-технические средства и средства защиты информации должны быть сертифицированными ФСТЭК России;
- обновления программного обеспечения должны быть безопасно получены, проверены и установлены на компонентах АС;
- поставляемые технические средства, ПО и средства защиты должны быть укомплектованы инструкциями по установке и эксплуатации;
- технические средства, программное обеспечение и средства защиты информации должны поставляться с комплектами соответствующих лицензий на использование;
- программное обеспечение должно проходить контроль отсутствия недеklarированных возможностей и отсутствия влияния на корректность работы средств защиты информации.

Ж.9 Функции заказчика и оператора по обеспечению защиты информации в АС

Функции заказчика по обеспечению защиты информации в АС:

- своевременное финансирование работ по обеспечению защиты информации в АС;
- проведение предварительных испытаний АС;
- создание необходимых для функционирования АС подразделений и служб;
- определение подразделений и должностных лиц, ответственных за проведение опытной эксплуатации и постоянной эксплуатации.

Функции оператора по обеспечению защиты информации в АС:

- пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

- регистрация событий, связанных с действиями от имени привилегированных учетных записей (администраторов) и событий, связанных с изменением привилегий учетных записей;

- обеспечение антивирусной защиты на этапе инициализации микропрограммного обеспечения средства вычислительной техники;

- хранение информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации;

- применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках;

- применение автоматизированных средств для обнаружения в информационной системе неразрешенного программного обеспечения (компонентов программного обеспечения) и уведомления об этом уполномоченных должностных лиц (администратора безопасности);

- анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в информационной системе для нарушения безопасности информации.

Ж.10 Стадии (этапы работ) создания системы защиты АС

Система защиты АС находится на этапе разработки технического задания для её дальнейшего проектирования.

Ж.11 Требования к сертифицированным средствам защиты информации

С учетом использования в АС сертифицированных по требованиям безопасности информации средств защиты информации, класс средств защиты должен быть следующим:

- средства вычислительной техники не ниже 5 класса;

- межсетевые экраны не ниже 3 класса в случае взаимодействия автоматизированной системы управления с информационно-

телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия такого взаимодействия;

— должны применяться средства защиты информации, программное обеспечение которых прошло проверку не ниже, чем по 4 уровню контроля отсутствия недеklarированных возможностей;

— заказчиком (оператором) в зависимости от потенциала нарушителя может приниматься решение о повышении уровня контроля отсутствия недеklarированных возможностей в программном обеспечении средств защиты информации.

Ж.12 Необходимые меры защиты информации в АС

Адаптированный базовый набор мер защиты информации АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В.Проценко» приведен в таблице Ж.2.

Таблица Ж.2 — Адаптированный базовый набор мер защиты информации в АС

Условное обозначение и номер меры	Меры защиты информации в АС
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых символов (защита обратной связи при вводе аутентификационной информации)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	

Продолжение таблицы Ж.2

Условное обозначение и номер меры	Меры защиты информации в АС
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (экранирование, фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование автоматизированной системы управления
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС)	
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

Продолжение таблицы Ж.2

Условное обозначение и номер меры	Меры защиты информации в АС
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	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
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений
СОВ.2	Обновление базы решающих правил
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей

Продолжение таблицы Ж.2

Условное обозначение и номер меры	Меры защиты информации в АС
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей
IX. Обеспечение целостности (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
X. Обеспечение доступности (ОДТ)	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, исполнительные устройства и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключая несанкционированный физический доступ

Продолжение таблицы Ж.2

Условное обозначение и номер меры	Меры защиты информации в АС
XII. Защита технических средств (ЗТС)	
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита автоматизированной системы и ее компонентов (ЗИС)	
ЗИС.1	Разделение функций по управлению (администрированию) автоматизированной системой управления, управлению (администрированию) системой защиты, функций по обработке информации и иных функций автоматизированной системы управления
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации
ЗИС.17	Разбиение автоматизированной системы управления на сегменты (сегментирование) и обеспечение защиты периметров сегментов
ЗИС.22	Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании
ЗИС.23	Защита периметра (физических и (или) логических границ) автоматизированной системы управления при ее взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями
XIV. Обеспечение безопасной разработки программного обеспечения (ОБР)	
ОБР.0	Разработка правил и процедур (политик) обеспечения безопасной разработки программного обеспечения

Продолжение таблицы Ж.2

Условное обозначение и номер меры	Меры защиты информации в АС
ОБР.1	Анализ уязвимостей и угроз безопасности информации в ходе разработки программного обеспечения
ОБР.2	Статический анализ кода программного обеспечения в ходе разработки программного обеспечения
ОБР.4	Тестирование на проникновение в ходе разработки программного обеспечения
ОБР.5	Динамический анализ кода программного обеспечения в ходе разработки программного обеспечения
ОБР.6	Документирование процедур обеспечения безопасной разработки программного обеспечения разработчиком и представление их заказчику (оператору)
XV. Управление обновлениями программного обеспечения (ОПО)	
ОПО.0	Разработка правил и процедур (политик) управления обновлениями программного обеспечения (включая получение, проверку и установку обновлений)
ОПО.1	Получение обновлений программного обеспечения от разработчика или уполномоченного им лица
ОПО.2	Тестирование обновлений программного обеспечения до его установки на макете или в тестовой зоне
XVI. Планирование мероприятий по обеспечению защиты информации (ПЛН)	
ПЛН.0	Разработка правил и процедур (политик) планирования мероприятий по обеспечению защиты информации
ПЛН.1	Определение лиц, ответственных за планирование, реализацию и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления
ПЛН.2	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в автоматизированных системах управления
ПЛН.3	Контроль выполнения мероприятий по обеспечению защиты информации в автоматизированных системах управления, предусмотренных утвержденным планом
XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	
ДНС.0	Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденных) ситуациях
ДНС.1	Разработка плана действий на случай возникновения нештатных (непредвиденных) ситуаций

Продолжение таблицы Ж.2

Условное обозначение и номер меры	Меры защиты информации в АС
ДНС.2	Обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.4	Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированных систем управления на случай возникновения нештатных (непредвиденных) ситуаций
ДНС.5	Обеспечение возможности восстановления автоматизированной системы управления и (или) ее компонент в случае возникновения нештатных (непредвиденных) ситуаций
XVIII. Информирование и обучение персонала (ИПО)	
ИПО.0	Разработка правил и процедур (политик) информирования и обучения персонала
ИПО.1	Информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
ИПО.2	Обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
ИПО.3	Проведение практических занятий с персоналом по правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации
XIX. Анализ угроз безопасности информации и рисков от их реализации (УБИ)	
УБИ.0	Разработка правил и процедур (политик) анализа угроз безопасности информации и рисков от их реализации
УБИ.1	Периодический анализ изменения угроз безопасности информации, возникающих в ходе эксплуатации автоматизированной системы управления
УБИ.2	Периодическая переоценка последствий от реализации угроз безопасности информации (анализ риска)
XX. Выявление инцидентов и реагирование на них (ИНЦ)	
ИНЦ.0	Разработка правил и процедур (политик) выявления инцидентов и реагирования на них
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов

Продолжение таблицы Ж.2

Условное обозначение и номер меры	Меры защиты информации в АС
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ.5	Принятие мер по устранению последствий инцидентов
ИНЦ.6	Планирование и принятие мер по предотвращению повторных инцидентов
XXI. Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)	
УКФ.0	Разработка правил и процедур (политик) управления конфигурацией автоматизированной системы управления и ее системы защиты
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию автоматизированной системы управления и ее системы защиты
УКФ.2	Управление изменениями конфигурации автоматизированной системы управления и ее системы защиты
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации автоматизированной системы управления и системы защиты на обеспечение защиты информации и согласование изменений в конфигурации автоматизированной системы управления с должностным лицом (работником), ответственным за обеспечение безопасности автоматизированной системы управления
УКФ.4	Документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и ее системы защиты
УКФ.5	Регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления

Ж.13 Реализация подсистемы технической защиты системы защиты информации АС

Ж.13.1. Подсистема межсетевого экранирования.

Подсистема межсетевого экранирования предназначена для разграничение доступа на сетевом уровне между сетевыми сегментами с различными требованиями к обеспечению информационной безопасности.

В АС межсетевое экранирование реализуется средствами межсетевого экранирования, ориентированными на фильтрацию сетевого трафика между сетевыми сегментами АС.

Конфигурация МЭ реализует следующий функционал информационной безопасности:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
- фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
- фильтрацию с учетом даты и времени;
- аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;
- регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- регистрацию и учет запросов на установление виртуальных соединений;
- локальную сигнализацию попыток нарушения правил фильтрации;
- идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- предотвращение доступа не идентифицированного пользователя

или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

- идентификацию и аутентификацию администратора МЭ при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

- регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ);

- регистрацию запуска программ и процессов (заданий, задач);

- регистрацию действия администратора МЭ по изменению правил фильтрации;

- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;

- контроль целостности своей программной и информационной части;

- контроль целостности программной и информационной части МЭ по контрольным суммам;

- восстановление свойств МЭ после сбоев и отказов оборудования;

- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора МЭ, процесса регистрации действий администратора МЭ, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

В качестве средств межсетевого экранирования следует применять прошедшее в установленном порядке процедуру оценки соответствия средство защиты информации (сертифицированное по требованиям безопасности

информации) «Altell Neo».

Ж.13.2. Подсистема защиты АС от НСД.

Подсистема защиты АС от НСД включает следующие компоненты, которые реализуют:

- управление доступом:
 - идентификацию и аутентификацию (проверку подлинности пользователя) при входе в систему по идентификатору (коду) и паролю условно - постоянного действия длиной не менее шести буквенно - цифровых символов;
 - идентификацию терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
 - идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;
 - контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- регистрация и учет:
 - регистрацию входа (выхода) пользователей в систему (из системы), либо регистрацию загрузки и инициализации ОС и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;
 - регистрацию выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа

(наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;

— регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки информации. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

— регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

— регистрацию попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

— учет всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);

— очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей;

— обеспечение целостности:

— обеспечение целостности программных средств системы защиты информации, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты информации

проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения конфиденциальной информации;

- физическую охрану технических средств АС (устройств и носителей информации), предусматривающую контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;

- периодическое тестирование функций системы защиты информации при изменении программной среды и пользователей информационной системы с помощью тест - программ, имитирующих попытки НСД;

- наличие средств восстановления системы защиты информации, предусматривающих ведение двух копий программных компонентов СЗИ, их периодическое обновление и контроль работоспособности.

Должно осуществляться управление СЗИ НСД администратором безопасности. Параметры механизмов защиты должны задаваться с помощью механизмов СЗИ НСД АС.

Ж.13.3 Подсистема антивирусной защиты.

ПАВЗ состоит из следующих основных уровней:

- антивирусная защита на уровне файловой системы;
- антивирусная защита на уровне web-трафика;
- централизованное управление антивирусной инфраструктурой корпоративной сети предприятия.

В качестве средств антивирусной защиты следует применять прошедшие в установленном порядке процедуру оценки соответствия антивирусные

средства (сертифицированные по требованиям безопасности информации).

Ж.13.4 Подсистема анализа защищённости.

Подсистема анализа защищённости реализует следующие механизмы:

- периодический контроль уровня защищённости;
- обнаружение уязвимостей в эксплуатируемом оборудовании и программном обеспечении;
- контроль соответствия АС требованиям стандартов безопасности.

Подсистема анализа защищённости обеспечивает:

- анализ защищённости операционных систем и системных сервисов;
- выявление уязвимостей рабочих станций/серверов путем анализа их конфигурации, состава используемого программного обеспечения, наличия открытых сетевых портов и запущенных сетевых служб.

Управление средствами анализа защищённости осуществляется централизованно.

В качестве подсистемы анализа защищённости необходимо применять ПО Сканер-ВС (сертификат ФСТЭК №2204 от 13.11.2010, срок действия до 13.11.2024).

Ж.13.5 Инженерно – технические мероприятия.

Из состава технических средств АС необходимо исключить (отключить, заблокировать) все компоненты (устройства), позволяющие осуществлять не предусмотренные технологическим процессом обработки действия с защищаемой информацией. Недействующие порты ЭВМ и устройств коммутации должны быть опломбированы, либо демонтированы, т.е. должна быть исключена возможность несанкционированного подключения к системе посторонних устройств.

Должен быть исключен визуальный обзор информации, выводимой на устройства отображения, из-за пределов КЗ, а также неконтролируемый доступ в помещения АС и непосредственно к СВТ и носителям информации

посторонних лиц.

На вход в BIOS ЭВМ должен быть установлен пароль длиной не менее 6 символов.

В BIOS ЭВМ и в ОС должны быть отключены все неиспользуемые устройства.

Установку ОС и ПО производить на первый раздел жесткого диска, второй раздел использовать под локальные файлы, средства восстановления и служебную информацию.

Приложение И

(обязательное)

Разрешительная система доступа к ресурсам АС на базе серверного парка

КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

РАЗРЕШИТЕЛЬНАЯ СИСТЕМА ДОСТУПА

(матрица доступа) к ресурсам АС на базе серверного парка корпоративной сети АО «ФНПЦ
«ПО «Старт» им. М.В. Проценко»

г. Заречный

Полномочия доступа пользователей к информационным ресурсам, программным и техническим средствам АС:

Должность	Группа АС	Ресурсы АС в ОС Linux												
		/	/bin	/boot	/dev	/etc	/home	/lib	/mnt	/proc	/root	/sbin	/sys	/usr
Сотрудники СПО	Системные администраторы	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD
Сотрудники ИБ	Администраторы безопасности информации	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD	RWAD
Пользователи АС	Пользователи АС	N	RN	N	RN	N	RN	N	RN	RN	N	RN	RN	RN

Должность	Группа АС	Ресурсы АС в ОС Windows		
		C:\	C:\users\	D:\
Сотрудники СПО	Системные администраторы	RWAD	RWAD	RWAD
Сотрудники ИБ	Администраторы безопасности информации	RWAD	RWAD	RWAD
Пользователи АС	Пользователи АС	RE	RWAD	RWAD

Лист ознакомления
с «Разрешительной системой доступа(матрицей доступа)»

№ п/п	ФИО	Должность	Подпись, дата
1			
2			
3			
4			
5			
6			
7			
8			

Приложение К

(обязательное)

Инструкция системному администратору

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

Инструкция системному администратору автоматизированной системы АО
«ФНПЦ «ПО «Старт» им. М.В. Проценко» на базе серверного парка
корпоративной сети

г. Заречный

К.1 Общие положения

Настоящая инструкция определяет функции, права, обязанности и порядок работы Системного администратора информации в автоматизированной системе (АС) на базе серверного парка корпоративной сети.

Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и защиты КИ, и не исключает обязательного выполнения их требований.

В своей практической деятельности Системный администратор АС (далее - Системный администратор) должен руководствоваться:

- «Технологическим процессом обработки информации в автоматизированной системе АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» на базе серверного парка корпоративной сети;
- «Инструкцией по использованию средств антивирусной защиты в автоматизированной системе АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» на базе серверного парка корпоративной сети;
- требованиями настоящей инструкции.

В своей практической деятельности Системный администратор использует АС, предназначенную для обработки информации следующих степеней конфиденциальности: для служебного пользования, коммерческая тайна, персональные данные, а также несекретной информации.

В своей практической деятельности Системный администратор АС использует следующие накопители информации:

- накопители информации, необходимые для выполнения функций системного администратора;
- накопители, необходимые для установки и настройки необходимого программного обеспечения (ПО).

Свои действия, совершаемые в АС: включение – выключение АС; перезагрузка АС, вход – выход в систему; копирование (перенос) информации на сменные носители информации; характер работ (работа с приложениями, создание, редактирование документа, работа с базами данных), действия по техническому обслуживанию АС — Системный администратор обязан зафиксировать в «Журнале учета работы и решения задач в АС».

Доступ Системного администратора к обслуживанию АС осуществляется в присутствии и под контролем Администратора безопасности АС.

Допуск Системного администратора к работе в АС должен быть оформлен документально в виде матрицы доступа к АС в установленном порядке.

Системный администратор, является лицом, ответственным за:

- установку, настройку и обновление общесистемного и прикладного ПО в АС;
- установку, настройку и обновление механизмов безопасности в АС.

В процессе работы в АС Системному администратору запрещается предоставлять свою рабочую сессию в АС другим исполнителям АС для работы с консоли.

Системный администратор АС в рамках своих функциональных обязанностей осуществляет выполнение процедур резервирования данных в установленном порядке.

В случае увольнения или изменения должностных обязанностей Администраторов АС должны быть приняты меры по оперативному изменению в АС персональных идентификаторов и паролей Администраторов АС.

Функциями Системного администратора являются:

- установка, настройка и обновление общесистемного и прикладного ПО;
- установка и настройка средств защиты информации;

- установка, настройка и обновление антивирусных средств;
- регулярное обновление антивирусных баз в АС;
- управление учетными записями исполнителей АС;
- управление полномочиями доступа исполнителей АС к информации на накопителях АС;
- периодический контроль за выполнением исполнителями АС требований по защите обрабатываемой информации путем анализа журнала (ов) протоколирования работы в АС;
- настройка и сопровождение подсистемы регистрации и учета действий исполнителей при работе в АС;
- регулярное проведение анализа системного журнала АС для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- архивирование журналов операционной системы и системы ЗИ;
- своевременное информирование Администратора безопасности АС о несанкционированных действиях персонала и участие в проведении расследования попыток НСД;
- периодическое тестирование функций установленной в АС СЗИ, особенно при изменении программной среды и полномочий исполнителей;
- резервирование и восстановление программной среды, программных средств и настроек СЗИ при сбоях.

Системный администратор имеет право:

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ, нарушения функционирования средств и систем защиты информации, нарушения целостности защитных знаков, пломб и

печатаей в АС, нарушении конфигурации и (или) состава технических и (или) программных средств АС (объекта информатизации в целом).

Системный администратор АС обязан:

- обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;
- проводить инструктаж исполнителей по правилам работы в АС с установленной СЗИ от НСД;
- в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- хранить и предоставлять архивные копии журналов ОС и журналов СЗИ при проведении периодических проверок АС;
- докладывать Администратору безопасности АС о неправомерных действиях исполнителей, приводящих к нарушению требований по защите информации с занесением данного факта в «Журнал учета работы и решения задач в АС».

Возложение на сотрудника обязанностей Системного администратора оформляется приказом по предприятию АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», с указанием АС, к работе с которой он допускается.

Контроль работоспособности и функционирование АС в установленном штатном режиме, контроль функционирования механизмов безопасности АС, а также защиту АС от несанкционированного доступа к информации осуществляет Администратор безопасности АС.

Техническое обслуживание АС — подключение — отключение периферийных устройств; вскрытие — закрытие корпусов серверов, периферийных устройств и др. (без изменения конфигурации АС) — осуществляется техническими специалистами АО «ФНПЦ «ПО «Старт» им. М.В. Проценко, только в присутствии и под контролем Администратора

безопасности АС. По окончании технического обслуживания Администратором безопасности АС производится отметка о факте технического обслуживания и о характере выполненных работ в «Журнале учета работы и решения задач в АС», а также, в случае изменения конфигурации АС, производится корректировка «Технического паспорта...».

К.2 Установка, настройка и обновление общесистемного и прикладного ПО.

Системный администратор обязан осуществлять установку, настройку и обновление общесистемного и прикладного ПО в соответствии с руководствами, инструкциями и рекомендациями по установке используемых программных продуктов.

АС должно быть установлено только ПО, указанное в «Техническом паспорте...» на АС.

Все ПО, используемое в АС должно иметь необходимые лицензии, либо быть свободно распространяемым.

СЗИ от НСД должны быть сертифицированы ФСТЭК РФ по требованиям безопасности информации.

К.3 Установка и обновление механизмов безопасности системы защиты информации.

Системный администратор АС обязан осуществлять установку, и обновление программного комплекса системы защиты информации в соответствии с руководством по администрированию, входящим в комплект поставки данного продукта.

Выполняя процедуру установки (переустановки) системы защиты информации, Системный администратор обязан выполнить следующие операции:

- запуск мастера установки;
- ввод лицензионного номера системы защиты;

- создание персонального идентификатора администратора системы защиты;
- настройка системы защиты;
- завершение установки и перезагрузка серверов.

К.4 Настройка системы защиты информации.

Системный администратор обязан осуществлять настройку системы защиты информации в АС в соответствии с «Руководством по администрированию» входящим в комплект поставки продукта, а также в соответствии с утвержденной установленным образом матрицей доступа к АС и другой документацией, регламентирующей работу в АС.

К.5 Антивирусная защита и обновление антивирусных средств.

В обязанности Системного администратора входит защита АС от поражения компьютерными вирусами, в том числе:

- проверка наличия антивирусных средств в АС;
- ежеквартальная проверка АС на предмет обнаружения вирусов;
- регулярное обновление антивирусных баз.

К.6 Управление учетными записями исполнителей АС.

Для доступа исполнителя к АС под управлением системы защиты информации, необходимо иметь в ней регистрационную запись этого исполнителя.

В функции Системного администратора входит управление учетными записями исполнителей АС:

- создание учетной записи исполнителя в АС;
- блокировка, изменение пароля и свойств учетной записи исполнителя АС;
- удаление учетной записи исполнителя в АС.

При увольнении или перемещении исполнителей, обнаружении попыток несанкционированного доступа к конфиденциальной информации, Системным

администратором принимаются меры по оперативному изменению паролей, идентификаторов и ключей защиты конфиденциальной информации.

К.7 Контроль за выполнением исполнителями ас требований по защите обрабатываемой информации.

Системный администратор обязан осуществлять контроль за выполнением исполнителями АС требований по защите обрабатываемой информации, анализируя журнал протоколирования работы в АС.

В случае обнаружения попыток несанкционированного доступа к информации, выявления нештатных ситуаций и иных чрезвычайных происшествий, работа в АС прекращается. Системный администратор АС немедленно докладывает о результатах просмотра журнала протоколирования работы в АС и других чрезвычайных происшествиях Администратору безопасности АС, который принимает решение о проведении административного расследования.

Архивирование и очистка журнала протоколирования работы. Данные протокола безопасности сохраняются до проведения периодической ежегодной проверки.

К.8 Порядок работы в АС.

Перед началом работы в АС Системный администратор обязан:

- получить в установленном порядке у ответственного за несекретное делопроизводство МНИ, в том числе МНИ для работы с КИ (с ограничительной пометкой «Для служебного пользования», «Коммерческая тайна», «Персональные данные»), предназначенные для выполнения функций администрирования;
- убедиться, что в помещении обеспечены условия для обработки конфиденциальной информации;
- убедиться в целостности и неизменности конфигурации и состава технических средств АС;

- убрать с рабочего места МНИ, не используемые в данном сеансе работы.

Для начала работы в АС Системный администратор обязан:

- включить АС (сервер), либо убедиться, что сервер включен;
- осуществить вход в систему посредством СЗИ от НСД, на запрос персонального идентификатора (имя, логин), ввести с клавиатуры свой идентификатор (имя, логин), либо разблокировать сервер;
- на запрос ввода пароля ввести с клавиатуры свой пароль и нажать клавишу *<Enter>*;
- дождаться завершения процесса загрузки операционной системы (ОС);
- выполнить свои обязанности по администрированию;
- произвести запись о проведенной работе в «Журнал учета работы и решения задач в АС».

При необходимости покинуть рабочее место АС в процессе работы, необходимо:

- заблокировать АС;
- сдать в установленном порядке Ответственному за несекретное делопроизводство:
- учтенные в несекретном делопроизводстве МНИ с ограничительной пометкой «Для служебного пользования», «Коммерческая тайна», «Персональные данные».

Чтобы разблокировать АС:

- на запрос ввода пароля ввести с клавиатуры свой пароль и нажать клавишу *<Enter>*.

При работе с МНИ Системный администратор обязан:

- устанавливать в АС только учтенные (соответственно степени

конфиденциальности хранимой и/или обрабатываемой информации) в несекретном делопроизводстве и в системе защиты информации МНИ;

— перед началом работы с МНИ осуществить проверку МНИ на предмет отсутствия компьютерных вирусов в соответствии с «Инструкцией по использованию средств антивирусной защиты в АС».

Для завершения сеанса работы в АС Системный администратор обязан:

— завершить сеанс работы сервера;

— сдать в установленном порядке ответственному за несекретное делопроизводство все полученные ранее МНИ, содержащие КИ.

Приложение Л
(обязательное)
Инструкция пользователю АС

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

Инструкция пользователю автоматизированной системы АО «ФНПЦ «ПО
«Старт» им. М.В. Проценко» на базе серверного парка корпоративной сети

г. Заречный

Л.1 Общие положения

Настоящая инструкция регламентирует общие положения и порядок работы Пользователя АС в АС на базе серверного парка корпоративной сети в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения защиты сведений, являющихся конфиденциальной информацией (КИ), и не исключает обязательного выполнения их требований.

В своей практической деятельности Пользователь АС (далее - Пользователь) должен руководствоваться:

- «Инструкцией по использованию средств антивирусной защиты в АС...»;
- требованиями настоящей инструкции.

В своей практической деятельности Пользователь использует АС, предназначенную для обработки информации следующих степеней конфиденциальности: для служебного пользования, коммерческая тайна, персональные данные, а также несекретной информации.

Допуск Пользователя к работе в АС должен быть оформлен документально в виде разрешительной системы доступа к ресурсам АС в установленном порядке.

Свои действия, совершаемые в АС: включение – выключение АС; смена пользователя (перезагрузка АС, вход – выход в систему); характер работ (работа с приложениями, создание, редактирование документа, отправка почты) — Пользователь обязан зафиксировать в «Журнале учета работы в АС».

Пользователь имеет право решать поставленные задачи в соответствии с полномочиями доступа к ресурсам АС, присвоенными Системным администратором данному пользователю. При этом для хранения файлов, содержащих КИ, разрешается использовать только специально выделенные каталоги на ПЭВМ/файловых серверах КС и учтённые в несекретном

делопроизводстве МНИ.

Присвоение Пользователю полномочий доступа к ресурсам АС осуществляется Системным администратором АС при первичной регистрации пользователя в АС в соответствии с Разрешительной системой доступа (РСД) к ресурсам АС.

Пользователь АС несет ответственность за правильность включения и выключения АС, вход в систему и за все совершаемые (не совершаемые) действия им при работе в АС.

Вход Пользователя в систему осуществляется на основе предъявления персонального идентификатора – имени (логин) и ввода личного пароля длиной не менее 8 символов, определяемых для Пользователя АС Системным администратором АС.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам Пользователя АС осуществляется периодическая смена пароля Пользователя. Смена личного пароля Пользователя АС осуществляется Системным администратором АС.

Резервное копирование, уничтожение и восстановление конфиденциальной информации, а также несекретной информации осуществляют Пользователь и Администратор безопасности АС.

Резервное копирование, уничтожение и восстановление общесистемной информации осуществляет Системный администратор АС.

В случае появления в системе сообщения об обнаружении вирусов, Пользователь АС обязан немедленно сообщить об этом Администратору безопасности АС или Системному администратору АС и прекратить работу в АС до разрешения Администратора безопасности АС.

В процессе работы Пользователю запрещается:

- использовать для постоянного хранения и обработки КИ, каталоги, за исключением каталогов, выделенных Системным администратором АС;
- осуществлять попытки несанкционированного доступа к ресурсам

АС, системы и других пользователей;

- предоставлять свою рабочую сессию в АС другим исполнителям АС для работы с консоли;

- работать в АС под чужими регистрационными данными (имя, пароль);

- пытаться подменять функции Системного администратора АС или Администратора безопасности АС или специалистов по техническому обслуживанию;

- нарушать целостность защитных знаков, пломб и печатей в АС и (или) осуществлять обработку информации, если нарушена целостность защитных знаков, пломб и печатей в АС;

- изменять конфигурацию и состав технических и (или) программных средств АС и (или) осуществлять обработку информации, если нарушена целостность и (или) конфигурация и состав технических и (или) программных средств АС;

- самостоятельно устанавливать и настраивать ПО в АС;

- покидать помещение с включенной АС до окончания работы;

- подключать (устанавливать) к СВТ из состава АС технические средства с элементами памяти (флэш, смартфон, электронная книга и т.п.), а также средства беспроводной передачи данных;

- при появлении системных сообщений (от ОС, СЗИ либо средств антивирусного контроля) самостоятельно принимать решение о продолжении работы.

Техническое обслуживание АС — подключение – отключение периферийных устройств; вскрытие – закрытие корпуса ПЭВМ, периферийных устройств и др. (без изменения конфигурации АС) — осуществляется техническими специалистами АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», только в присутствии и под контролем Администратора безопасности АС. По

окончании технического обслуживания Администратором безопасности АС производится отметка о факте технического обслуживания и о характере выполненных работ в «Журнале учета работы в АС», а также, в случае изменения конфигурации АС, производится корректировка «Технического паспорта...».

По всем возникающим вопросам при работе в АС, Пользователю необходимо обращаться к Администратору безопасности АС или Системному администратору АС.

Л.2 Порядок работы в АС

Перед началом работы в АС Пользователь обязан:

- получить (при необходимости) в установленном порядке у ответственного за несекретное делопроизводство МНИ, в том числе МНИ для работы с КИ (с ограничительной пометкой «Для служебного пользования», «Коммерческая тайна», «Персональные данные»), предназначенные для хранения (переноса и др. производственных нужд) ДСП, КТ, ПДн, а также несекретной информации;

- убедиться, что в помещении обеспечены условия для обработки конфиденциальной информации;

- убедиться в целостности и неизменности конфигурации и состава технических средств АС;

- убрать с рабочего места носители информации, не используемые в данном сеансе работы.

Для начала работы в АС Пользователь обязан:

- включить АС (ПЭВМ), нажав кнопку <Питание> на системном блоке;

- осуществить вход в систему посредством СЗИ от НСД, на запрос персонального идентификатора (имя, логин), ввести с клавиатуры свой идентификатор (имя, логин);

— на запрос ввода пароля ввести с клавиатуры свой пароль и нажать клавишу <Enter>.

Набираемые символы не будут отображаться на экране. Вместо вводимых символов в поле диалога отображаются символы ‘*’.

Стирание ошибочно набранных символов в строке ввода производится клавишей <BackSpace>, для исправлений также используйте клавиши ‘ç’, ‘è’ или <Delete>.

Внимание!

При появлении предупреждающих сообщений или сообщений об ошибках, записать текст сообщения, появившегося на экране, и немедленно обратиться к Администратору безопасности (Системному администратору АС) для выяснения причины.

— дождаться завершения процесса загрузки операционной системы (ОС);

— предъявить необходимые для выполнения производственных задач учтённые в несекретном делопроизводстве МНИ;

— выполнить необходимые действия в рамках производственных задач;

— произвести запись о проведенной работе в «Журнал учета работы в АС».

При необходимости покинуть рабочее место АС в процессе работы, необходимо:

— выключить АС (ПЭВМ);

— сдать в установленном порядке ответственному за несекретное делопроизводство все полученные ранее МНИ и полученные в процессе работы в АС распечатки, содержащие КИ, либо убрать в сейф:

— все полученные ранее МНИ;

— полученные в процессе работы в АС распечатки, содержащие

КИ;

- сейф закрыть на ключ и опечатать личной печатью.

В порядке исключения, при необходимости кратковременного отлучения от рабочего места АС, разрешается не выключать АС, выполнив следующие действия:

- заблокировать АС (ПЭВМ);
- убрать в сейф:
 - все полученные ранее МНИ;
 - полученные в процессе работы в АС распечатки, содержащие

КИ;

- сейф закрыть на ключ и опечатать личной печатью.

Чтобы разблокировать АС (ПЭВМ) необходимо на запрос ввода пароля ввести с клавиатуры свой пароль и нажать клавишу <Enter>.

При работе с МНИ Пользователь обязан:

- устанавливать в АС только учтенные (соответственно степени конфиденциальности хранимой и/или обрабатываемой информации) в несекретном делопроизводстве (с ограничительной пометкой «Для служебного пользования», «Коммерческая тайна», «Персональные данные») и в СЗИ МНИ;
- перед началом работы с МНИ, Пользователь осуществляет проверку содержимого МНИ на отсутствие вирусов штатными антивирусными средствами, установленными в АС, в соответствии с «Инструкцией по использованию средств антивирусной защиты ...». В случае обнаружения вирусов на МНИ Пользователь обязан немедленно сообщить об этом Администратору безопасности АС или Системному администратору АС и прекратить работу с данным МНИ.

Для завершения сеанса работы в АС Пользователь обязан:

- завершить сеанс работы ОС;

- выключить ПЭВМ;
- сдать в установленном порядке ответственному за несекретное делопроизводство все полученные ранее МНИ и полученные в процессе работы в АС распечатки, содержащие КИ.

Приложение М

(обязательное)

Инструкция администратору безопасности АС

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

Инструкция администратору безопасности автоматизированной системы АО
«ФНПЦ «ПО «Старт» им. М.В. Проценко» на базе серверного парка
корпоративной сети

г. Заречный

М.1 Общие положения

Настоящая инструкция определяет функции, права, обязанности и порядок работы Администратора безопасности информации в автоматизированной системе (АС) на базе серверного парка корпоративной сети.

Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и защиты сведений, являющихся КИ, и не исключает обязательного выполнения их требований.

В своей практической деятельности Администратор безопасности АС (далее - Администратор безопасности) должен руководствоваться:

- «Технологическим процессом обработки информации в автоматизированной системе АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» на базе серверного парка корпоративной сети;
- «Инструкцией по использованию средств антивирусной защиты в автоматизированной системе АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» на базе серверного парка корпоративной сети;
- требованиями настоящей инструкции.

В своей практической деятельности Администратор безопасности использует АС, предназначенную для обработки информации следующих степеней конфиденциальности: для служебного пользования, коммерческая тайна, персональные данные, а также несекретной информации.

Свои действия, совершаемые в АС: включение – выключение АС; смена пользователя (перезагрузка АС, вход – выход в систему); копирование (перенос) информации на сменные носители информации; характер работ (работа с приложениями, создание, редактирование документа, работа с базами данных) — Администратор безопасности обязан зафиксировать в «Журнале учета работы и решения задач в АС».

Администратор безопасности допущен к защищаемой информации, обрабатываемой в АС в полном объеме.

Допуск Администратора безопасности к работе в АС должен быть оформлен документально в виде матрицы доступа к АС в установленном порядке.

Доступ Администратора безопасности к обслуживанию АС осуществляется самостоятельно, но он не допущен к администрированию ресурсов АС.

Администратор безопасности, является лицом, ответственным за функционирование АС в установленном штатном режиме, а также за защиту АС от несанкционированного доступа к информации.

В процессе работы в АС Администратору безопасности запрещается предоставлять свою рабочую сессию в АС другим Исполнителям АС для работы с консоли и работать в АС под чужими регистрационными данными (имя, пароль).

Техническое обслуживание АС — подключение — отключение периферийных устройств; вскрытие — закрытие корпусов серверов, периферийных устройств и др. (без изменения конфигурации АС) — осуществляется техническими специалистами АО «ФНПЦ «ПО «Старт» им. М.В. Проценко, только в присутствии и под контролем Администратора безопасности АС. По окончании технического обслуживания Администратором безопасности АС производится отметка о факте технического обслуживания и о характере выполненных работ в «Журнале учета работы и решения задач в АС», а также, в случае изменения конфигурации АС, производится корректировка «Технического паспорта...».

Функциями Администратора безопасности являются:

- контроль доступа лиц к АС в соответствии с «Матрицей доступа к АС...»;
- контроль за целостностью защитных знаков, пломб и печатей в АС;

- контроль за неизменностью конфигурации и состава технических и программных средств АС (объекта информатизации в целом);
- обеспечение функционирования АС в установленном штатном режиме, а также защита АС от несанкционированного доступа к информации;
- контроль за установкой, настройкой и обновлением общесистемного ПО, прикладного ПО и системы защиты информации в АС Системным администратором АС;
- контроль за выполнением пользователями АС требований по защите обрабатываемой информации, контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты КИ, при проведении работ в АС;
- контроль за регулярным обновлением антивирусных баз в АС;
- резервное копирование, уничтожение и восстановление конфиденциальной информации, а также несекретной информации;
- анализ файла журнала безопасности АС, предоставляемого Системным администратором АС (ежемесячно или по требованию);
- поддержание и контроль соблюдения пользователями установленного порядка и правил антивирусной защиты информации в АС;
- своевременное информирование начальника АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» о несанкционированных действиях персонала и участие в проведении расследования попыток НСД;
- ведение (своевременное создание и изменение) документации на АС в соответствии с требованиями нормативных документов;
- контроль работоспособности и использования средств защиты информации, контроль соблюдения требований по размещению и использованию АС, указанных в предписании на эксплуатацию.

Возложение на сотрудника обязанностей Администратора безопасности оформляется приказом по предприятию АО «ФНПЦ «ПО «Старт» им. М.В.

Проценко» с указанием АС, к работе с которой он допускается.

Администратор безопасности информации имеет право:

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ, нарушения функционирования средств и систем защиты информации, нарушения целостности защитных знаков, пломб и печатей в АС, нарушении конфигурации и (или) состава технических и (или) программных средств АС (объекта информатизации в целом).

Администратор безопасности информации АС обязан:

- обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;
- проводить инструктаж пользователей по правилам работы в АС с установленной СЗИ от НСД;
- в случае отказа средств и систем защиты информации, а также других выявленных нарушениях, принимать меры по прекращению функционирования АС до момента их восстановления;
- вести документацию на АС в соответствии с требованиями нормативных документов.

Установку общесистемного ПО, прикладного ПО и механизмов безопасности в АС, антивирусную защиту и обновление антивирусных средств, управление учетными записями пользователей АС, управление полномочиями доступа пользователей АС к информации на накопителях АС, работу с журналом (и) протоколирования работы в АС, установку и настройку системы защиты информации — осуществляет Системный администратор АС.

М.2 Контроль за установкой и обновлением общесистемного ПО,

прикладного ПО и системы защиты информации в АС системным администратором АС.

Администратор безопасности обязан осуществлять контроль за установкой, настройкой и обновлением общесистемного ПО, прикладного ПО и системы защиты информации Системным администратором АС.

Все работы по обслуживанию АС должны фиксироваться Администратором безопасности в «Журнале учета работы и решения задач в АС».

М.3 Контроль за выполнением исполнителями АС требований по защите обрабатываемой информации.

Администратор безопасности обязан осуществлять контроль за выполнением исполнителями АС требований по защите обрабатываемой информации.

Все выявленные в АС нарушения должны фиксироваться в «Журнале учета работы и решения задач в АС».

В случае обнаружения попыток несанкционированного доступа к информации, выявления нештатных ситуаций и иных чрезвычайных происшествий, работа в АС прекращается. Администратор немедленно докладывает о происшествиях руководству АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», которое принимает решение о проведении административного расследования.

М.4 Порядок работы в АС.

Перед началом работы в АС Администратор безопасности обязан:

— получить (при необходимости) в установленном порядке у ответственного за несекретное делопроизводство МНИ, в том числе МНИ для работы с КИ (с ограничительной пометкой «Для служебного пользования», «Коммерческая тайна», «Персональные данные»), предназначенные для хранения (переноса и др. производственных нужд) ДСП, КТ, ПДн, а также несекретной информации;

— убедиться, что в помещении обеспечены условия для обработки

конфиденциальной информации;

- убедиться в целостности и неизменности конфигурации и состава технических средств АС;

- убрать с рабочего места носители информации, не используемые в данном сеансе работы.

Для начала работы в АС Администратор безопасности обязан:

- включить АС (сервер), либо убедиться, что сервер включен;
- на запрос персонального идентификатора (имя, логин) ввести с клавиатуры свой идентификатор (имя, логин);

- на запрос ввода пароля ввести с клавиатуры свой пароль и нажать клавишу <Enter>;

- дождаться завершения процесса загрузки операционной системы (ОС);

- выполнить свои обязанности по администрированию;

- произвести запись о проведенной работе в «Журнал учета работы и решения задач в АС».

При необходимости покинуть рабочее место АС в процессе работы, необходимо:

- заблокировать АС;

- сдать в установленном порядке Ответственному за несекретное делопроизводство учтенные в несекретном делопроизводстве носители информации с ограничительной пометкой «Для служебного пользования», «Коммерческая тайна», «Персональные данные».

Чтобы разблокировать ЭВМ – на запрос ввода пароля ввести с клавиатуры свой пароль и нажать клавишу <Enter>.

При работе с МНИ Администратор безопасности обязан:

- устанавливать в АС только учтенные (соответственно степени конфиденциальности хранимой и/или обрабатываемой информации) в

несекретном делопроизводстве и в системе защиты информации МНИ;

- перед началом работы с МНИ осуществить проверку МНИ на предмет отсутствия компьютерных вирусов в соответствии с «Инструкцией по использованию средств антивирусной защиты в АС».

Для завершения сеанса работы в АС Администратор безопасности обязан:

- завершить сеанс работы сервера;
- сдать в установленном порядке ответственному за несекретное делопроизводство все полученные ранее МНИ, содержащие КИ.

Приложение Н
(обязательное)
Журнал учета работ в АС

Инв. № _____

292

ЖУРНАЛ
учета работ в АС на базе серверного парка корпоративной сети
АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

число листов:

начат:

окончен:

срок хранения: 3г. ст.259

[illegible]

Приложение П

(обязательное)

Инструкция по использованию средств антивирусной защиты

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

Инструкция по использованию средств антивирусной защиты в
автоматизированной системы АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» на
базе серверного парка корпоративной сети

г. Заречный

П.1 Общие положения

Настоящая инструкция определяет порядок использования средств антивирусной защиты исполнителями (администраторами) в автоматизированной системе на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»(далее – АС)

Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

В своей практической деятельности Исполнители АС должны руководствоваться:

- «Описанием технологического процесса обработки информации в АС ...»;
- «Инструкцией администратору безопасности АС ...»;
- «Инструкцией системному администратору АС ...»;
- требованиями настоящей инструкции.

В своей практической деятельности Исполнители АС используют АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», предназначенную для обработки и хранения информации следующих степеней конфиденциальности: для служебного пользования, коммерческая тайна, персональные данные, а также несекретной информации.

Допуск Исполнителей АС к работе в АС должен быть оформлен документально в виде матрицы доступа к ресурсам АС в установленном порядке.

Установку, настройку и обновление антивирусных средств в АС осуществляет Системный администратор АС.

Периодическую проверку наличия антивирусных средств в АС и регулярное обновление антивирусных баз в АС осуществляет Системный администратор АС.

Контроль за наличием антивирусных средств в АС, ежемесячным обновлением антивирусных баз и ежемесячной автоматической полной проверкой АС на предмет обнаружения вирусов осуществляет Администратор безопасности АС.

В АС в качестве антивирусного средства защиты используются «Kaspersky Endpoint Security для Windows 10», «Kaspersky Endpoint Security for Linux».

П.2 Порядок работы с средствами антивирусной защиты на серверах под управлением операционной системы ms windows server

Работа со средствами антивирусной защиты при работе со съемными МНИ:

Перед началом работы с МНИ Исполнитель АС обязан:

- установить в АС МНИ;
- дождаться автоматического появления окна с прогрессом проверки

подключенного устройства на наличие вредоносных программ (рис. 1).

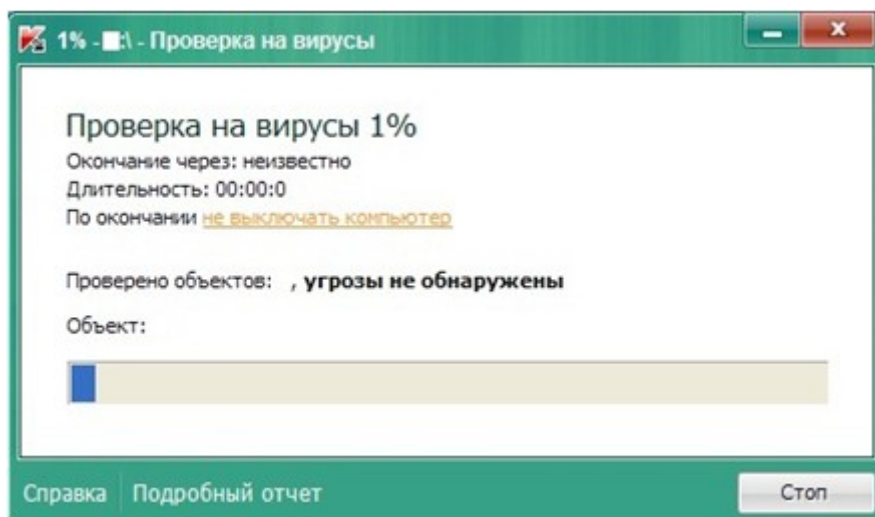


Рисунок П.1 – Проверка съемного МНИ

В случае, если окно не появилось:

- выбрать ресурс (МНИ);
- вызвать контекстное меню, нажав правую клавишу мыши на

выбранном ресурсе, и запустить «Проверить на вирусы»;

— дождаться появления окна с прогрессом проверки МНИ.

Внимание!

В случае если не запустилась автоматическая проверка МНИ и попытка ручного запуска также закончилась неуспешно, Исполнитель АС обязан прекратить все работы в АС и сообщить об этом Администратору безопасности или Системному администратору.

— в появившемся окне с прогрессом проверки ресурса файловой системы дождаться результата проверки ресурса;

— в случае обнаружения вирусных угроз (рис. 2) прекратить все работы в АС, обратиться к Администратору безопасности АС или Системному администратору АС для решения данной проблемы, иначе (рис. 3) продолжить работу в АС.

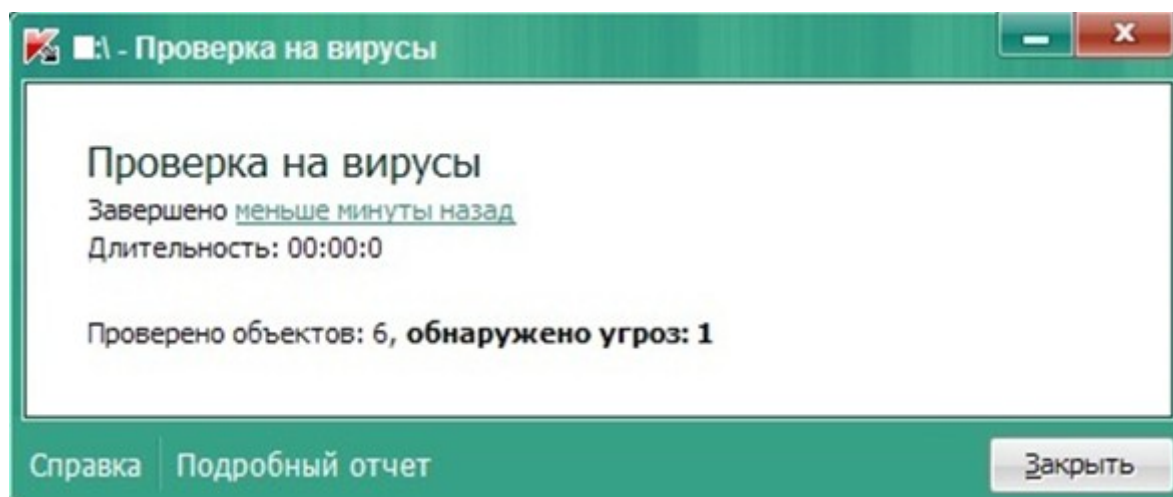


Рисунок П.2 – Отрицательный результат проверки съемного МНИ

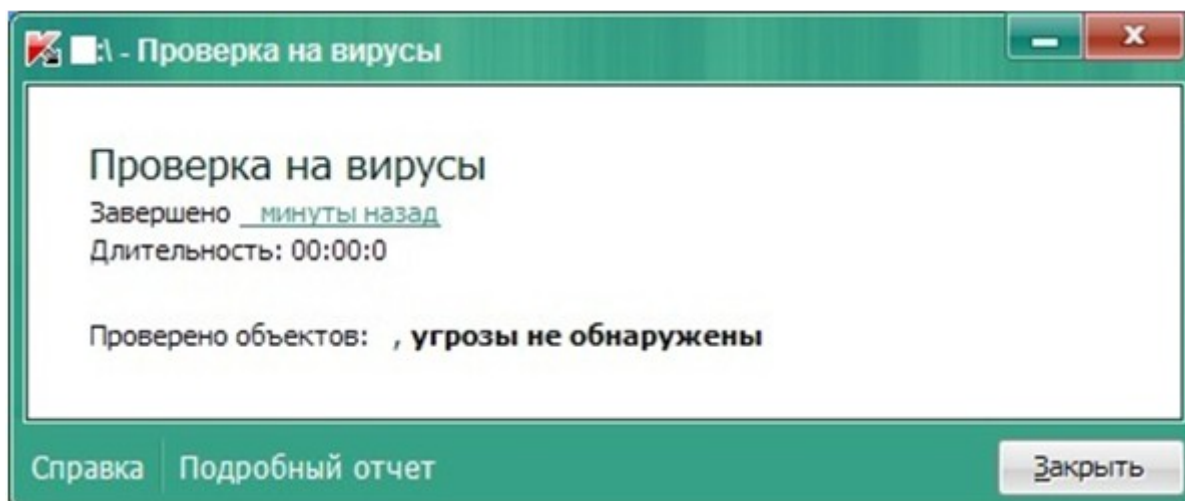


Рисунок П.3 – Положительный результат проверки съемного МНИ

Работа с средствами антивирусной защиты при работе с ресурсами файловой системы АС.

При необходимости проверки ресурса АС на наличие вредоносных программ Исполнитель АС обязан:

- выбрать ресурс АС;
- вызывать контекстное меню, нажав правую кнопку мыши, и выбрать вкладку «Проверить на вирусы»;
- в появившемся окне с прогрессом проверки ресурса файловой системы дождаться результата проверки ресурса;
- в случае обнаружения вирусных угроз прекратить все работы в АС, обратиться к Администратору безопасности АС или Системному администратору АС для решения данной проблемы;
- в случае, если вирусные угрозы не обнаружены, Исполнитель АС продолжает работу в АС.

П.3 Порядок работы с средствами антивирусной защиты на серверах под управлением операционной системы Янукс 4.0

Работа со средствами антивирусной защиты при работе со съемными МНИ:

Перед началом работы с МНИ Исполнитель АС обязан:

- установить в АС МНИ;
- смонтировать МНИ командой: `mount /dev/<имя_устройства> /media;`
- проверить МНИ с помощью команды:
`/opt/kaspersky/kav4fs/bin/kav4fs-control --action <действие> --scan-file /media;`
- задать действие Recommended над обнаруженными опасными объектами.

Внимание!

В случае если проверка закончилась неуспешно, Исполнитель АС обязан прекратить все работы в АС и сообщить об этом Администратору безопасности или Системному администратору:

- дождаться результата проверки ресурса;
- в случае обнаружения вирусных угроз прекратить все работы в АС, обратиться к Администратору безопасности АС или Системному администратору АС для решения данной проблемы, иначе продолжить работу в АС.

Работа с средствами антивирусной защиты при работе с ресурсами файловой системы АС.

При необходимости проверки ресурса АС на наличие вредоносных программ Исполнитель АС обязан:

- выбрать файловый ресурс АС;
- запустить проверку файлового ресурса с помощью команды
`/opt/kaspersky/kav4fs/bin/kav4fs-control --action <действие> --scan-file <Путь_к_ресурсу>;`
- дождаться результата проверки ресурса;
- в случае обнаружения вирусных угроз прекратить все работы в АС, обратиться к Администратору безопасности АС или Системному администратору АС для решения данной проблемы;

— в случае, если вирусные угрозы не обнаружены, Исполнитель АС продолжает работу в АС.

Приложение Р

(обязательное)

Технический паспорт АС на базе серверного парка КС АО «ФНПЦ «ПО
«Старт» им. М.В.Проценко»

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ ФИО

« __ » _____ 202__ г.

УТВЕРЖДАЮ

Главный инженер

_____ ФИО

« __ » _____ 202__ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА
БАЗЕ СЕРВЕРНОГО ПАРКА КОРПОРАТИВНОЙ СЕТИ АО «ФНПЦ «ПО
«СТАРТ» ИМ. М.В. ПРОЦЕНКО»

г. Заречный

Р.1 Общие сведения об объекте

Наименование объекта: АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Расположение объекта: г. Заречный Пензенской области, пр. Мира 1, АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Класс защищенности АС – К2; уровень защищенности ПДн – 3.

Р.2 Состав оборудования объекта

Перечень основных технических средств и систем, входящих в состав объекта:

№ п/п	Тип ОТСС	Заводской номер	Серийный номер	Примечание
1	СХД резервного копирования StoreOnce (HP Storeonce 4500)	0174590		
2	СХД 3PAR 7200(HP StoreServ 7200 (M6710/7000 Encl))	0174588		
3	AltellNeo Master	0174598	04615/2, з/з E366592	
4	ME5200	0174596		
5	Blade-система HP c7000	0174591	CZJ43304QB	

Перечень вспомогательных технических средств, входящих в состав ИС (средств вычислительной техники, не участвующих в обработке конфиденциальной информации):

№ п/п	Тип ВТСС	Заводской номер	Примечание
1	Телефон	-	1 шт.
2	Сервера Ascon	-	-
3	Манипулятор «мышь» Logitech	-	1 шт.
4	Кондиционер 1 STULZ STU000831	-	1 шт.
5	Датчик пожарной сигнализации	-	4 шт.
6	Клавиатура Logitech	-	1 шт.
7	Монитор Samsung	-	1 шт.

Р.3 Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта:

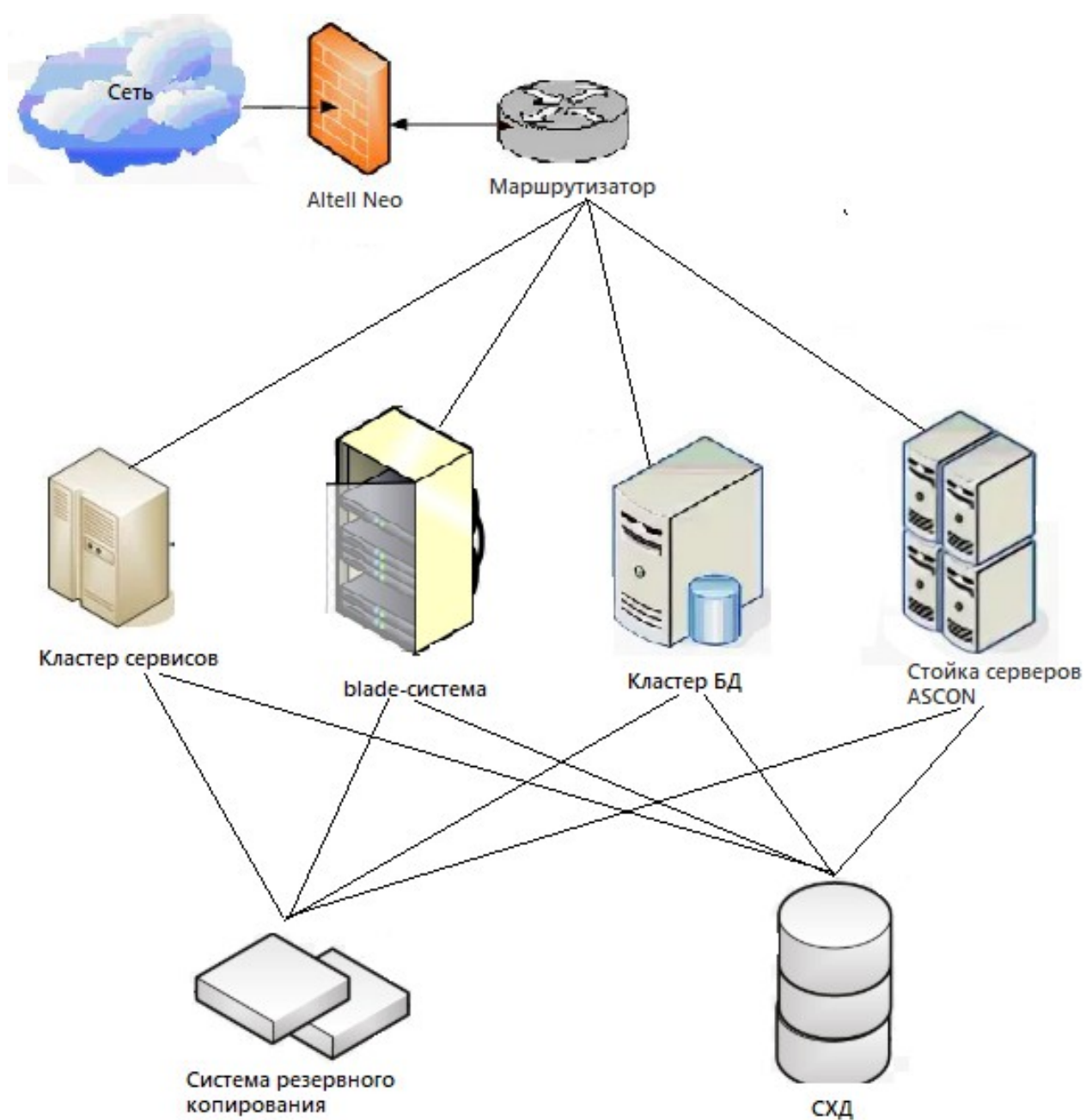


Рисунок Р.1 – Структурная схема АС

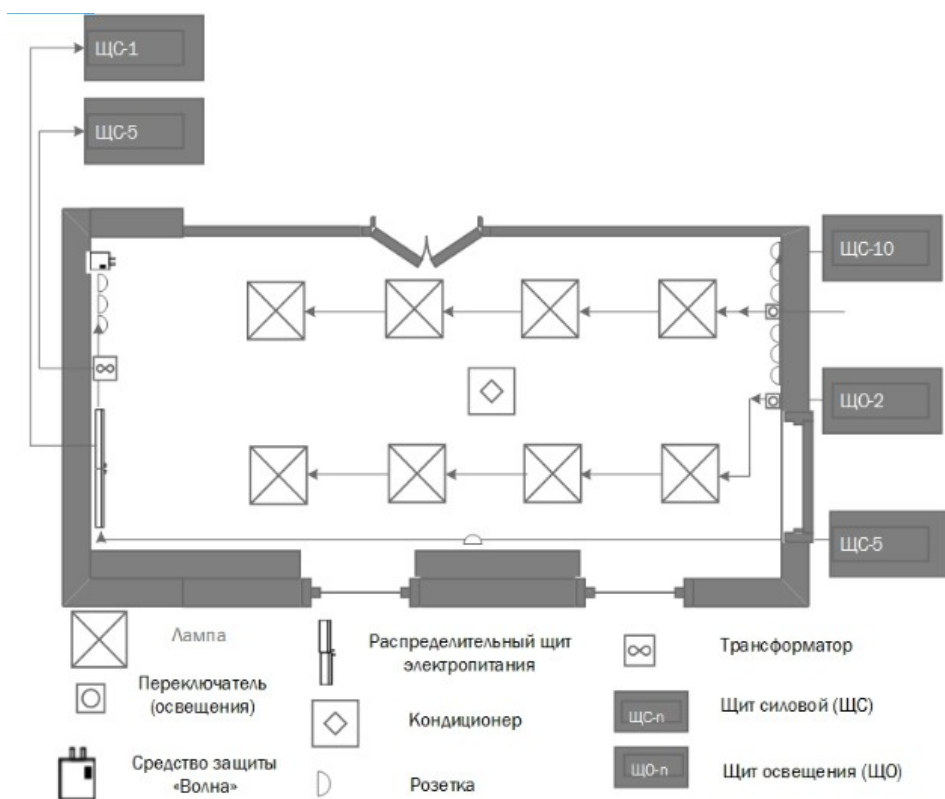


Рисунок Р.2 – Схема сети электропитания и освещения

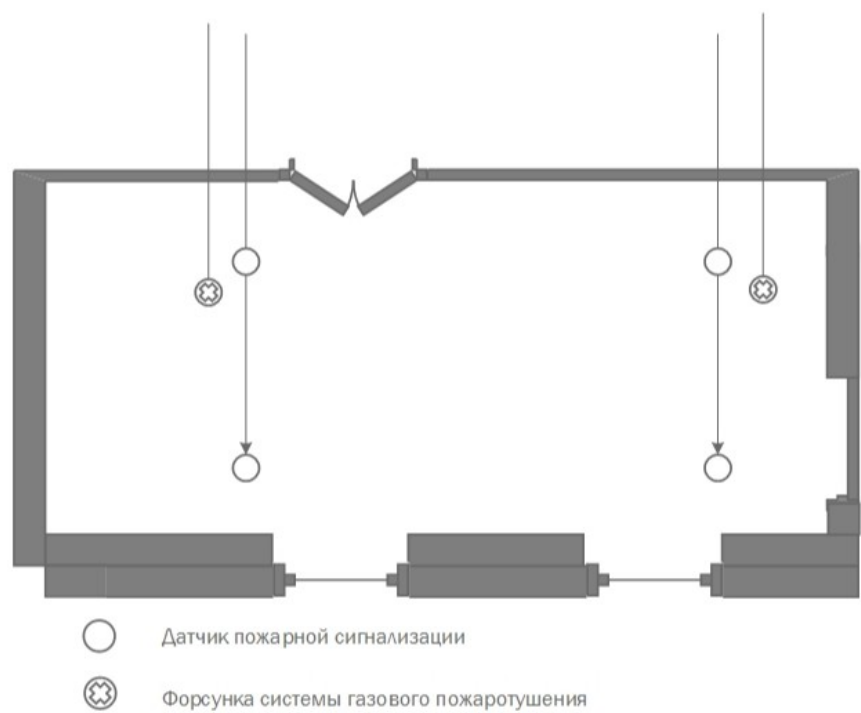


Рисунок Р.3 – Схема пожарной сигнализации и системы пожаротушения

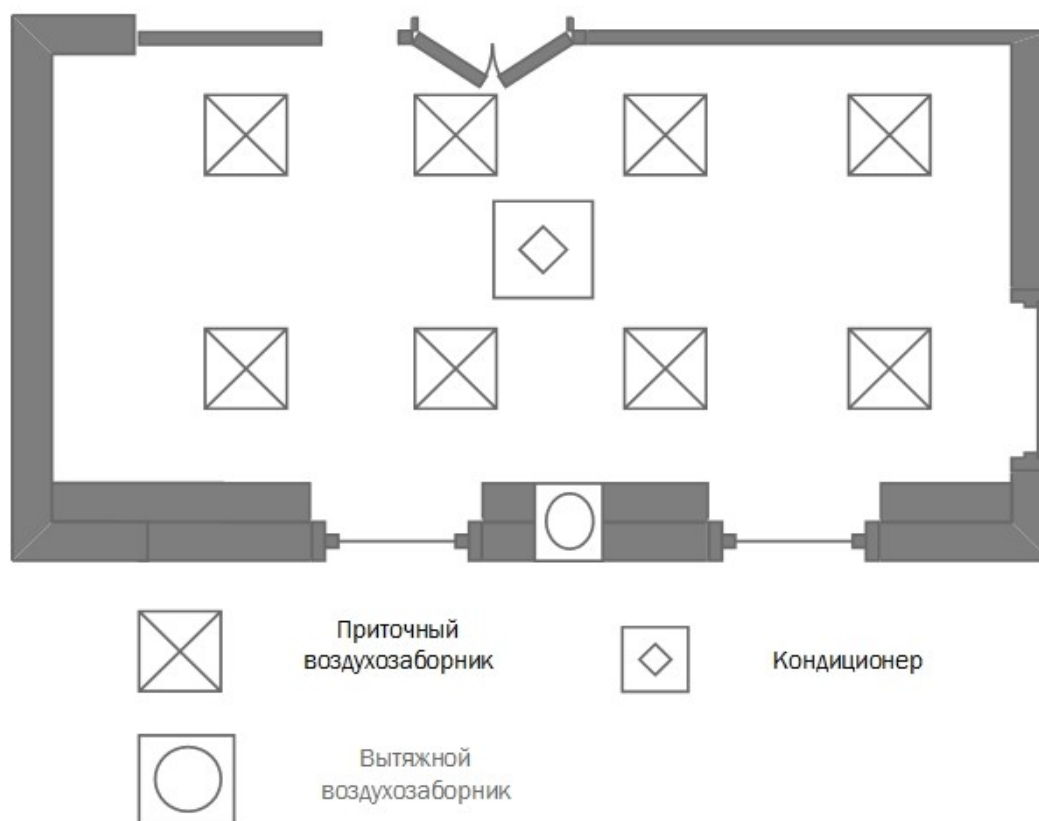


Рисунок Р.4 – Схема вентиляции и кондиционирования

Перечень средств защиты информации:

№ п/ п	Наименование и тип	Заводской номер
1	ОС Янукс 4.0	з/з В 373794 № копии: 19/389
2	Межсетевой экран Altel Neo Master	174598
3	Антивирус Kaspersky Endpoint Security 8 для Linux	с.н: СМПИ8067-12971 №сборки: Ах000105414-МР з/з: Л 895613
4	Антивирус Kaspersky Endpoint Security 10 для Windows	с.н: СМПИ8067-12971 №сборки: Ах000105414-МР з/з: Л874337
5	Kaspersky Security Center	с.н: СМПИ8067-12971

		№сборки: Ах000105414-МР з/з: Л 872210
6	Средство анализа защищенности «Сканер-ВС»	рег.№ 100000242 з/з Е 331902
7	ОС AstraLinux 1.6	з/з В 324234 № копии:20/310
8	СЗИ DallasLock	27271631

Р.4 Сведения о соответствии ОТСС объекта ВТ требованиям безопасности информации

Сведения о сертификатах на ОТСС объекта:

Сведения о специальных проверках ОТСС объекта:

Сведения о лабораторных специсследованиях ОТСС объекта:

Сведения об объектовых специсследованиях:

Сведения об аттестации объекта ВТ на соответствие требованиям по безопасности информации:

-

Р.5 Учет проведения регламентных проверок

[illegible]

Р.6 Лист регистрации изменений

(Изменение состава и размещения ОТСС, ВТСС и средств защиты объекта ВТ)

[illegible]

Приложение С
(обязательное)

Приказ о назначении администраторов безопасности и системных администраторов АС на базе серверного парка КС АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

ПРИКАЗ

О назначении администраторов безопасности и системных администраторов АС на базе серверного парка корпоративной сети АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

№ _____

г. Заречный

от «__» _____ 202_ г.

Для обеспечения безопасности при автоматизированной обработке информации в АС на базе серверного парка корпоративной сети, предназначенной для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, расположенной в АО «ФНПЦ «ПО «Старт» им. М.В.Проценко»

ПРИКАЗЫВАЮ:

С.1 Назначить администраторами безопасности, ответственными за функционирование АС в установленном штатном режиме, а также за защиту АС от не-санкционированного доступа к информации:

- отдел системного программного обеспечения;
- группу защиты информации отдела защиты информации.

С.2 Назначить системными администраторами, ответственными за установку, настройку и обновление общесистемного ПО, прикладного ПО и механиз-

мов безопасности в АС – отдел системного программного обеспечения.

С.3 Контроль за исполнением данного приказа оставляю за собой.

С.4 Приказ вступает в силу со дня его подписания.

Главный инженер	_____	ФИО
С приказом ознакомлены:	_____	ФИО
	_____	ФИО
	_____	ФИО
	_____	ФИО
	_____	ФИО

Приложение Т
(обязательное)
Протокол проверки на оригинальность