**Общество с ограниченной ответственностью**

**«Орган по аттестации»**

**лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации № 2446 от 30.09.2014**

|  |  |
| --- | --- |
| УТВЕРЖДАЮ  Генеральный директор  ООО «ВЛАДЕЛЕЦ ИСПДН»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. | УТВЕРЖДАЮ  Генеральный директор  ООО «ОРГАН ПО АТТЕСТАЦИИ» |



**ЧАСТНОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**«ВЛАДЕЛЕЦ ИСПДН»**

**ООО «ВЛАДЕЛЕЦ ИСПДН»**

**На 47 листах**

**Действует с 27.02.2024**

**СОДЕРЖАНИЕ**

Термины и определения 3

Перечень сокращений и обозначений 5

1. Общие сведения 7

1.1 Наименование системы 7

1.2 Основание для проведения работ 7

1.3 Наименование организаций заказчика и исполнителя 7

1.4 Перечень документов, на основании которых разрабатывается СЗПДн 8

1.5 Плановые сроки начала и окончания работ 9

1.6 Порядок оформления и предъявления заказчику результатов работ 9

2. Цели и назначение создания СЗПДн «ВЛАДЕЛЕЦ ИСПДН» 10

3. Характеристика объекта информатизации 11

3.1 Основные сведения об объекте 11

3.2 Состав персональных данных, обрабатываемых в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 13

3.3 Перечень объектов защиты ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 13

3.4 Сведения о классификации системы 14

4. Требования к СЗПДн «ВЛАДЕЛЕЦ ИСПДН» 15

4.1 Требования к СЗПДн «ВЛАДЕЛЕЦ ИСПДН» в целом 15

4.2 Требования к функциям защиты применяемым в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 16

4.2.1 Состав мер по обеспечению ИБ при их использовании в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 17

4.2.2 Требования к мерам (функциям) защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 19

4.2.3 Требования к защите ПДн при их обработке в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 21

4.3 Базовый набор мер (функций) защиты ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 22

4.4 Требования к средствам ЗИ в составе СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 31

4.4.1 Требования к СЗИ от несанкционированного доступа 31

4.4.2 Требования к средствам антивирусной защиты информации 33

4.4.3 Требования к средствам межсетевого экранирования 35

4.4.4 Требования к средствам анализа защищенности 37

4.5 Требования к поставляемым средствам защиты информации 37

4.6 Требования по стандартизации и унификации 37

4.7 Требования к надежности 38

4.8 Требования к численности и квалификации персонала 38

4.9 Функции заказчика по обеспечению защиты информации в информационной системе 39

4.10 Требования к защите информации при информационном взаимодействии с иными информационно-телекоммуникационными сетями 39

4.11 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн 40

4.12 Требования к организационному обеспечению 40

5. Состав и содержание работ по созданию СЗПДн 43

6. Порядок контроля и приемки СЗПДн 44

7. Требования к документированию 45

8. Источники разработки 46

Лист согласования 47

Термины и определения

**Администратор безопасности** – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию СЗИ

**Антивирусная защита** – защита информации и компонентов информационной системы (ИС) от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов)

**Безопасность персональных данных** - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных

**Вирус (компьютерный, программный)** - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению

**Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

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

**Информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств

**Информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов

**Компонент (системы, сети)** - программное, программно-аппаратное или техническое средство, входящее в состав систем и сетей

**Контролируемая зона** - пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей Организации и посторонних транспортных, технических и иных материальных средств

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания

**Межсетевой экран** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы

**Модель угроз** – перечень возможных угроз информации

**Система защиты персональных данных** - совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах

**Средство антивирусной защиты** - программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации

**Угроза безопасности информации** – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации

Перечень сокращений и обозначений

152-ФЗ – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1119 ПП – постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

АРМ – автоматизированное рабочее место

АС – автоматизированная система

БД – база данных

БД ПКВ – база данных признаков вредоносных компьютерных программ (вирусов)

ЗБ – задание по безопасности

ИБ – информационная безопасность

ИС – информационная система

ИСПДн – информационная система персональных данных

КВ -компьютерный вирус

ЛВС – локальная вычислительная сеть

МЭ - межсетевой экран

НСД – несанкционированный доступ

ОРД – организационно распорядительная документация в части защиты персональных данных, обрабатываемых в информационной системе персональных данных

ОС – операционная система

ПДн – персональные данные

ПЗ – профиль защиты

ПКВ - признак компьютерного вируса

ПЭВМ – персональная электронно-вычислительная машина

ПО – программное обеспечение

САВЗ – средство антивирусной защиты

СВТ – средства вычислительной техники

СЗИ – средство защиты информации

СЗПДн - система защиты персональных данных

СКЗИ – средство криптографической защиты информации

СКУД – Система контроля и управления доступом

СУБД – Система управления базами данных

ТС – Технические средства

ФЗ – Федеральный закон

ФСБ России – Федеральная служба безопасности Российской Федерации

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации

ФТБ – функциональные требования безопасности

ЦОД - центр обработки данных

ЧТЗ - частное техническое задание

1. Общие сведения

В настоящем документе содержится перечень требований к системе защиты персональных данных (далее по тексту – СЗПДн) информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее – ИСПДн «ВЛАДЕЛЕЦ ИСПДН», ИСПДн).

Настоящее частное техническое задание (ЧТЗ) может дополняться и корректироваться по согласованию Исполнителя и Заказчика.

## 1.1 Наименование системы

Полное наименование системы – система защиты персональных данных информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» Общества с ограниченной ответственностью «ВЛАДЕЛЕЦ ИСПДН».

Краткое наименование – СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

## 1.2 Основание для проведения работ

Частное техническое задание (ЧТЗ) на создание СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» разрабатывается в рамках выполнения работ по Договору между Обществом с ограниченной ответственностью «ВЛАДЕЛЕЦ ИСПДН» (ООО «ВЛАДЕЛЕЦ ИСПДН») и Обществом с ограниченной ответственностью «Орган по аттестации» (ООО «ОРГАН ПО АТТЕСТАЦИИ»).

## 1.3 Наименование организаций заказчика и исполнителя

**Заказчик:** Общество с ограниченной ответственностью «ВЛАДЕЛЕЦ ИСПДН», ИНН, ОГРН (далее - ООО «ВЛАДЕЛЕЦ ИСПДН», Общество), адрес местонахождения.

**Исполнитель:** Общество с ограниченной ответственностью «Орган по аттестации», ИНН, (далее - ООО «ОРГАН ПО АТТЕСТАЦИИ»), адрес местонахождения:.

**Основания осуществления деятельности:**

ООО «ОРГАН ПО АТТЕСТАЦИИ» осуществляет деятельность в области создания СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» на основании следующих лицензий:

- лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации;

- лицензия ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) рег..

## 1.4 Перечень документов, на основании которых разрабатывается СЗПДн

Разработка СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется на основании следующих документов:

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

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Разработка СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется в соответствии с требованиями следующих документов:

- «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утверждены Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119);

- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены приказом ФСТЭК России от 18 февраля 2013 года № 21);

В качестве исходных данных для разработки СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» используются следующие документы:  
 - Отчет об обследовании информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН»;

- Модель угроз безопасности информации информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН».

Разработка настоящего ЧТЗ осуществлялось с учетом требований следующих документов:

- ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

- ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

- Информационное сообщение об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных от 20 ноября 2012 года № 240/24/4669 (ФСТЭК России).

## 1.5 Плановые сроки начала и окончания работ

Плановые сроки начала и окончания работ устанавливаются требованиями Договора.

## 1.6 Порядок оформления и предъявления заказчику результатов работ

Порядок оформления и предъявления Заказчику результатов работ определяются в соответствии с требованиями Договора.

2. Цели и назначение создания СЗПДн «ВЛАДЕЛЕЦ ИСПДН»

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должна обеспечивать защиту информационных ресурсов ИСПДн «ВЛАДЕЛЕЦ ИСПДН» от потенциальных злоумышленников, непроизвольных действий и угроз информационной безопасности, определенных в Модели угроз безопасности информации (МУ).

Целью реализации СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» является снижение вероятного ущерба от реализации угроз ИБ и выполнение требований законодательства РФ в части защиты информации.

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» предназначена для защиты информации, не составляющей государственную тайну, содержащейся в информационной системе, а также ПО и технических средств ИСПДн «ВЛАДЕЛЕЦ ИСПДН», обрабатывающих защищаемую информацию.

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Характеристика объекта информатизации

## 3.1 Основные сведения об объекте

ИСПДн «ВЛАДЕЛЕЦ ИСПДН» (далее также ИСПДн) на базе 1 (одного) объекта вычислительной техники расположена по адресу.

Назначение ИСПДн «ВЛАДЕЛЕЦ ИСПДН»: ИСПДн «ВЛАДЕЛЕЦ ИСПДН» предназначена для автоматизации процессов экономической и организационной деятельности Общества.

Задачами ИСПДн «ВЛАДЕЛЕЦ ИСПДН» является:

­ Реализации уставных целей компании;

­ Реализации кадровой политики и финансовых расчётов с персоналом и контрагентами.

Физически ИСПДн «ВЛАДЕЛЕЦ ИСПДН» состоит из одного АРМ на базе ПЭВМ, подключенного к сети Интернет через ЛВС Общества (см. рисунок 1):

Таблица 1 - краткие технические сведения о ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

|  |  |
| --- | --- |
| **Показатель** | **Значение** |
| **Количественные характеристики ИСПДн** | |
| Серверные компоненты | отсутствуют |
| Клиентские компоненты | 1 (одно) автоматизированное рабочее место (АРМ) на базе ПЭВМ без среды виртуализации |
| **Качественные характеристики клиентских компонент** | |
| Аппаратная платформа | Intel (Intel(R) Core(TM) i5-4200U CPU @ 1.60GHz 2.30 GHz) |
| Форм-фактор аппаратной платформы | Ноутбук |
| Среда виртуализации | Не используется |
| Сегментирование | Не используется |
| Операционная система | Windows 10 Pro (19045.4046) |
| Система хранения данных | Внутренний жесткий диск |
| Общесистемное программное обеспечение (ОСПО) | Будет уточняться на этапе проектирования |
| Специальное программное обеспечение (СПО) | Microsoft Office 2016 |
| Используемые средства защиты | Штатные средства операционной системы (ОС) |

Основной функционал ИСПДн «ВЛАДЕЛЕЦ ИСПДН» реализуется на базе типового офисного программного обеспечения, функционирующего локально. ИСПДн «ВЛАДЕЛЕЦ ИСПДН» не передает ПДн через информационно-телекоммуникационные сети международного информационного обмена «Интернет».

В состав ИСПДн «ВЛАДЕЛЕЦ ИСПДН» входят следующие структурные элементы:

а) программные средства:

– базовая система ввода-вывода программно-технических средств;

– системное программное обеспечение (операционная система);

– общесистемное программное обеспечение (утилиты и драйверы системного обеспечения, включая утилиты и драйверы управления аппаратными ресурсами);

– специальное программное обеспечение, на базе которого реализуется основной функционал ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

б) штатные механизмы защиты программно-технических средств:

– средства идентификации и аутентификации пользователей;

– средства управления доступом пользователей;

– средства обеспечения регистрации и учета действий пользователей.

в) каналы информационного взаимодействия.

Для получения целевых функций необходимо пройти аутентификацию на АРМ, где существует возможность аутентифицироваться двум категориям субъектов доступа (см. таблицу 2):

Таблица 2 - Категории субъектов доступа ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

|  |  |  |
| --- | --- | --- |
| № | Категория субъекта доступа | Описание |
| 1 | Администратор | Решение задач управления пользователями, параметрами ПО, функциями и параметрами безопасности |
| 2 | Пользователь | Обработка ПДн |

## 3.2 Состав персональных данных, обрабатываемых в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» на момент ее обследования обрабатываются следующие сведения, составляющие персональные данные: фамилия, имя, отчество, дата рождения, пол, сведения о трудовом стаже.

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» одновременно обрабатываются данные менее 100 000 субъектов персональных данных как сотрудников, так и не являющихся сотрудниками оператора. В соответствии с пунктом 5 Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" ИСПДн «ВЛАДЕЛЕЦ ИСПДН» является информационной системой, обрабатывающей иные категории персональных данных, так как в ней не обрабатываются персональные данные:

- специальные персональные данные;

- биометрические персональные данные;

- общедоступные персональные данные.

## 3.3 Перечень объектов защиты ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Объектами защиты в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» являются:

- информация, обрабатываемая в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», включая персональные данные;

- технические средства, включая средства вычислительной техники, машинные носители информации, технические средства обработки информации, системы и средства связи и передачи данных;

- UEFI/BIOS, системное программное обеспечение (ПО), общесистемное и сервисное программное обеспечение (ОСПО) и прикладное (специальное) программное обеспечение (СПО);

- физические линии связи и сетевое оборудование;

- средства защиты информации.

## 3.4 Сведения о классификации системы

Специалистами ООО «ВЛАДЕЛЕЦ ИСПДН» была проведена классификация и установление уровня защищенности (УЗ) ИСПДн «ВЛАДЕЛЕЦ ИСПДН» по требованиям безопасности информации.

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется обработка иных категории персональных данных, менее чем 100 000 субъектов персональных данных как сотрудников, так и не являющихся сотрудниками оператора. В соответствии с документом «Модель угроз и нарушителя безопасности информационной системы персональных данных…» для ИСПДн «ВЛАДЕЛЕЦ ИСПДН» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В соответствии с **пп. б) п.12** Постановления Правительства РФ от 1 ноября 2012 г. № 1119 и с учетом перспектив увеличения объема обрабатываемых персональных данных до количества более 100 000 субъектов персональных данных, не являющихся сотрудниками оператора, комиссия установила для ИСПДн «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» необходимость обеспечения 3-го уровня защищенности персональных данных (УЗ3).

Аттестация или оценка соответствия в иной форме по требованиям безопасности информации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» ранее не проводилась.

****4. Требования к СЗПДн**** ****«ВЛАДЕЛЕЦ ИСПДН»****

## 4.1 Требования к СЗПДн «ВЛАДЕЛЕЦ ИСПДН» в целом

Разрабатываемая СЗПДн должна обеспечивать защиту обрабатываемой в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» информации, в соответствии с требованиями действующих нормативно-правовых актов Российской Федерации (РФ) в области защиты информации.

Разрабатываемая СЗПДн не должна накладывать каких-либо существенных ограничений на информационные технологии, используемые в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» не включает в себя средства физической безопасности, так как данные средства защиты входят в состав общей системы физической защиты помещений, в которых расположены аппаратные компоненты ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

СЗПДн «ВЛАДЕЛЕЦ ИСПДН» создается в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должна реализовывать меры защиты информации, выбранные в соответствии с пунктом 9 документа «Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден приказом ФСТЭК России от 18 февраля 2013 года № 21).

Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

В случае применения средств криптографической защиты информации в составе СЗПДн «ВЛАДЕЛЕЦ ИСПДН» необходимо выполнение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утверждены Приказом ФСБ России от 10 июля 2014 г. N 378).

## 4.2 Требования к функциям защиты применяемым в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Меры защиты информации должны реализовываться в рамках СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» в зависимости от установленного уровня защищенности (УЗ) ПДн, а также актуальных угроз безопасности информации и структурно-функциональных характеристик информационной системы. Выбор мер (функций) защиты информации для их реализации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должен быть проведен на этапе проектирования СЗПДн и должен включать (рисунок 3):

А) определение базового набора мер защиты информации для установленного уровня защищенности информационной системы в соответствии с базовыми наборами мер защиты информации, приведенными в приложении к документу «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден приказом ФСТЭК России от 18 февраля 2013 г. № 21);

Б) адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам ИСПДн «ВЛАДЕЛЕЦ ИСПДН», информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

В) уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, приведенных в приложении к документу «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21), в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в Модель угроз и нарушителя «ВЛАДЕЛЕЦ ИСПДН»;

Г) дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

При невозможности реализации в рамках СЗПДн «ВЛАДЕЛЕЦ ИСПДН» отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации. В этом случае в ходе разработки СЗПДн «ВЛАДЕЛЕЦ ИСПДН» должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

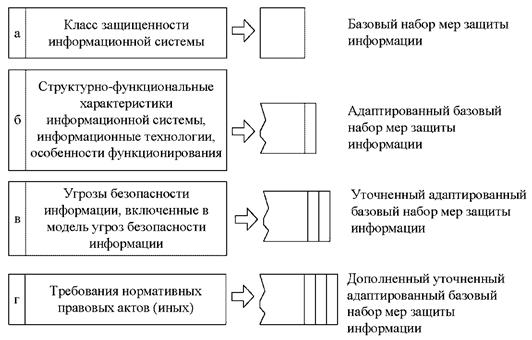


Рисунок 3 - Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе

### 4.2.1 Состав мер по обеспечению ИБ при их использовании в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

В соответствии с приказом ФСТЭК России от 18 февраля 2013 г. № 21 в состав мер по обеспечению безопасности персональных данных, реализуемых в рамках СЗПДн с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят (рисунок 4):

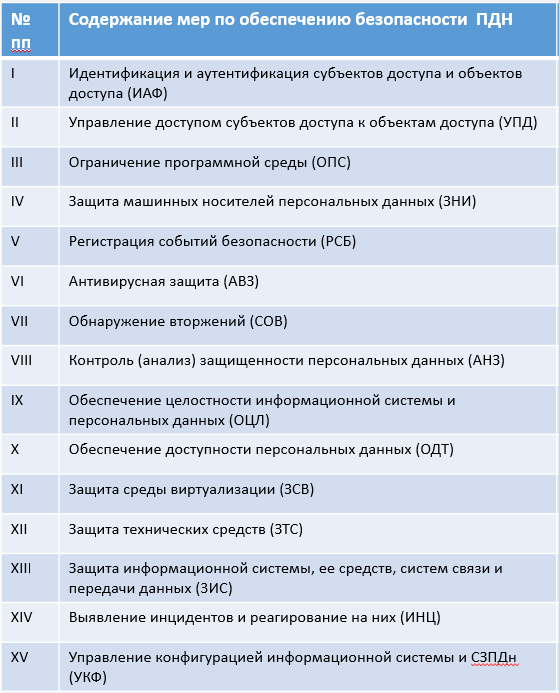


Рисунок 4 - Состав мер по обеспечению безопасности персональных данных

(I) идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);

(II) управление доступом субъектов доступа к объектам доступа (УПД);

(III) ограничение программной среды (ОПС);

(IV) защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных) (ЗНИ);

(V) регистрация событий безопасности (РСБ);

(VI) антивирусная защита (АВЗ);

(VII) обнаружение (предотвращение) вторжений (СОВ);

(VIII) контроль (анализ) защищенности персональных данных (АНЗ);

(IX) обеспечение целостности информационной системы и персональных данных (ОЦЛ);

(X) обеспечение доступности персональных данных (ОДТ);

(XI) защита среды виртуализации (ЗСВ);

(XII) защита технических средств (ЗТС);

(XIII) защита информационной системы, ее средств, систем связи и передачи данных (ЗИС);

(XIV) выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них (ИНЦ);

(XV) управление конфигурацией информационной системы и системы защиты персональных данных (УКФ).

### 4.2.2 Требования к мерам (функциям) защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Требования к мерам по обеспечению безопасности персональных данных, реализуемым в рамках СЗПДн, в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден приказом ФСТЭК России от 18 февраля 2013 г. № 21):

**(I) Меры по идентификации и аутентификации (ИАФ)** субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

**(II) Меры по управлению доступом (УПД)** субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

**(III) Меры по ограничению программной среды** **(ОПС)** должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

**(IV) Меры по защите машинных носителей** **(ЗНИ)** персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

**(V) Меры по регистрации событий безопасности** **(РСБ)** должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

**(VI) Меры по антивирусной защите (АВЗ)** должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

**(VII) Меры по обнаружению (предотвращению) вторжений** **(СОВ)** должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

**(VIII) Меры по контролю (анализу) защищенности** **(АНЗ)** персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

**(IX) Меры по обеспечению целостности информационной системы (ОЦЛ)** и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

**(X) Меры по обеспечению доступности персональных данных (ОДТ)** должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

**(XI) Меры по защите среды виртуализации** **(ЗСВ)** должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

**(XII) Меры по защите технических средств (ЗТС)** должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

**(XIII) Меры по защите информационной системы, ее средств, систем связи и передачи данных** **(ЗИС)** должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

**(XIV) Меры по выявлению инцидентов и реагированию на них** **(ИНЦ)** должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

**(XV) Меры по управлению конфигурацией информационной системы** **и системы защиты** **(УКФ)** персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

### 4.2.3 Требования к защите ПДн при их обработке в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Для обеспечения 3-го уровня защищенности персональных данных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 01.11.2012 № 1119, к СЗПДн «ВЛАДЕЛЕЦ ИСПДН» предъявляются следующие требования:

– организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей персональных данных;

– утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

– необходимо, чтобы было назначено должностное лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе.

## 4.3 Базовый набор мер (функций) защиты ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Меры (функции) защиты, подлежащие реализации в СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН», в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден приказом ФСТЭК России от 18 февраля 2013 г. № 21), в рамках базового набора мер по обеспечению безопасности персональных данных для 3-ого (третьего) уровня защищенности персональных данных включают (Таблица 3):

Таблица 3 - Состав и содержание мер по обеспечению безопасности 3 УЗ ПДн

| **Условное обозначение и № меры** | **Содержание мер по обеспечению безопасности персональных данных** | **УЗ ПДн** | | | | **Подлежит реализации**  **для 3 УЗ** |
| --- | --- | --- | --- | --- | --- | --- |
| **4** | **3** | **2** | **1** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + | Да |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |  |  | + | + | Нет |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | + | + | Да |
| 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 | + | + | + | + | Да |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + | Да |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | + | + | Да |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + | + | + | Да |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + | Да |
| 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 | + | + | + | + | Да |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + | + | + | Да |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | + | + | + | Да |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + | + | Да |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных |  |  |  |  | Нет |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |  |  |  |  | Нет |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |  |  |  |  | Нет |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |  | + | + | + | Да |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |  | + | + | + | Да |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |  |  |  |  | Нет |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + | + | + | Да |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + | + | Да |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + | + | Да |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + | + | Да |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |  |  | + | + | Нет |
| **III. Ограничение программной среды (ОПС)** | | | | | | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |  |  |  |  | Нет |
| 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 |  |  | + | + | Нет |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |  |  |  | + | Нет |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |  |  |  |  | Нет |
| **IV. Защита машинных носителей персональных данных (ЗНИ)** | | | | | | |
| ЗНИ.1 | Учет машинных носителей персональных данных |  |  | + | + | Нет |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных |  |  | + | + | Нет |
| ЗНИ.3 | Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны |  |  |  |  | Нет |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах |  |  |  |  | Нет |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных |  |  |  |  | Нет |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители персональных данных |  |  |  |  | Нет |
| ЗНИ.7 | Контроль подключения машинных носителей персональных данных |  |  |  |  | Нет |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания |  | + | + | + | Да |
| **V. Регистрация событий безопасности (РСБ)** | | | | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + | Да |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + | Да |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + | Да |
| 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 |  |  |  |  | Нет |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |  |  | + | + | Нет |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |  |  |  |  | Нет |
| РСБ.7 | Защита информации о событиях безопасности | + | + | + | + | Да |
| **VI. Антивирусная защита (АВЗ)** | | | | | | |
| АВЗ.1 | Реализация антивирусной защиты | + | + | + | + | Да |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | + | + | + | Да |
| **VII. Обнаружение вторжений (СОВ)** | | | | | | |
| СОВ.1 | Обнаружение вторжений |  |  | + | + | Нет |
| СОВ.2 | Обновление базы решающих правил |  |  | + | + | Нет |
| **VIII. Контроль (анализ) защищенности персональных данных (АНЗ)** | | | | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |  | + | + | + | Да |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + | + | Да |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |  | + | + | + | Да |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |  | + | + | + | Да |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |  |  | + | + | Нет |
| **IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)** | | | | | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |  |  | + | + | Нет |
| ОЦЛ.2 | Контроль целостности персональных данных, содержащихся в базах данных информационной системы |  |  |  |  | Нет |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |  |  |  |  | Нет |
| 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) |  |  | + | + | Нет |
| ОЦЛ.5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |  |  |  |  | Нет |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |  |  |  |  | Нет |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |  |  |  |  | Нет |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях |  |  |  |  | Нет |
| **X. Обеспечение доступности персональных данных (ОДТ)** | | | | | | |
| ОДТ.1 | Использование отказоустойчивых технических средств |  |  |  |  | Нет |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |  |  |  |  | Нет |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |  |  |  | + | Нет |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных |  |  | + | + | Нет |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала |  |  | + | + | Нет |
| **XI. Защита среды виртуализации (ЗСВ)** | | | | | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + | + | + | Да |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + | Да |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |  | + | + | + | Да |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |  |  |  |  | Нет |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |  |  |  |  | Нет |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |  |  | + | + | Нет |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций |  |  | + | + | Нет |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |  |  | + | + | Нет |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |  | + | + | + | Да |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей |  | + | + | + | Да |
| **XII. Защита технических средств (ЗТС)** | | | | | | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |  |  |  |  | Нет |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |  |  |  |  | Нет |
| 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 | + | + | + | + | Да |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | + | + | + | Да |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |  |  |  |  | Нет |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (3ИС)** | | | | | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы |  |  |  | + | Нет |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |  |  |  |  | Нет |
| 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 беспроводным каналам связи | + | + | + | + | Да |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |  |  |  |  | Нет |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |  |  |  |  | Нет |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами |  |  |  |  | Нет |
| 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 |  |  |  |  | Нет |
| 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 |  |  |  |  | Нет |
| 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 |  |  |  |  | Нет |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |  |  |  |  | Нет |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |  |  | + | + | Нет |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю |  |  |  |  | Нет |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя |  |  |  |  | Нет |
| ЗИС.14 | Использование устройств терминального доступа для обработки персональных данных |  |  |  |  | Нет |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных |  |  | + | + | Нет |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |  |  |  |  | Нет |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |  |  | + | + | Нет |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения |  |  |  |  | Нет |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |  |  |  |  | Нет |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |  | + | + | + | Да |
| **XIV. Выявление инцидентов и реагирование на них (ИНЦ)** | | | | | | |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них |  |  | + | + | Нет |
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов |  |  | + | + | Нет |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами |  |  | + | + | Нет |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий |  |  | + | + | Нет |
| ИНЦ.5 | Принятие мер по устранению последствий инцидентов |  |  | + | + | Нет |
| ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов |  |  | + | + | Нет |
| **XV. 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 |  | + | + | + | Да |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |  | + | + | + | Да |
| 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 |  | + | + | + | Да |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |  | + | + | + | Да |

## 4.4 Требования к средствам ЗИ в составе СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

В составе СЗПДн должно использоваться только лицензионное программное обеспечение средств защиты информации, кроме того, должны применяться только серийно выпускаемые программные и технические средства.

В составе СЗПДн должны применяться средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия **6 класса** и **6 уровня доверия**, а также средства вычислительной техники **не ниже 5 класса** (РД СВТ);

В случае необходимости применения СКЗИ в составе СЗПДн в соответствии с Приказом ФСБ России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных

### 4.4.1 Требования к СЗИ от несанкционированного доступа

Используемые в составе СЗПДн «ВЛАДЕЛЕЦ ИСПДН» средства защиты от несанкционированного доступа должны обеспечивать:

– контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.);

– для каждой пары (субъект – объект) в средствах вычислительной техники должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу средств вычислительной техники (объекту);

– механизм, претворяющий в жизнь дискреционные правила разграничения доступа;

– контроль доступа, применимый к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов);

– механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил разграничения доступа, в том числе возможность санкционированного изменения списка пользователей средств вычислительной техники и списка защищаемых объектов;

– возможность предоставления прав изменения правил разграничения доступа выделенным субъектам;

– идентификацию пользователей при запросах на доступ;

– препятствие доступа к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась;

– предотвращение доступа субъекту к остаточной информации при первоначальном назначении или при перераспределении внешней памяти;

Возможность регистрации следующих событий:

- использование идентификационного и аутентификационного механизма;

- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);

- создание и уничтожение объекта;

- действия по изменению правил разграничения доступа.

При этом для каждого из этих действий должна регистрироваться следующая информация:

- дата и время;

- субъект, осуществляющий регистрируемое действие;

- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);

- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Возможность ознакомления с регистрационной информацией:

– периодический контроль за целостностью программной и информационной части средств защиты информации;

– возможность тестирования реализации правил разграничения доступа (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения правил разграничения доступа);

– возможность тестирования успешного осуществления идентификации и аутентификации, а также их средства защиты;

– возможность тестирования регистрации событий, очистки остаточной информации и работы механизма контроля целостности.

### 4.4.2 Требования к средствам антивирусной защиты информации

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» могут использоваться средства антивирусной защиты (САВЗ) 6 класса защиты типа «А», типа «Б» и типа «В».

Средства антивирусной защиты типа «А» представляет собой программное средство, используемое для построения антивирусной защиты ИС и предназначенное для централизованного администрирования САВЗ, установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах). Средства антивирусной защиты типа «А» не должны применяться в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и(или) «В». Средства антивирусной защиты типа «А» должны устанавливаться на АРМ (сервере) администратора безопасности. Администратор безопасности должен иметь возможность удаленно устанавливать и конфигурировать клиентские САВЗ на всех сетевых АРМ (серверах) в пределах вычислительной сети, входящей в область ответственности администратора безопасности.

Средства антивирусной защиты типа «Б» представляет собой программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации, предназначенное для применения на серверах информационных систем. Средства антивирусной защиты типа «Б» должны устанавливаться на серверы информационной системы, функционирующей на базе вычислительной сети.

Средства антивирусной защиты типа «В» представляет собой программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации, предназначенное для применения на автоматизированных рабочих местах информационных систем. Средства антивирусной защиты типа «В» должны устанавливаться на автоматизированные рабочие места информационной системы, функционирующей на базе вычислительной сети.

Средства антивирусной защиты (САВЗ) ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должны обеспечивать:

а) для САВЗ класса «А»:

- возможность отображения сигнала тревоги на автоматизированное рабочее место (АРМ) администратора безопасности, указывающего на обнаружение КВ на пользовательских автоматизированных рабочих местах;

- возможность получения и установки обновлений БД ПКВ без применения средств автоматизации и в автоматизированном режиме с сетевого ресурса;

- возможность администраторам безопасности управлять режимом выполнения функций безопасности САВЗ (обработка зараженных объектов на АРМ и серверах вычислительной сети; выполнение автоматизированного запуска САВЗ на АРМ и серверах вычислительной сети с заданными условиями поиска компьютерных вирусов (КВ) и режимами реагирования по расписанию; выполнение удаленного администрирования процессов обнаружения КВ, обновления базы данных (БД) признаков компьютерных вирусов (ПКВ) и компонентов САВЗ);

- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;

- поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности;

- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;

- возможность читать информацию из записей аудита.

б) для САВЗ класса «Б»:

- возможность выполнения проверок с целью обнаружения зараженных КВ объектов;

- возможность выполнения проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;

- возможность выполнения проверок с целью обнаружения зараженных КВ объектов по команде; в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; путем запуска с необходимыми параметрами функционирования своего кода внешней программой;

- возможность выполнения проверок с целью обнаружения зараженных КВ объектов сигнатурными методами;

- возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов;

- возможность получения и установки обновлений БД ПКВ без применения средств автоматизации;

- возможность генерирования записей аудита для событий, подвергаемых аудиту;

- возможность чтения информации из записей аудита;

- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;

- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;

- поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов.

в) для САВЗ класса «В»:

- возможность выполнения проверок с целью обнаружения зараженных КВ объектов в файловых областях носителей информации;

- возможность выполнения проверок с целью обнаружения зараженных КВ объектов по команде;

- возможность выполнения проверок с целью обнаружения зараженных КВ объектов сигнатурными методами;

- возможность получения и установки обновлений БД ПКВ без применения средств автоматизации;

- возможность генерирования записей аудита для событий, подвергаемых аудиту;

- возможность чтения информации из записей аудита;

- возможность ассоциации событий аудита с идентификаторами субъектов;

- ограничение доступа к чтению записей аудита;

- поиск, сортировку, упорядочение данных аудита;

- возможность уполномоченным пользователям (ролям) управлять

- режимом выполнения функций безопасности САВЗ;

- возможность уполномоченным пользователям (ролям) управлять

- параметрами настройки функций безопасности САВЗ;

- поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и пользователями ИС.

### 4.4.3 Требования к средствам межсетевого экранирования

Межсетевой экран (МЭ) представляет собой программный или программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков и используемое в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа.

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» могут использоваться средства межсетевого экранирования (МЭ) 6 класса защиты типа «А» и типа «В». МЭ типа «А» – это МЭ, применяемый на физической границе (периметре) информационн

ой системы или между физическими границами сегментов информационной системы. МЭ типа «В» – это МЭ, применяемый на узле (хосте) информационной системы.

МЭ типа «А» должен обеспечивать нейтрализацию следующих угроз безопасности информации:

- несанкционированный доступ к информации, содержащейся в информационной системе;

- отказ в обслуживании информационной системы и (или) ее отдельных компонентов;

- несанкционированная передача информации из информационной системы в информационно-телекоммуникационные сети или иные информационные системы;

- несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности;

- несанкционированное получение сведений о сети информационной системы (автоматизированной системы управления), а также об ее узлах.

МЭ типа «В» должен обеспечивать нейтрализацию следующих угроз безопасности информации:

- несанкционированный доступ к информации, содержащейся в информационной системе;

- отказ в обслуживании информационной системы и (или) ее отдельных компонентов;

- несанкционированная передача информации из информационной системы в информационно-телекоммуникационные сети или иные информационные системы;

- несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности.

В МЭ типа «А» должны быть реализованы следующие функции безопасности:

- контроль и фильтрация;

- идентификация и аутентификация;

- регистрация событий безопасности (аудит);

- обеспечение бесперебойного функционирования и восстановление;

- управление (администрирование).

В МЭ типа «В» должны быть реализованы следующие функции безопасности:

- контроль и фильтрация;

- регистрация событий безопасности (аудит);

- обеспечение бесперебойного функционирования и восстановление;

- тестирование и контроль целостности;

- управление (администрирование).

В МЭ типа «А» и типа «В» не должно содержаться программ, не выполняющих (не задействованных в реализации) функций безопасности или не предназначенных для обеспечения функционирования МЭ (сторонних программ).

### 4.4.4 Требования к средствам анализа защищенности

Используемые в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» средства анализа защищенности (сканеры безопасности) должны иметь 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, а также иметь возможность формирования отчетов по результатам выявления (поиска) уязвимостей.

## 4.5 Требования к поставляемым средствам защиты информации

Поставляемые средства защиты информации должны быть ранее не эксплуатируемыми (новыми).

Поставляемые средства защиты информации должны реализовывать функции по обеспечению безопасности персональных данных в соответствии с требованиями действующего законодательства и настоящего Частного технического задания.

При поставке средств защиты информации должны соблюдаться все авторские и смежные с ними права разработчика.

Поставляемые средства защиты информации должны быть совместимы с программными и программно-аппаратными средствами ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

## 4.6 Требования по стандартизации и унификации

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должна строиться на основе ограниченного числа видов, типов и конфигураций программных, аппаратных средств и технологий защиты.

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должна строиться на базе серийно выпускаемых средств защиты информации.

При выборе средств защиты информации для СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» преимущество должны иметь средства защиты информации, имеющие сертификаты (свидетельства) совместимости со средствами защиты информации, также применяемыми в СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

## 4.7 Требования к надежности

При выборе средств защиты информации для СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» преимущество должны иметь средства защиты информации, прошедшие функциональное тестирование, оценку качества и/или надежности, независимыми от производителей исследовательскими и испытательными организациями.

Период восстановления средств защиты информации в составе СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» после сбоев не должен превышать установленного периода восстановления комплекса средств автоматизации в ИСПДн.

Время и порядок восстановления СЗПДн в случаях сбоев в целом согласовываются с ИСПДн «ВЛАДЕЛЕЦ ИСПДН» на стадии технического проектирования.

## 4.8 Требования к численности и квалификации персонала

Численность и качественный состав персонала СЗПДн должны быть определены на этапе технического проектирования, исходя из состава внедряемых средств защиты информации, комплекса организационно-технических мероприятий, а также существующей организационно-штатной структуры и квалификационных нормативов, применяемых в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

В составе персонала требуется выделение следующих лиц, обеспечивающих эксплуатацию СЗПДн в составе ИСПДн:

- Ответственный за обеспечение безопасности ПДн.

- Администратор информационной безопасности.

Для обеспечения защиты ПДн, содержащихся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», Заказчиком назначается должностное лицо (сотрудник), ответственное за обеспечение безопасности ПДн.

Для эксплуатации СЗПДн в составе ИСПДн «ВЛАДЕЛЕЦ ИСПДН» Заказчиком назначается администратор информационной безопасности, который должен обладать достаточными знаниями в области системного администрирования сертифицированных средств защиты информации.

Структура и функции персонала, обслуживающего и эксплуатирующего программно-аппаратные средства СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должны быть закреплены во внутренних положениях и в должностных инструкциях.

Персонал ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должен осуществлять обслуживание и эксплуатацию ИСПДн «ВЛАДЕЛЕЦ ИСПДН» по рабочим дням в рабочее время с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности ИСПДн в целом и СЗПДн в ее составе.

## 4.9 Функции заказчика по обеспечению защиты информации в информационной системе

Для обеспечения защиты информации, обрабатываемой в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» Заказчик должен обеспечивать требования, установленные нормативно-методическими и законодательными актами Российской Федерации в сфере защиты информации и требованиями настоящего Частного технического задания, в том числе обеспечить:

- назначение подразделения или должностного лица (работника), ответственных за защиту информации;

- эксплуатацию ИСПДн и СЗПДн, а также используемых технических и программных средств и средств защиты информации в соответствии с требованиями технической, проектной и эксплуатационной документацией;

- ограничение доступа в помещения с элементами ИСПДн, а также техническим средствам и средствам защиты информации;

- ознакомление пользователей ИСПДн с требованиями организационно-распорядительных документов по защите информации, нормативно-методических и законодательных актов по защите информации под роспись;

- управление конфигурацией ИСПДн в ходе ее эксплуатации в соответствии с требованиями, установленными организационно-распорядительной, проектной и эксплуатационной документации и требованиями нормативно-правовых и законодательных актов в области защиты информации;

- контроль (мониторинг) за обеспечением установленного уровня защищенности информации, содержащейся в ИСПДн;

- в случае невозможности обслуживания СЗПДн в целом или отдельных ее элементов привлечение на договорной основе третьих лиц, имеющих соответствующие лицензии ФСТЭК России и (или) ФСБ России на оказание услуг в данной сфере деятельности;

- вывод ИСПДн из эксплуатации после принятия решения об окончании обработки информации в соответствии с требованиями действующего законодательства.

## 4.10 Требования к защите информации при информационном взаимодействии с иными информационно-телекоммуникационными сетями

Взаимодействие ИСПДн «ВЛАДЕЛЕЦ ИСПДН» с иными информационно-телекоммуникационными сетями, в т.ч. сетью Интернет, должно осуществляться с использованием средств межсетевого экранирования, средств обнаружения вторжений и антивирусной защиты, сертифицированных ФСТЭК России.

## 4.11 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн

Физический доступ неуполномоченных лиц к компонентам СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должен быть запрещен.

Электропитание должно осуществляться от сети переменного тока напряжением (220±20) В с частотой (50±1) Гц.

Нормальными климатическими условиями эксплуатации системы являются:

- температура окружающего воздуха (20 ±2) °С (не более 25°С);

- относительная влажность окружающего воздуха 20-70% (не более 75% в холодный период, в теплый для 25°С – не более 65%, для 24°С и ниже – не более 70%);

- допустимый уровень шума не более 65 дБ (допустимый уровень вибрации не должен превышать по амплитуде 0,1 мм и по частоте 25 Гц).

Система должна сохранять работоспособность при воздействии следующих климатических факторов:

- температура окружающего воздуха от 10°С до 35°С;

- относительная влажность воздуха от 40% до 80% при температуре 25°С.

Для всех средств защиты информации, входящих в состав СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН», рекомендуется обеспечить возможность официальной технической поддержки со стороны производителя.

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

## 4.12 Требования к организационному обеспечению

Должна быть обеспечена физическая охрана объекта информатизации (технических средств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения с элементами ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Организация доступа к ТС ИСПДн «ВЛАДЕЛЕЦ ИСПДН» при проведении ремонтных работ, уборки помещений, визитах посетителей должна осуществляться только в сопровождении и под наблюдением ответственного лица.

В организации должен действовать регламент по обращению с парольной информацией, определяющий порядок создания, использования и вывода из обращения парольной информации, а также порядок действий персонала в случае компрометации пароля.

Все помещения с элементами ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должны быть оборудованы системами пожарной сигнализации или иными средствами пожаротушения.

Должны быть определены лица, ответственные за мероприятия по защите информации, за нормальное функционирование и контроль работы СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Должны быть разработаны технологические инструкции по обеспечению информационной безопасности лицам, ответственным за обеспечение безопасности информации, ответственным за функционирование СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН», а также лицам, допущенным непосредственно к работе в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Допуск к обработке информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» с определением полномочий пользователей должен осуществляться на основании Перечня лиц, доступ которым к защищаемой информации, в т.ч. персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения служебных (трудовых) обязанностей и Матрицы доступа.

На период обработки защищаемой информации в помещениях, где размещаются ТС ИСПДн «ВЛАДЕЛЕЦ ИСПДН», должны находиться только лица, допущенные в установленном порядке к обрабатываемой информации. Допуск других лиц для проведения необходимых профилактических мероприятий может осуществляться в эти помещения только с разрешения руководителя организации или администратора безопасности.

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» быть определен порядок использования машинных носителей информации (HDD, CD, DVD, флеш-накопители и др.). Используемые в технологическом процессе обработки информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» машинные носители информации подлежат обязательному учету.

Организация антивирусной защиты должна осуществляться в соответствии с требованиями организационно-распорядительной документации по защите информации и документацией на используемые средства антивирусной защиты.

Разрабатываемые организационно-распорядительные документы по защите информации должны включать:

1. Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей.

2. Приказ о назначении должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных.

3. Приказ о назначении должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в электронном журнале сообщений, необходимы для выполнения служебных (трудовых) обязанностей.

4. Приказ о создании отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных. Или приказ о возложении обязанностей по обеспечению безопасности персональных данных в информационной системе персональных данных на имеющееся подразделение.

5. Положение по защите персональных данных в информационной системе персональных данных.

6. Правила доступа в помещения с информационной системой персональных данных в рабочее и нерабочее время, а также в нештатных ситуациях.

7. Перечень лиц, имеющих право доступа в помещения с информационной системой персональных данных.

8. Журнал учета носителей персональных данных с использованием регистрационных (заводских) номеров.

9. Технический паспорт информационной системы.

10. Разрешительная система доступа к защищаемым информационным ресурсам, программным и техническим средствам информационной системы.

11. Описание технологического процесса обработки информации в информационной системе.

12. Инструкция пользователю системы защиты информации информационной системы (при наличии в ролевой модели).

13. Инструкция администратору безопасности информации информационной системы.

14. Инструкция по эксплуатации системы защиты информации.

15. Приказ(ы) о границах контролируемой зоны объекта информатизации.

16. Приказ(ы) о назначении на роль / должность системного администратора и администратора ИБ.

17. Должностная / функциональная инструкция системного администратора и администратора ИБ.

18. Акт классификации / установления уровня защищенности.

5. Состав и содержание работ по созданию СЗПДн

Состав и содержание работ по созданию СЗПДн приведены в таблице 26.

Таблица 26 – Перечень и содержание этапов работ по созданию СЗПДн

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Наименование этапа** | **Содержание работ** |
| 1 | Разработка СЗПДн | На данном этапе разрабатываются следующие документы:  Технический проект на создание подсистемы «Информационная безопасность» в составе:  – Пояснительная записка к техническому проекту.  – \*Спецификация средств защиты информации (включая средства криптографической защиты информации при необходимости их применения).  – Ведомость технического проекта.  – \*Структурная схема СЗДПн.  – \*Описание комплекса средств СЗПДн.  \* - документы могут не разрабатываться при включении соответствующих сведений в пояснительную записку |
| 2 | Поставка, установка и настройка средств защиты персональных данных. | Поставка, установка и настройка средств защиты персональных данных осуществляется для Заказчика за счет Заказчика с учетом требований к системе защиты информации информационной системы в соответствии с техническим заданием на создание информационной системы и техническим проектом.  На данном этапе формируются следующие отчетные документы:  – Акт установки средств защиты информации. |
| 3 | Аттестация ИСПДн по требованиям безопасности персональных данных | Аттестация информационной системы должна проводится в соответствии с программой и методиками аттестационных испытаний, утвержденной Исполнителем и согласованной с Заказчиком.  По результатам аттестационных испытаний Исполнителем должны быть оформлены:  - Программа и методики аттестационных испытаний.  - Протоколы аттестационных испытаний.  - Заключение по результатам аттестационных испытаний.  - Аттестат соответствия требованиям по безопасности персональных данных (в случае положительного заключения).  При невозможности выдачи Аттестата соответствия в Заключении должны быть указаны выявленные недостатки с рекомендациями по их устранению. |

6. Порядок контроля и приемки СЗПДн

Контроль и приемка работ осуществляются на основании настоящего Частного технического задания, соответствующих программ и методик испытаний.

Содержание отчетных материалов согласуется на уровне ответственных специалистов Заказчика и Исполнителя.

Дополнения, уточнения или изменения в технической задание могут вноситься по согласованию Сторон и должны оформляться в виде приложений к настоящему Частному техническому заданию и подписываться уполномоченными представителями Сторон.

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

Испытания проводятся на площадках развертывания СЗПДн.

7. Требования к документированию

Перечень подлежащих к разработке комплектов и видов документов, а также формы их представления Заказчику и требования к их оформлению представлены в Договоре.

Вся документация должна быть выполнена на русском языке.

8. Источники разработки

Настоящее Частное техническое задание разработано на основе следующих документов и информационных материалов:

- Договор между ООО «ВЛАДЕЛЕЦ ИСПДН» и ООО «ОРГАН ПО АТТЕСТАЦИИ»;

- Модель угроз безопасности информации Информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН»;

- Отчет об обследовании информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН»;

- Акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН».

Лист согласования

СОСТАВИЛИ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование организации, предприятия | Должность  исполнителя | Фамилия и инициалы | Подпись | Дата |
| ООО «ОРГАН ПО АТТЕСТАЦИИ» |  |  |  |  |

СОГЛАСОВАНО

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование организации, предприятия | Должность  исполнителя | Фамилия и инициалы | Подпись | Дата |
|  |  |  |  |  |
|  |  |  |  |  |