СОГЛАСОВАНО

Председатель профкома

_____ О.М. Баландина

« ___ » _____ 2018 г.

УТВЕРЖДАЮ

Директор МОУ-СОШ №1

_____ Л.П. Карманова

« ___ » _____ 2018 г.

СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

наименование вида АС

Муниципальное общеобразовательное учреждение средняя общеобразовательная школа №1

наименование объекта информатизации

МОУ-СОШ №1

сокращенное наименование АС

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На ___ листах

Подписан: Карманова Лидия Прокопьевна
DN: C=RU, O=МОУ-СОШ №1 г. Петровск-Забайкальский, CN=Карманова Лидия Прокопьевна, E=school-1-pzb@mail.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: г. Петровск-Забайкальский
Дата: 2022.04.20 14:03:00+09'00'

2018 г.

ОГЛАВЛЕНИЕ

1. СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС	- антивирусные средства
АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
АСЗИ	- автоматизированная система в защищённом исполнении
ИВС	- информационная вычислительная сеть
ИСПДн	- информационная система персональных данных
ИС	- информационная система
МЭ	- межсетевой экран
ОС	- операционная система
ПДн	- персональные данные
ПМВ	- программно-математическое воздействие
ПО	- программное обеспечение
ПЭМИН	- побочные электромагнитные излучения и наводки
САЗ	- система анализа защищённости
СЗИ	- средства защиты информации
СЗПДн	- система (подсистема) защиты персональных данных
СКЗИ	- средства криптографической защиты информации
СОВ	- система обнаружения вторжений
СФК	- среда функционирования криптосредства
ТС	- техническое средство
ТЗ	- техническое задание
УБПДн	- угрозы безопасности персональных данных
СЗКИ	- система (подсистема) защиты конфиденциальной информации
КИ	- конфиденциальная информация
УБКИ	- угрозы безопасности конфиденциальной информации

2. ОБЩИЕ СВЕДЕНИЯ

Наименование системы: Система защиты персональных данных в МОУ-СОШ №1

Исполнитель: г. Петровск-Забайкальский микрорайон Федосеевка 3

Настоящее ТЗ составлено в соответствии со следующими действующими нормативно-методическими документами:

[1] - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[3] - Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК от 18 февраля 2013 г. №21;

[4] - Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

[5] - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

[6] - Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России).

[7] - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждены приказом ФСТЭК от 11 февраля 2013 г. №17;

[8] - ГОСТ 19.201 – 78. Техническое задание. Требования к содержанию и оформлению;

[9] - Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11 февраля 2014 г.

3. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

В МОУ-СОШ №1 (далее – школа) производится обработка персональных данных, поэтому она попадает под действие закона [2].

В соответствии с [3] требуется обеспечить безопасность персональных данных. Безопасность персональных данных обеспечивается выполнением комплекса организационных и технических мер защиты, которые определяются в соответствии с нормативно-методическими документами ФСТЭК России.

Система защиты должна разрабатываться с целью предотвращения ущерба от возможной реализации нарушений характеристик безопасности. Угрозы безопасности определены в «Модели угроз безопасности персональных данных при их обработке в школе (далее - Модель угроз).

Настоящий документ разработан для решения следующих задач:

- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

- создание регламента проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

- создание регламента мероприятий, обеспечивающих контроль за обеспечением уровня защищённости персональных данных.

Требования для системы защиты формируются с учётом Модели угроз, Модели нарушителя и предварительно определённого класса.

4. ХАРАКТЕРИСТИКА ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Объектом защиты являются персональные данные, обрабатываемые в школе.

В соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах» для школы определен **второй класс защищенности (К2)**.

В соответствии с постановлением Правительства № 1119 от 01.11.2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» школы классифицирована как информационная система персональных данных (далее - ИСПДн) и установлена необходимость обеспечения **2-го уровня защищенности персональных данных (УЗ 2)**.

Обработка ПДн в школе осуществляется с использованием средств автоматизации.

ИСПДн включает в свой состав:

- выделенные автоматизированные рабочие места (АРМ), имеющие подключения к сетям связи общего пользования;
- центр обработки данных, состоящий из виртуальных серверов базы данных и Web-серверов, образующих единую информационную систему
- один физический сервер баз данных.

ИСПДн имеет подключение к сетям связи общего пользования и сетям международного информационного обмена.

По режиму обработки ПДн ИСПДн является многопользовательской.

Описание системы в целом и актуальные угрозы приведены в Модели угроз безопасности персональных данных.

5. ТРЕБОВАНИЯ К СИСТЕМЕ

В данном разделе формулируются требования по безопасности информации и предлагаются меры для их выполнения.

5.1. Требования к структуре и функционированию

Средства защиты информации от несанкционированного доступа, применяемые в ИСПДн, должны обеспечивать безопасность как физических, так и виртуальных компонентов. Должна быть реализована аутентификация администраторов виртуальной инфраструктуры и разграничение доступа к средствам управления виртуальной инфраструктурой.

Для обеспечения безопасности ПДн в ИСПДн, в рамках системы защиты персональных данных применяются следующие меры:

- Идентификация и аутентификация субъектов доступа и объектов доступа;
- Управление доступом субъектов доступа к объектам доступа;
- Ограничение программной среды;
- Защита машинных носителей информации;
- Регистрация событий безопасности;
- Антивирусная защита;
- Обнаружение (предотвращение) вторжений;
- Контроль (анализ) защищённости персональных данных;
- Защита среды виртуализации;
- Защита технических средств;
- Защита информационной системы, ее средств, систем связи передачи данных;
- Выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы;
- Управление конфигурацией информационной системы и системы защиты персональных данных.

Кроме того, при передаче информации по открытым каналам связи в качестве меры защиты информации применятся средства криптографической защиты информации и средства межсетевого экранирования.

Согласно [4], для обеспечения второго класса защищенности информационной системы требуется выполнение базового перечня требований к реализации мер защиты информации в информационной системе, указанных в таблице 1.

Таблица 1

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Требования к реализации меры защиты информации
1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия. Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC - адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства. Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации. Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора по защите информации.
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе: • определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств; • формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство; • присвоение идентификатора пользователю и (или) устройству; • предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени; • блокирование идентификатора пользователя после установленного оператором времени неиспользования.
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	Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе: • определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации; • изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы; • выдача средств аутентификации пользователям;

		• генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации); • установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля).
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации.
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.
2. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей: • определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей); • объединение учетных записей в группы (при необходимости); • верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя; • заведение, активация, блокирование и уничтожение учетных записей пользователей; • пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором; • порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов; • оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях; • уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе; • предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа. Методы управления доступом реализуются в зависимости от особенностей функционирования информационной системы, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

		• дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа; • ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности); • мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа. Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее: • фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором; • разрешение передачи информации в информационной системе только по маршруту, установленному оператором; • изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором; запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.
УПД.4	Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы	Оператором должно быть обеспечено разделение полномочий (ролей), пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа, в соответствии с разделением полномочий (ролей).
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам,	Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для

	обеспечивающим функционирование информационной системы	выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями. Оператором должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий.
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе). Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с ИАФ.4.
УПД. 10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.
УПД. 11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации. Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (веб-сайтам, порталам, иным общедоступным ресурсам). Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств). Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, регламентируются в организационно-распорядительных документах оператора по защите информации.
УПД. 13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа). Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает: • установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы; • ограничение на использование удаленного доступа в

		соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с УПД.2; • предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций); • мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы; • контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации). Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.
УПД. 14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Оператором должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе. Регламентация и контроль использования технологий беспроводного доступа должны включать: • ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с УПД.2; • предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций); • мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы; • контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой. Правила и процедуры применения технологий беспроводного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.
УПД. 15	Регламентация и контроль использования в информационной системе мобильных технических средств	Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе. В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства). Регламентация и контроль использования мобильных технических средств должны включать: • установление (в том числе документальное) видов доступа

		(беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы; • использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30; • ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с УПД.2; • мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы; • запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством. Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации.
УПД. 16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Оператором должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы. Управление взаимодействием с внешними информационными системами должно включать: • предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с УПД.2; • определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем; • определение системных учетных записей, используемых в рамках данного взаимодействия; • определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем; • определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.
УПД. 17	Обеспечение доверенной загрузки средств вычислительной техники	В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки. Доверенная загрузка должна обеспечивать: • блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность

		информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы; • контроль доступа пользователей к процессу загрузки операционной системы; • контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники. Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в организационно-распорядительных документах оператора по защите информации.
3. 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	Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы: • определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы; • настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения); • выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или не включение в домен); • контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов); • определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации. Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов. Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке («белый список»), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации

		(документируются). Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5. Оператором должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с АН3.4, а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.
4. Защита машинных носителей информации (ЗНИ)		
ЗНИ.1	Учет машинных носителей информации	Оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Учету подлежат: • съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства); • портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства); • машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках). Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации. Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации. Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).
ЗНИ.2	Управление доступом к машинным носителям персональных данных	Оператором должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в информационной системе: определение должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим: • съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства); • портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства); • машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках); • предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим

		для выполнения своих должностных обязанностей (функций); Правила и процедуры доступа к машинным носителям информации регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать: • определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе; • определение оператором категорий пользователей, которым предоставлен • доступ к разрешенным к использованию интерфейсов ввода (вывода); • принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода); • контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода). В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), могут применяться: • опечатывание интерфейсов ввода (вывода); • использование механических запирающих устройств; • удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода); • применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода). Правила и процедуры контроля использования интерфейсов ввода (вывода) регламентируются в организационно-распорядительных документах оператора по защите 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)	Оператором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации. Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны быть разработаны оператором и включены в организационно-распорядительные документы по защите информации.
5. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Оператором должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения. События безопасности, подлежащие регистрации в информационной системе, должны определяться с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации,

		доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации. События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется оператором исходя из возможностей реализации угроз безопасности информации и фиксируется в организационно-распорядительных документах по защите информации (документируется). В информационной системе как минимум подлежат регистрации следующие события: вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы; подключение машинных носителей информации и вывод информации на носители информации; запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации; попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа; попытки удаленного доступа. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с РСБ.2.
РСБ. 2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности. При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

		При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный). При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип). При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер). При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе. Состав и содержание информации о событиях безопасности, подлежащих регистрации, отражаются в организационно-распорядительных документах оператора по защите информации.
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать: возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с РСБ.1; генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 с составом и содержанием информации, определенными в соответствии с РСБ.2; хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ.1. Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.
РСБ.4	Реагирование на сбои при	В информационной системе должно осуществляться реагирование

	регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	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. Реагирование на сбои при регистрации событий безопасности должно предусматривать: • предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности; • реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности. Правила и процедуры реагирования на сбои при регистрации событий безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Оператором должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе. В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности. Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них регламентируются в организационно-распорядительных документах оператора по защите информации.
РСБ. 6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	В информационной системе должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.
РСБ. 7	Защита информации о событиях безопасности	В информационной системе должна обеспечиваться защита информации о событиях безопасности. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам. Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.
6. Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации,

		предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации. Реализация антивирусной защиты должна предусматривать: • применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы); • установку, конфигурирование и управление средствами антивирусной защиты; • предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты; • проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов); • проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов; • оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов); • определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами). Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.
АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов). Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать: • получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов); • получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов); • контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов). Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации.
7. Обнаружение вторжений (СОВ)		
СОВ.1	Обнаружение вторжений	Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию

		(носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений. Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак. Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором. Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам. Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования информационных систем. Правила и процедуры обнаружения (предотвращения) вторжений (компьютерных атак) регламентируются в организационно-распорядительных документах оператора по защите информации.
СОВ.2	Обновление базы решающих правил	Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе. Обновление базы решающих правил системы обнаружения вторжений должно предусматривать: • получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил; • получение из доверенных источников и установку обновлений базы решающих правил; • контроль целостности обновлений базы решающих правил. Правила и процедуры обновления базы решающих правил регламентируются в организационно-распорядительных документах оператора по защите информации.
8. Контроль (анализ) защищенности информации (АН3)		
АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе. Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Оператором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода. Оператором должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении)

		обновлений. Контроль установки обновлений проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с АВЗ.2, баз решающих правил систем обнаружения вторжений в соответствии с СОВ.2, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации. Правила и процедуры контроля установки обновлений программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Оператором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Оператором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).
АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.
9.Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать: • контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы; • контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы; • контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы; • тестирование с периодичностью установленной оператором функций безопасности средств защиты информации, в

		том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АНЗ.1 и АНЗ.2; • обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3. В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ. Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций. Для обеспечения возможности восстановления программного обеспечения в информационной системе должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать: • восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения; • восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации; возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.
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)	Оператором должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама). Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам. Защита от спама обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты: фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами; фильтрация а основе информации об отправителе электронного сообщения (в том числе с использованием «черных»

		списков(запрещенные отправители) и (или) «белых» списков (разрешенные отправители). Оператором должно осуществляться обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков. Правила и процедуры обнаружения и реагирования на поступление незапрашиваемой информации регламентируются в организационно- распорядительных документах оператора по защите информации.
10. Обеспечение доступности персональных данных (ОДТ)		
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Оператором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование. Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами). При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с ОЦЛ.3, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах.
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации	Оператором должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее: • резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью; • разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации; • регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации; • принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность. Правила и процедуры резервного копирования информации регламентируются в организационно-распорядительных документах оператора по защите информации.
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала	Оператором должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала. Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать: определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации; восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала; регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.

		Правила и процедуры восстановления информации с резервных машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации	Оператором должен осуществляться контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривающий: • контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности); • мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей); • мониторинг состояния и качества предоставления уполномоченным лицом (провайдером)услуг по передаче информации. Условия, права и обязанности, содержание и порядок контроля должны определяться в договоре (соглашении), заключаемом между оператором и уполномоченным лицом на предоставление вычислительных ресурсов (мощностей) или передачу информации с использованием информационно-телекоммуникационных сетей связи.
11. Защита среды виртуализации (ЗСВ)		
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться: • идентификация и аутентификация администраторов управления средствами виртуализации; • идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре; • блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации; • защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования; • защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий; • идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1 – ИАФ.7.
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных	При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться: • контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры; • контроль доступа субъектов доступа к файлам-образам

	машин	виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды; • управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа; • контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил). Кроме того, меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать: • разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг); • разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в информационной системе в целом.
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в РСБ.1, должны подлежать регистрации следующие события: • запуск (завершение) работы компонентов виртуальной инфраструктуры; • доступ субъектов доступа к компонентам виртуальной инфраструктуры; • изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения; • изменения правил разграничения доступа к компонентам виртуальной инфраструктуры. При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры. При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры. При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального

		аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры. При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры	В информационной системе должно осуществляться управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с УПД.3, ЗИС.3. При реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться: • фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования; • обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности); • контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам; • отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети; • обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов; • обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети; семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них	Оператором должно обеспечиваться управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных. При управлении перемещением виртуальных машин (контейнеров)

	данных	и обрабатываемых на них данных должны обеспечиваться: • регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения); • управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных); • управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации; • управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных). Управление перемещением виртуальных машин (контейнеров) должно предусматривать: • полный запрет перемещения виртуальных машин (контейнеров); • ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы); • ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с ОЦЛ.1. При реализации мер по контролю целостности компонентов виртуальной инфраструктуры должны обеспечиваться: • контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов); • контроль целостности состава и конфигурации виртуального оборудования; • контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин; • контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы). В информационной системе должен обеспечиваться контроль целостности резервных копий виртуальных машин (контейнеров).
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	В информационной системе должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с ОДТ.2, ОДТ.4, ОДТ.5. При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры должны обеспечиваться: • определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре; • резервное копирование виртуальных машин (контейнеров); • резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;

		• резервирование программного обеспечения виртуальной инфраструктуры; • резервирование каналов связи, используемых в виртуальной инфраструктуре; периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с АВЗ.1, АВЗ.2. При реализации соответствующих мер должны обеспечиваться: проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов; проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	В информационной системе должно обеспечиваться разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17.
12. Защита технических средств (ЗТС)		
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Оператором должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования. Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации. Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.
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 к средствам обработки информации, средствам	Оператором должны обеспечиваться 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 к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены. Контроль и управление физическим доступом должны предусматривать: • определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

	защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	• санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены; • учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены. Правила и процедуры контроля и управления физическим доступом регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Оператором должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.
13. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы	В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации(функций безопасности) и функциональных возможностей пользователей по обработке информации. Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий. Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно- технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее	Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны. Защита информации обеспечивается путем защиты каналов связи

	передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	В информационной системе должны осуществляться запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации. Запрет несанкционированной удаленной активации должен осуществляться в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечение, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы). Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) путем управления программным обеспечением. В исключительных случаях для решения установленных оператором отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств. При этом должно быть обеспечено определение и фиксирование в организационно-распорядительных документах по защите информации (документирование) перечня периферийных устройств, для которых допускается возможность удаленной активации и обеспечен контроль за активацией таких устройств.
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	Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента) в информационной системе, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий. При контроле использования технологий мобильного кода должно быть обеспечено: определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в информационной системе; определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций информационной системы, для которых необходимо применение технологии мобильного кода; регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода; исключение возможности использования запрещенного мобильного кода в информационной системе, а также внедрение мобильного кода в местах, не разрешенных для его установки. Правила и процедуры контроля использования технологий мобильного кода регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗИС.8	Контроль санкционированного и	Оператором должны осуществляться контроль санкционированного и исключение несанкционированного

	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	использования технологий передачи речи в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи. При контроле использования технологий передачи речи должно быть обеспечено: • определение перечня технологий (сервисов) передачи речи разрешенных и (или) запрещенных для использования в информационной системе; • определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи речи в соответствии с установленными ролями; • реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи речи; • регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи речи; • исключение возможности использования запрещенной технологии передачи речи в информационной системе, а также разработки, приобретения и внедрения технологий передачи речи субъектам доступа (пользователям), которым не разрешено ее использование. Технология передачи речи включает, в том числе, передачу речи через Интернет (в частности VoIP). Правила и процедуры контроля использования технологий передачи речи регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи видеоинформации в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи видеоинформации, их анализ и реагирование на нарушения, связанные с использованием технологий передачи видеоинформации. При контроле использования технологий передачи видеоинформации должно быть обеспечено: • определение перечня технологий (сервисов) передачи видеоинформации разрешенных и (или) запрещенных для использования в информационной системе; • определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи видеоинформации в соответствии с установленными ролями; • реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи видеоинформации; • регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи видеоинформации; • исключение возможности использования запрещенной технологии передачи видеоинформации в информационной системе, а также разработки, приобретения и внедрения технологий передачи видеоинформации субъектов доступа (пользователям), которым не разрешено ее использование. Технология передачи видеоинформации включает, в том числе, применение технологий видеоконференцсвязи. Правила и процедуры контроля передачи видеоинформации регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗИС.11	Обеспечение подлинности сетевых соединений	В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том

	(сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»). Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация в соответствии с ИАФ.2 и ЗИС.10. Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов (в частности в соответствии с ЗИС.3).
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю	Оператором должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю. Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться: определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты); обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с ЗИС.3; регистрация событий, связанных с отправкой информации другому пользователю в соответствии с РСБ.2.
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя	Оператором должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя. Для исключения возможности отрицания пользователем факта получения информации должны осуществляться: определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты); обеспечение целостности полученной информации в соответствии с ЗИС.3; регистрация событий, связанных с получением информации от другого пользователя в соответствии с РСБ.2.
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором, направленных на обеспечение их конфиденциальности и целостности. Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	Оператором должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы. Сегментирование информационной системы проводится с целью построения многоуровневой (эшелонированной) системы защиты информации путем построения сегментов на различных физических доменах или средах. Принципы сегментирования информационной системы определяются оператором с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и должны заключаться в снижении вероятности реализации угроз и (или) их локализации в рамках одного сегмента. Сегментирование информационной системы также может

		проводиться с целью разделения информационной системы на сегменты, имеющие различные классы защищенности информационной системы. При сегментировании информационной системы должна быть обеспечена защита периметров сегментов информационной системы в соответствии с УПД.3 и ЗИС.23.
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе.
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	В информационной системе должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы. Оператором должен быть определен перечень угроз (типов угроз) безопасности информации, направленных на отказ в обслуживании. Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в информационной системе мер защиты информационной системы в соответствии с ЗИС.23 и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с ОДТ.2, ОДТ.4 и ОДТ.5.
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	В информационной системе должна осуществляться защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая: • управление (контроль) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы); • обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации). Правила и процедуры защиты периметра информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения	В информационной системе должно осуществляться завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения.
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	Оператором должна осуществляться защита применяемых в информационной системе мобильных технических средств.
14. Выявление инцидентов и реагирование и реагирование на них (ИНЦ)		
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование	В информационной системе условия оговариваются в распорядительных документах.

	на них	
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	В информационной системе должен быть заведен журнал регистрации инцидентов.
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	В информационной системе условия оговариваются в распорядительных документах.
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 повторного возникновения инцидентов	
15. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	В информационной системе условия оговариваются в распорядительных документах.
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных	
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	

Криптографические меры защиты информации, предназначенные для исключения НСД к защищаемой информации при ее передачи, между центром обработки данных и рабочими местами отдаленных филиалов, по каналам связи сетей общего пользования и (или) международного обмена. Криптографическая защита информации реализуется путем внедрения сертифицированных программно-аппаратных комплексов для центра обработки данных и отдаленных филиалов в виде программных модулей с функциями межсетевого экранирования. Обеспечение шифрования сетевого трафика, передаваемого по открытым каналам связи между центром обработки данных и отдаленными филиалами осуществляется по ГОСТ 28147-89 с длиной ключа не менее 256 бит.

При организации криптографической защиты информации имеется возможность:

- использование удостоверяющего центра с целью использования механизмов электронной подписи в прикладном программном обеспечении;

- организации отказоустойчивых решений для обеспечения доступности информационных ресурсов центра обработки данных;

- совместимости с технологией защиты информации КриптоПро для реализации защищенного взаимодействия со смежными информационными системами.

Межсетевое экранирование предназначено для защиты информационно-вычислительной сети от несанкционированного доступа со стороны внешних сетей, в том числе сети Интернет. Межсетевое экранирование реализуется в виде сертифицированных программно-аппаратных комплексов с возможностью централизованного управления конфигурацией устройств.

Для адаптации базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы исключаются меры, не используемые в информационной системе и добавляются рекомендуемые меры, указанные в таблице 2.

Таблица 2

Название и назначение меры защиты информации		
Условное обозначение и номер меры	**Меры защиты информации в ИС**	**Требования к реализации меры защиты информации**
ИСКЛЮЧАЮТСЯ		
2. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Исключается ввиду отсутствия
9.Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к	Исключается ввиду отсутствия

	функционированию информационной системы (защита от спама)	
13. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Исключается ввиду отсутствия

Уточненные и усиленные меры защиты информации для обеспечения второго класса защищенности информационной системы, указаны в таблице 3

Таблица 3

Условное обозначение и номер меры	**Меры защиты информации в информационных системах**	**Требования к реализации меры защиты информации**
1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. **Требования к усилению ИАФ.1 для класса защищенности 2:** в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов) с использованием сети связи общего пользования, в том числе сети интернет; в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей) с использованием сети связи общего пользования, в том числе сети интернет.
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия. Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC- адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства. Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации. Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора по защите информации.
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе: • определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств; • формирование идентификатора, который однозначно

		идентифицирует пользователя и (или) устройство; • присвоение идентификатора пользователю и (или) устройству; • предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени; • блокирование идентификатора пользователя после установленного оператором времени неиспользования. **Требования к усилению ИАФ.3 для класса защищенности 2:** оператором должно быть исключено повторное использование идентификатора пользователя в течение не менее одного года; оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 90 дней.
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	Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе: • определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации; • изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы; • выдача средств аутентификации пользователям; • генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации); • установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля). **Требования к усилению ИАФ.4 для класса защищенности 2:** длина пароля не менее шести символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней.
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации.
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.
2. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних	Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей: • определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения;

	пользователей	гостевая (анонимная), временная и (или) иные типы записей); • объединение учетных записей в группы (при необходимости); • верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя; • заведение, активация, блокирование и уничтожение учетных записей пользователей; • пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором; • порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов; • оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях; • уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе; • предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами. **Требования к усилению УПД.1 для класса защищенности 2:** • оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей; • в информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования; • в информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования более 90 дней;
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа. Методы управления доступом реализуются в зависимости от особенностей функционирования информационной системы, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов: • дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа; • ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности); • мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа,

		отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа. Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа. **Требования к усилению УПД.2 для класса защищенности 2:** • в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему; • в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам; • в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением;
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее: • фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором; • разрешение передачи информации в информационной системе только по маршруту, установленному оператором; • изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором; • запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.
УПД.4	Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы	Оператором должно быть обеспечено разделение полномочий (ролей), пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа, в соответствии с разделением полномочий (ролей).
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

		Оператором должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий.
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе). Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с ИАФ.4.
УПД. 10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя. **Требования к усилению УПД.10 для класса защищенности 2:** • в информационной системе должно обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя до 15 минут; • в информационной системе на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы);
УПД. 11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации. Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (веб-сайтам, порталам, иным общедоступным ресурсам). Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств). Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, регламентируются в организационно-распорядительных документах оператора по защите информации.
УПД. 13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа). Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает: • установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа

		информационной системы; • ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с УПД.2; • предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций); • мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы; • контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации). Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению УПД.13 для класса защищенности 2:** • в информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы; • в информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации; • в информационной системе обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой.
УПД. 15	Регламентация и контроль использования в информационной системе мобильных технических средств	Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе. В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства). Регламентация и контроль использования мобильных технических средств должны включать: • установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы; • использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30; • ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с УПД.2;

		• мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы; • запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством. Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению УПД.15 для класса защищенности 2:** • оператором обеспечивается запрет использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации; • оператором обеспечивается запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);
УПД. 16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Оператором должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы. Управление взаимодействием с внешними информационными системами должно включать: • предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с УПД.2; • определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем; • определение системных учетных записей, используемых в рамках данного взаимодействия; • определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем; • определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем. **Требования к усилению УПД.16 для класса защищенности 2:** Оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий: • при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы; • при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о

		защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).
УПД. 17	Обеспечение доверенной загрузки средств вычислительной техники	В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки. Доверенная загрузка должна обеспечивать: • блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы; • контроль доступа пользователей к процессу загрузки операционной системы; • контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники. Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению УПД.17 для класса защищенности 2:** в информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения;
3. 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	Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы: • определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы; • настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения); • выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или не включение в домен); • контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов); • определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации. Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.
ОПС.3	Установка (инсталляция) только разрешенного к	Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе

	использованию программного обеспечения и (или) его компонентов	программного обеспечения и (или) его компонентов. Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке («белый список»), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации (документируются). Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5. Оператором должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с АНЗ.4, а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.
4. Защита машинных носителей информации (ЗНИ)		
ЗНИ.1	Учет машинных носителей информации	Оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Учету подлежат: • съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства); • портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства); • машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках). Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации. Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации. Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски). **Требования к усилению ЗНИ.1 для класса защищенности 2:** оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая информацию о возможности использования машинного носителя информации вне информационной системы
ЗНИ.2	Управление доступом к	Оператором должны быть реализованы следующие функции по

	машинным носителям персональных данных	управлению доступом к машинным носителям информации, используемым в информационной системе: определение должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим: • съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства); • портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства); • машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках); • предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций); Правила и процедуры доступа к машинным носителям информации регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать: • определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе; • определение оператором категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода); • принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода); • контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода). В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), могут применяться: • опечатывание интерфейсов ввода (вывода); • использование механических запирающих устройств; • удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода); • применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода). Правила и процедуры контроля использования интерфейсов ввода (вывода) регламентируются в организационно-распорядительных документах оператора по защите 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)	Оператором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации. Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации

		должны быть разработаны оператором и включены в организационно-распорядительные документы по защите информации. **Требования к усилению ЗНИ.8 для класса защищенности 2:** оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации; оператором должны применяться меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;
5. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Оператором должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения. События безопасности, подлежащие регистрации в информационной системе, должны определяться с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации. События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется оператором исходя из возможностей реализации угроз безопасности информации и фиксируется в организационно-распорядительных документах по защите информации (документируется). В информационной системе как минимум подлежат регистрации следующие события: вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы; подключение машинных носителей информации и вывод информации на носители информации; запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации; попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа; попытки удаленного доступа. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с РСБ.2. **Требования к усилению РСБ.1 для класса защищенности 2:**

		• оператором должен обеспечиваться 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; • оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей; • оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом осуществляется хранение только записей о выявленных событиях безопасности;
РСБ. 2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности. При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный). При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип). При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта

		доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер). При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе. Состав и содержание информации о событиях безопасности, подлежащих регистрации, отражаются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению РСБ.2 для класса защищенности 2:** в информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающую полнотекстовую запись привилегированных команд (команд, управляющих системными функциями).
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать: возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с РСБ.1; генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 с составом и содержанием информации, определенными в соответствии с РСБ.2; хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ.1. Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению РСБ.3 для класса защищенности 2:** в информационной системе должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.
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	В информационной системе должно осуществляться 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. Реагирование на сбои при регистрации событий безопасности должно предусматривать: • предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности; • реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров

		сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности. Правила и процедуры реагирования на сбои при регистрации событий безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Оператором должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе. В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности. Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них регламентируются в организационно-распорядительных документах оператора по защите информации.
РСБ. 6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	В информационной системе должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.
РСБ. 7	Защита информации о событиях безопасности	В информационной системе должна обеспечиваться защита информации о событиях безопасности. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам. Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению РСБ.7 для класса защищенности 2:** в информационной системе обеспечивается резервное копирование записей регистрации (аудита).
6. Антивирусная защита (АВЗ)		
АВ3.1	Реализация антивирусной защиты	Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации. Реализация антивирусной защиты должна предусматривать: • применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других

		средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы); • установку, конфигурирование и управление средствами антивирусной защиты; • предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты; • проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов); • проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов; • оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов); • определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами). Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению АВ3.1 для класса защищенности 2:** в информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности; в информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах);
АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов). Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать: • получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов); • получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов); • контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов). Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению АВ3.2 для класса защищенности 2:** в информационной системе должно обеспечиваться централизованное управление обновлением базы данных

		признаков вредоносных компьютерных программ (вирусов).
7. Обнаружение вторжений (СОВ)		
СОВ.1	Обнаружение вторжений	Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений. Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак. Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором. Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам. Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования информационных систем. Правила и процедуры обнаружения (предотвращения) вторжений (компьютерных атак) регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению СОВ.1 для класса защищенности 2:** в информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы.
СОВ.2	Обновление базы решающих правил	Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе. Обновление базы решающих правил системы обнаружения вторжений должно предусматривать: • получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил; • получение из доверенных источников и установку обновлений базы решающих правил; • контроль целостности обновлений базы решающих правил. Правила и процедуры обновления базы решающих правил регламентируются в организационно-распорядительных документах оператора по защите информации.
8. Контроль (анализ) защищенности информации (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе. Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей. **Требования к усилению АНЗ.1 для класса защищенности 2:** оператором обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно- аппаратных платформ, уязвимостей программного

		обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей; оператор должен уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях; оператором предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности).
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Оператором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода. Оператором должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений. Контроль установки обновлений проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с АВ3.2, баз решающих правил систем обнаружения вторжений в соответствии с СОВ.2, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации. Правила и процедуры контроля установки обновлений программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Оператором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. **Требования к усилению АН3.3 для класса защищенности 2:** в информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации;
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Оператором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация). **Требования к усилению АН3.4 для класса защищенности 2:** в информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты

		информации.
АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе. **Требования к усилению АН3.5 для класса защищенности 2:** в информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей;.
9.Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать: • контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы; • контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы; • контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы; • тестирование с периодичностью установленной оператором функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АН3.1 и АН3.2; • обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3. В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ. Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению ОЦЛ.1 для класса защищенности 2:** в информационной системе контроль целостности средств защиты информации должен осуществляться по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы; оператором исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды;
ОЦЛ.3	Обеспечение возможности восстановления	Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при

	программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	возникновении нештатных ситуаций. Для обеспечения возможности восстановления программного обеспечения в информационной системе должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать: • восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения; • восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации; возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.
10. Обеспечение доступности персональных данных (ОДТ)		
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Оператором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование. Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами). При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с ОЦЛ.3, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах.
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации	Оператором должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее: • резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью; • разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации; • регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации; • принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность. Правила и процедуры резервного копирования информации регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению ОДТ.4 для класса защищенности 2:** оператором должна осуществляться с установленной

		имперiодичностью проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий (периодичность проверки работоспособности определяется оператором); оператором должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала	Оператором должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала. Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать: определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации; восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала; регистрация событий, связанных восстановлением информации с резервных машинных носителей информации. Правила и процедуры восстановления информации с резервных машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации	Оператором должен осуществляться контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривающий: • контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности); • мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей); • мониторинг состояния и качества предоставления уполномоченным лицом (провайдером)услуг по передаче информации. Условия, права и обязанности, содержание и порядок контроля должны определяться в договоре (соглашении), заключаемом между оператором и уполномоченным лицом на предоставление вычислительных ресурсов (мощностей) или передачу информации с использованием информационно-телекоммуникационных сетей связи.
11. Защита среды виртуализации (ЗСВ)		
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами	При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться: • идентификация и аутентификация администраторов управления средствами виртуализации; • идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в

	виртуализации	виртуальной инфраструктуре; • блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации; • защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования; • защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий; • идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1 – ИАФ.7. **Требования к усилению ЗСВ.1 для класса защищенности 2:** в информационной системе должны обеспечиваться взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе.
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться: • контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры; • контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды; • управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа; • контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил). Кроме того, меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать: • разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг); • разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в информационной системе в целом. **Требования к усилению ЗСВ.2 для класса защищенности 2:** в информационной системе должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры; в информационной системе должен обеспечиваться доступ к конфигурации виртуальных машин только администраторам

		виртуальной инфраструктуры.
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в РСБ.1, должны подлежать регистрации следующие события: • запуск (завершение) работы компонентов виртуальной инфраструктуры; • доступ субъектов доступа к компонентам виртуальной инфраструктуры; • изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения; • изменения правил разграничения доступа к компонентам виртуальной инфраструктуры. При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры. При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры. При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры. При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке

		изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры	В информационной системе должно осуществляться управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с УПД.3, ЗИС.3. При реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться: • фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования; • обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности); • контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам; • отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети; • обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов; • обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети; семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Оператором должно обеспечиваться управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных. При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных должны обеспечиваться: • регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения); • управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных); • управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации; • управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных). Управление перемещением виртуальных машин (контейнеров) должно предусматривать: • полный запрет перемещения виртуальных машин (контейнеров); • ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы); • ограничение перемещения виртуальных машин

		(контейнеров) между сегментами информационной системы. **Требования к усилению ЗСВ.6 для класса защищенности 2:** оператором должно обеспечиваться перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах информационной системы только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных);
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с ОЦЛ.1. При реализации мер по контролю целостности компонентов виртуальной инфраструктуры должны обеспечиваться: • контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов); • контроль целостности состава и конфигурации виртуального оборудования; • контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин; • контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы). В информационной системе должен обеспечиваться контроль целостности резервных копий виртуальных машин (контейнеров). **Требования к усилению ЗСВ.7 для класса защищенности 2:** в информационной системе должен обеспечиваться контроль состава аппаратной части компонентов виртуальной инфраструктуры.
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	В информационной системе должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с ОДТ.2, ОДТ.4, ОДТ.5. При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры должны обеспечиваться: • определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре; • резервное копирование виртуальных машин (контейнеров); • резервное копирование данных, обрабатываемых в виртуальной инфраструктуре; • резервирование программного обеспечения виртуальной инфраструктуры; • резервирование каналов связи, используемых в виртуальной инфраструктуре; периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с АВЗ.1, АВЗ.2. При реализации соответствующих мер должны обеспечиваться:

		проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов; проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов. **Требования к усилению ЗСВ.9 для класса защищенности 2:** в информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты.
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	В информационной системе должно обеспечиваться разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17.
12. Защита технических средств (ЗТС)		
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Оператором должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования. Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации. Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.
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 к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Оператором должны обеспечиваться 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 к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены. Контроль и управление физическим доступом должны предусматривать: ● определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены; ● санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены; ● учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены. Правила и процедуры контроля и управления физическим

		доступом регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Оператором должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.
13. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы	В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации(функций безопасности) и функциональных возможностей пользователей по обработке информации. Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий. Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно- технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами. **Требования к усилению ЗИС.1 для класса защищенности 2:** в информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов безопасности.
ЗИС.3	Обеспечение защиты персональных данных 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	Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны. Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

	беспроводным каналам связи	
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	В информационной системе должны осуществляться запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации. Запрет несанкционированной удаленной активации должен осуществляться в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечение, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы). Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) путем управления программным обеспечением. В исключительных случаях для решения установленных оператором отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств. При этом должно быть обеспечено определение и фиксирование в организационно-распорядительных документах по защите информации (документирование) перечня периферийных устройств, для которых допускается возможность удаленной активации и обеспечен контроль за активацией таких устройств. **Требования к усилению ЗИС.5 для класса защищенности 2:** в информационной системе должна обеспечиваться возможность физического отключения периферийных устройств (например, отключение при организации и проведении совещаний в помещениях, где размещены видеокамеры и микрофоны).
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	Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента) в информационной системе, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий. При контроле использования технологий мобильного кода должно быть обеспечено: определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в информационной системе; определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций информационной системы, для которых необходимо применение технологии мобильного кода; регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода; исключение возможности использования запрещенного мобильного кода в информационной системе, а также внедрение мобильного кода в местах, не разрешенных для его установки. Правила и процедуры контроля использования технологий мобильного кода регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению ЗИС.7 для класса защищенности 2:**

		в информационной системе должны быть реализованы механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода) и иные действия, определяемые оператором.
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	Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи речи в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи. При контроле использования технологий передачи речи должно быть обеспечено: • определение перечня технологий (сервисов) передачи речи разрешенных и (или) запрещенных для использования в информационной системе; • определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи речи в соответствии с установленными ролями; • реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи речи; • регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи речи; • исключение возможности использования запрещенной технологии передачи речи в информационной системе, а также разработки, приобретения и внедрения технологий передачи речи субъектам доступа (пользователям), которым не разрешено ее использование. Технология передачи речи включает, в том числе, передачу речи через Интернет (в частности VoIP). Правила и процедуры контроля использования технологий передачи речи регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи видеоинформации в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи видеоинформации, их анализ и реагирование на нарушения, связанные с использованием технологий передачи видеоинформации. При контроле использования технологий передачи видеоинформации должно быть обеспечено: • определение перечня технологий (сервисов) передачи видеоинформации разрешенных и (или) запрещенных для использования в информационной системе; • определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи видеоинформации в соответствии с установленными ролями; • реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи видеоинформации; • регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи видеоинформации; • исключение возможности использования запрещенной технологии передачи видеоинформации в информационной системе, а также разработки, приобретения и внедрения

		технологий передачи видеоинформации субъектов доступа (пользователям), которым не разрешено ее использование. Технология передачи видеоинформации включает, в том числе, применение технологий видеоконференцсвязи. Правила и процедуры контроля передачи видеоинформации регламентируются в организационно-распорядительных документах оператора по защите информации.
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»). Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация в соответствии с ИАФ.2 и ЗИС.10. Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов (в частности в соответствии с ЗИС.3).
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю	Оператором должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю. Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться: определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты); обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с ЗИС.3; регистрация событий, связанных с отправкой информации другому пользователю в соответствии с РСБ.2.
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя	Оператором должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя. Для исключения возможности отрицания пользователем факта получения информации должны осуществляться: определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты); обеспечение целостности полученной информации в соответствии с ЗИС.3; регистрация событий, связанных с получением информации от другого пользователя в соответствии с РСБ.2.
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором, направленных на обеспечение их конфиденциальности и целостности. Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты	Оператором должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы. Сегментирование информационной системы проводится с целью

	периметров сегментов информационной системы	построения многоуровневой (эшелонированной) системы защиты информации путем построения сегментов на различных физических доменах или средах. Принципы сегментирования информационной системы определяются оператором с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и должны заключаться в снижении вероятности реализации угроз и (или) их локализации в рамках одного сегмента. Сегментирование информационной системы также может проводиться с целью разделения информационной системы на сегменты, имеющие различные классы защищенности информационной системы. При сегментировании информационной системы должна быть обеспечена защита периметров сегментов информационной системы в соответствии с УПД.3 и ЗИС.23.
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	В информационной системе должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы. Оператором должен быть определен перечень угроз (типов угроз) безопасности информации, направленных на отказ в обслуживании. Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в информационной системе мер защиты информационной системы в соответствии с ЗИС.23 и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с ОДТ.2, ОДТ.4 и ОДТ.5.
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	В информационной системе должна осуществляться защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая: • управление (контроль) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы); • обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации). Правила и процедуры защиты периметра информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации. **Требования к усилению ЗИС.23 для класса защищенности 2:** в информационной системе должна быть обеспечена возможность размещения публичных общедоступных ресурсов (в частности общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы; в информационной системе должно быть обеспечено предоставление доступа во внутренние сегменты информационной системы (демилитаризованную зону) из

		внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия); оператор должен ограничить количество точек доступа в информационную систему из внешних информационных систем и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков; оператором в информационной системе: • должен применяться отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса; • должны быть установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса; • должна обеспечиваться защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или криптографических методов в соответствии с законодательством Российской Федерации; в информационной системе должен быть исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»)
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения	В информационной системе должно осуществляться завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения.
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	Оператором должна осуществляться защита применяемых в информационной системе мобильных технических средств.
14. Выявление инцидентов и реагирование и реагирование на них (ИНЦ)		
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	В информационной системе условия оговариваются в распорядительных документах.
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	В информационной системе должен быть заведен журнал регистрации инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	В информационной системе условия оговариваются в распорядительных документах.
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 повторного возникновения инцидентов	
15. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	В информационной системе условия оговариваются в распорядительных документах
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных	
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	

В соответствии [7] для обеспечения защиты персональных данных в информационной системе второго класса защищенности, имеющей взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена, применяются:

- средства вычислительной техники не ниже 5 класса;

- системы обнаружения вторжения и средства антивирусной защиты не ниже 4 класса;

- межсетевые экраны не ниже 3 класса;

- средства криптографической защиты не ниже КС2.

5.2. Требования к численности и квалификации персонала, режиму его работы

Квалификация персонала должна быть достаточной для осуществления им настройки общесистемных и сетевых сервисов СЗПДн и настройки СЗИ СЗПДн.

Персонал СЗПДн должен осуществлять обслуживание и эксплуатацию СЗПДн по рабочим дням в рабочее время, с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности СЗПДн.

5.3. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн

При создании СЗПДн должны использоваться унифицированные, однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, удобства эксплуатации.

Климатические условия эксплуатации компонентов СЗПДн должны соответствовать требованиям ГОСТ 21552-84 и ГОСТ 27201-87.

Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

- оперативное обслуживание,
- профилактические работы.

Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств, целостности ресурсов системы. Оперативное обслуживание не должно нарушать выполнения функций СЗПДн в целом.

Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗПДн, для которых такое обслуживание предусмотрено эксплуатационной документацией.

Объём и порядок выполнения технического обслуживания технических и программных средств СЗПДн должны определяться эксплуатационной документацией.

Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть запрещён.

Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗПДн.

5.4. Требования к программному обеспечению

Выбор программных (программно-аппаратных) средств защиты должен проводиться с учётом средств защиты, эксплуатируемых у Заказчика.

Предлагаемое к использованию ПО должно быть лицензировано фирмой-производителем.

Решения по использованию ПО должны приниматься с учётом обеспечения поддержки его функционирования производителем или поставщиком данного ПО.

В процессе эксплуатации СЗПДн лицензии на дополнительные функции ПО должны поддерживаться в актуальном состоянии.

Средства защиты информации, входящие в состав СЗПДн, должны быть сертифицированы на соответствие требованиям руководящих документов ФСТЭК по защите от НСД к информации.

5.5. Требования к техническому обеспечению

Выбор аппаратных (программно-аппаратных) средств защиты должен проводиться с учётом средств защиты, эксплуатируемых у Заказчика.

Аппаратные компоненты должны обеспечивать функции диагностики, резервирования и взаимозаменяемости.

В составе СЗПДн должны использоваться аппаратные (программно-аппаратные) СЗИ, сертифицированные по требованиям ФСТЭК России и ФСБ России.

5.6. Требования к организационному обеспечению

Должна осуществляться физическая охрана помещений, в которых находятся средства ИСПДн (устройства и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надёжных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.

Мониторы АРМ должны располагаться таким образом, чтобы препятствовать возможности несанкционированного визуального съёма информации с них.

Для обеспечения безопасности персональных данных, обрабатываемых с использованием виртуальной инфраструктуры необходимо обеспечить такую модель безопасности, при которой администратор мог бы в полном объеме выполнять свои функции по администрированию виртуальной инфраструктуры, не имея при этом доступа к данным, обрабатываемым внутри виртуальных машин.

Также необходим специальный механизм управления правами в системе разграничения доступа, при котором администратор безопасности не имеет прав на систему виртуализации, а администратор виртуальной инфраструктуры, в свою очередь, не имеет полномочий на назначение прав в системе разграничения доступа. Подобный механизм может быть реализован с помощью сертифицированных СЗИ.

6. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Работы по созданию СЗПДн осуществляются по этапам:

1. Предпроектный этап:
   - обследование ИСПДн;
   - классификация ИСПДн;
   - разработка Модели угроз;
   - разработка Технического задания (ТЗ) на создание СЗПДн.
2. Этап проектирования:
   - разработка спецификации системы защиты ИСПДн;
   - разработка эксплуатационной документации (в случае необходимости);
   - разработка организационно-распорядительной документации (в случае необходимости).
3. Ввод в действие:
   - поставка оборудования и ПО согласно спецификации, разработанной на этапе проектирования;
   - монтаж оборудования, установка и настройка ПО в соответствии с проектными решениями;
   - предварительные испытания и ввод в эксплуатацию;
   - аттестационные испытания системы защиты информации на соответствие требованиям по безопасности информации;
   - в случае положительного заключения по результатам аттестационных испытаний выдача аттестата соответствия требованиям по безопасности информации.

На предпроектном этапе проводится обследование ИСПДн:

- уточняется перечень ПДн, подлежащих защите;
- уточняется информация о категориях и составе ПДн, обрабатываемых автоматизированными и неавтоматизированными способами; проводится анализ состава ПДн в ИСПДн, собирается информация о защищённости ПДн;
- уточняются условия расположения объекта защиты относительно границ контролируемой зоны;
- уточняются конфигурация и топология ИСПДн и систем связи в целом и их компонентов, физические, функциональные и технологические связи как

внутри этих систем, так и с другими системами различного уровня и назначения;

- уточняются состав технических средств и систем, предполагаемых к использованию в СЗПДн, условия их расположения, общесистемные и прикладные программные средства;
- уточняются режимы обработки информации в ИСПДн в целом и в отдельных ее компонентах; для ИСПДн производится анализ собранной информации об угрозах и их показателях для разработки Модели угроз;
- уточняется класс ИСПДн;
- разрабатывается Модель угроз для ИСПДн на основе методических рекомендаций ФСТЭК России, а также Модель нарушителя (в случае необходимости) на основе методических рекомендаций ФСБ России;
- уточняется степень участия сотрудников в обработке информации, характер их взаимодействия между собой и с администратором ИБ;
- разрабатывается ТЗ на создание СЗПДн.

На этапе проектирования разрабатывается спецификация системы защиты персональных данных, а также необходимая эксплуатационная и организационно-распорядительная документация.

На этапе ввода в действие выполняются следующие работы:

- поставка оборудования и ПО на площадку Пользователя согласно спецификации, разработанной на этапе проектирования;
- монтаж оборудования, установка и настройка ПО в соответствии с проектными решениями;
- предварительные испытания и ввод в эксплуатацию;
- инструктаж персонала Пользователя по работе с основными компонентами СЗПДн;
- в случае необходимости проводится обучение персонала Пользователя использованию СЗИ, применяемых в СЗПДн.
- аттестационные испытания системы защиты информации на соответствие требованиям по безопасности информации

7. ПОРЯДОК КОНТРОЛЯ И ПРИЁМКИ

Контроль и приёмка работ осуществляются на основании ТЗ.

Содержание отчётных материалов согласуется на уровне специалистов Заказчика и Исполнителя в соответствии с ТЗ. Исполнитель должен быть заранее проинформирован Заказчиком о порядке и сроках согласования отчётных материалов, перечне вопросов, которые подлежат согласованию, составе согласующих подразделений и организаций и степени их компетенции при согласовании тех или иных разделов отчётной документации.

В случае необходимости может быть проведена защита предлагаемых решений в процессе технического совещания специалистов Исполнителя и Заказчика.

Настоящее ТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование, и утверждение ТЗ.

Замечания по отчётным материалам должны быть представлены Исполнителю с техническим обоснованием в письменной форме.

Испытания проводятся на площадках развертывания СЗПДн.

Сроки приемки работ определяются календарными планами и сроками проведения соответствующих этапов в соответствии с техническими требованиями на создание СЗПДн.

8. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

Реализация требований настоящего раздела не входит в перечень работ, выполняемых Исполнителем в рамках создания СЗПДн. Данные требования должны быть реализованы Заказчиком.

На этапе ввода СЗПДн должен быть определен перечень должностей, допущенных к обработке ПДн, обрабатываемых в ИСПДн.

Должен быть определен перечень информации, классифицируемой как ПДн.

Разграничение прав доступа в серверные помещения должно регламентироваться внутренними организационно-распорядительными документами Заказчика.

Компоненты СЗПДн, в том числе телекоммуникационное оборудование, должны быть подключены к источникам бесперебойного питания.

Серверное помещение должно быть оборудовано средствами вентиляции и кондиционирования воздуха, достаточными для работы оборудования в соответствии с документацией производителя, а также средствами автоматического пожаротушения и пожарной сигнализации.