Утвержден

**СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**«ВЛАДЕЛЕЦ ИСПДН»**

**ООО «ВЛАДЕЛЕЦ ИСПДН»**

**ТЕХНИЧЕСКИЙ ПРОЕКТ**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Листов 44

**2024**

**СОДЕРЖАНИЕ**

Перечень сокращений и обозначений 3

1. Общие положения 4

1.1 Наименование проектируемой системы 4

1.2 Перечень документов, на основании которых разрабатывается СЗПДн 4

1.3 Назначение и цели создания СЗПДн ИСПДн 5

1.4 Функции СЗПДн ИСПДн 6

2. Характеристика объекта информатизации 7

2.1 Описание ИСПДн 7

2.2 Состав персональных данных, обрабатываемых в ИСПДн 8

2.3 Перечень объектов защиты ИСПДн 9

2.4 Сведения о классификации системы 9

3. Обобщенная модель защиты 10

3.1 Определение субъектов и объектов доступа 10

3.2 Определение методов управления доступом 11

3.3 Выбор мер защиты информации 12

3.3.1 Определение базового набора мер защиты информации ИСПДн 13

3.3.2 Адаптация базового набора мер защиты информации ИСПДн 22

3.3.3 Уточнение адаптированного базового набора мер защиты информации 31

3.3.4 Дополнение уточненного адаптированного базового набора мер защиты информации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 34

4. Основные технические решения 35

4.1 Анализ дополненного уточненного адаптированного базового набора мер защиты информации и описание вариантов их реализации 35

4.2 Критерии выбора средств защиты информации 35

5 Мероприятия по подготовке объекта автоматизации к вводу в действие 37

5.1 Мероприятия по сбору и приведению входной информации к виду, пригодному для обработки на ЭВМ 37

5.2 Мероприятия по обучению и проверке квалификации персонала 37

5.3 Мероприятия по изменению объекта автоматизации и созданию необходимых подразделений и рабочих мест 37

5.4 Другие мероприятия, исходящие из специфических особенностей создаваемой СЗПДн ИСПДн 37

5.5 Разработка эксплуатационной и организационно-распорядительной документации 40

ЗАКЛЮЧЕНИЕ 42

ЛИСТ СОГЛАСОВАНИЯ 44

# 

# Перечень сокращений и обозначений

АИБ - Администратор информационной безопасности

АРМ – автоматизированное рабочее место

АС – автоматизированная система

БД – база данных

ВИ - Виртуальная инфраструктура

ЗИ - Защита информации

ИБ - Информационная безопасность

ИС – информационная система

ИСПДн – информационная система персональных данных

КЗ - контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ - межсетевой экран

НСД – несанкционированный доступ

ОРД – организационно распорядительная документация в части защиты информации

ОС - операционная система

ПДн – персональные данные

ПО – программное обеспечение

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

ТП - Технический проект

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

ЭП - Электронная подпись

# 1. Общие положения

Система защиты персональных данных (далее - СЗПДн) информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее – ИСПДн «ВЛАДЕЛЕЦ ИСПДН», 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»).

**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:

## 1.1 Наименование проектируемой 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 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);

- Приказ 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 Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10 июля 2014 года № 378.

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 проекта 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).

## 1.3 Назначение и цели создания СЗПДн 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.

## 1.4 Функции СЗПДн ИСПДн

Основные схемотехнические решения, структура системы информационной безопасности, состав средств защиты информации СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и технологии защиты определяются:

- структурно-функциональными характеристиками ИСПДн «ВЛАДЕЛЕЦ ИСПДН», используемыми информационными технологиями, особенностями функционирования информационной системы;

- моделью угроз безопасности информации (МУ) ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- требованиями руководящих документов ФСТЭК России и ФСБ России, предъявляемыми к установленному уровню защищенности ПДн;

- требованиями о защите информации, установленными иными нормативными правовыми актами в области защиты информации.

Компоненты СЗПДн комплексно выполняют функции по защите информации от несанкционированного доступа, антивирусной защиты, ориентированные на эффективное обеспечение информационной безопасности ИСПДн.

# 2. Характеристика объекта информатизации

## 2.1 Описание ИСПДн

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

ИСПДн «ВЛАДЕЛЕЦ ИСПДН» (далее также ИСПДн) расположена по адресу:

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

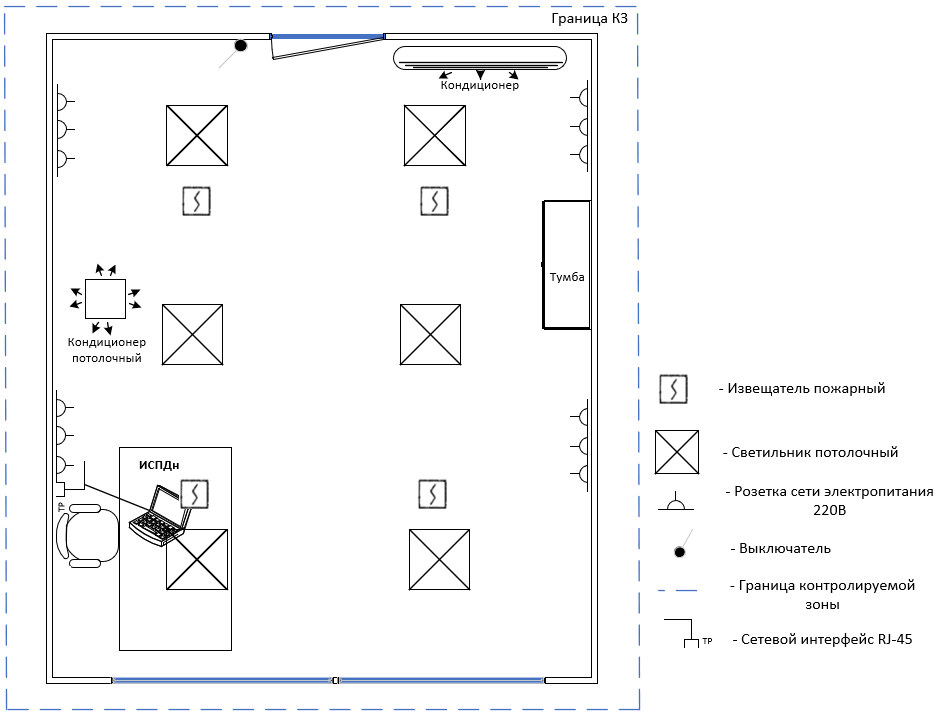


Рисунок 1- Схема расположения технических средств ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Взаимодействие субъектов доступа осуществляется на следующих программных уровнях ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

В состав ИСПДн «ВЛАДЕЛЕЦ ИСПДН» входят следующие компоненты:

а) программные средства:

– базовая система ввода-вывода программно-технических средств;

– системное программное обеспечение (операционная система);

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

– специальное программное обеспечение (СПО), на базе которого реализуется основной функционал ИС.

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.

Беспроводной доступ (с использованием специального оборудования прямой беспроводной связи) к компонентам ИСПДн «ВЛАДЕЛЕЦ ИСПДН» не осуществляется.Мобильный доступ к компонентам ИСПДн «ВЛАДЕЛЕЦ ИСПДН» с помощью мобильных и портативных технических средств отсутствует.Технологии мобильного кода в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» не используются.Для администрирования ИСПДн «ВЛАДЕЛЕЦ ИСПДН» используются только штатные средства операционных систем и прикладного программного обеспечения ИСПДн «ВЛАДЕЛЕЦ ИСПДН».Ввод и передача речевой, видео- и графической- информации с помощью технических средств обработки речевой, видео- и графической информации (видеокамеры, микрофоны) в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» не осуществляется.

## 2.2 Состав персональных данных, обрабатываемых в 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 субъектов, 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.

## 2.3 Перечень объектов защиты 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.

## 2.4 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 субъектов, 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).**

## ****3. Обобщенная модель защиты****

## 3.1 Определение субъектов и объектов доступа

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» объектами доступа являются:

- информация, обрабатываемая в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» (включая ПДн);

- технические средства:

- автоматизированное рабочее место (АРМ) сотрудников ООО «ВЛАДЕЛЕЦ ИСПДН», предназначенное для обработки ПДн, а также для обслуживания и управления компонентами ИСПДн (администрирования);

- машинными носителями информации (машинные носители информации, входящие в состав вычислительной инфраструктуры ИСПДн, машинные носители информации, входящие в состав АРМ, съемные машинные носители информации);

- системы и средства связи и передачи данных (активное сетевое оборудование и физические линии связи, обеспечивающие коммутацию, маршрутизацию и передачу данных в рамках ИСПДн);

- программные средства:

– базовая система ввода-вывода программно-технических средств;

– системное программное обеспечение (операционная система);

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

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

- средства защиты информации (средства идентификации и аутентификации пользователей, средства управления доступом пользователей, средства обеспечения регистрации и учета действий пользователей, антивирусные средства, средства межсетевого экранирования), входящие в СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Субъектами доступа в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» являются:

- пользователи ИСПДн «ВЛАДЕЛЕЦ ИСПДН», взаимодействующие с системным, общесистемным и прикладным программным обеспечением на АРМ, входящих в состав ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- администраторы безопасности, осуществляющие администрирование СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- системные администраторы, сетевые администраторы, сетевые инженеры, осуществляющие техническое обслуживание и администрирование технических и программных средств ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

## 3.2 Определение методов управления доступом

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» методы управления доступом реализуются с учетом особенностей функционирования информационной системы и угроз безопасности информации.

Существует три основных метода управления доступом:

- дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и списка объектов доступа, 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 и каждого объекта доступа, являющиеся комбинациями иерархических и неиерархических категорий.

Поскольку все пользователи имеют различный доступ к защищаемой информации (персональным данным), а администрирование средств защиты информации возлагается на администратора безопасности, предлагается реализовать ролевой метод управление доступом, который будет предусматривать следующие роли:

- Системный администратор (CA) - этот субъект доступа обладает полными правами по созданию, удалению, блокированию учетных записей пользователей и назначению им полномочий (ролей) на АРМ ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- Администратор информационной безопасности (АИБ) - этот субъект доступа обладает полными правами по установке, настройке, удалению и администрированию всех средств защиты информации, используемых СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН», а также полными правами по созданию, удалению, блокированию учетных записей пользователей и назначению им полномочий (ролей) применительно к средствам защиты информации;

В ООО «ВЛАДЕЛЕЦ ИСПДН» фактически роли СА и АИБ совмещают одни и те же сотрудники, что допускается для УЗ 3 согласно положениям Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Таким образом ролевая модель ООО «ВЛАДЕЛЕЦ ИСПДН» соответствует требованиям для 3 УЗ (Замечаний нет).

- Пользователь (П) - этот субъект доступа обладает возможностями по внесению, редактированию, копированию информации только на уровне Приложения ИСПДн «ВЛАДЕЛЕЦ ИСПДН». Роль «Пользователь» может предусматривать различные подвиды с ограничениями, установленными по доступу к различному функционалу системы.

## 3.3 Выбор мер защиты информации

В ходе проектирования СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется выбор мер защиты информации для их реализации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» в соответствии с частным техническим заданием на создание СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Выбор мер защиты осуществляется в соответствии с порядком, установленным пунктом 9 документа «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):

- определение базового набора мер защиты информации для установленного уровня защищенности ИСПДн «ВЛАДЕЛЕЦ ИСПДН» в соответствии с базовыми наборами мер защиты информации документа «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);

- адаптация 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 ИСПДн «ВЛАДЕЛЕЦ ИСПДН», или структурно-функциональными характеристиками, не свойственными ИСПДн «ВЛАДЕЛЕЦ ИСПДН»);

- 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»;

- 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.

### 3.3.1 Определение базового набора мер защиты информации 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» (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21), в качестве начального выбирается один из четырех базовых наборов мер защиты информации, соответствующий установленному уровню защищенности ПДн.

Меры защиты информации, обозначенные знаком «+» в Приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, включаются в базовый набор мер защиты информации для соответствующего уровня защищенности ПДн. Меры защиты информации, не обозначенные знаком «+», к базовому набору мер не относятся, и применяются при последующих действиях по адаптации, уточнению, дополнению мер защиты информации, а также разработке компенсирующих мер защиты информации.

Меры (функции) защиты, подлежащие реализации в СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН», в рамках базового набора мер по обеспечению безопасности персональных данных для 3-ого (третьего) уровня защищенности (УЗ3) персональных данных определены ниже.

Таблица 1 - Состав и содержание мер по обеспечению безопасности УЗ3 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 |

### 3.3.2 Адаптация базового набора мер защиты информации ИСПДн

Адаптация базового набора мер защиты информации предполагает изменение начально выбранного базового набора мер защиты информации в части его максимальной адаптации применительно к структуре, реализации и особенностям эксплуатации ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

При адаптации базового набора мер защиты информации учитывались:

– цели и задачи защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

– перечень мероприятий, проводимых оператором по обеспечению безопасности информации в рамках организации в целом;

– применяемые информационные технологии и структурно-функциональные характеристики ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Адаптация базового набора мер защиты информации предусматривает исключение мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Состав и содержание адаптированного базового набора мер защиты информации для ИСПДн «ВЛАДЕЛЕЦ ИСПДН» приведены ниже.

Таблица 2 - Адаптированный базовый набор мер защиты для ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

| **Условное обозначение и № меры** | **Содержание мер по обеспечению безопасности персональных данных** | **УЗ ПДн** | | | | **Подлежит реализации**  **для УЗ** | **Указание к применению** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 3 | 2 | 1 |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + | Да | Применимо |
| 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 | Применимо |
| 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 | Применимо |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + | Да | Применимо |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | + | + | Да | Нет |
| **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 | Применимо |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + | Да | Применимо |
| 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 | Применимо |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + | + | + | Да | Применимо |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | + | + | + | Да | Применимо |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + | + | Да | Применимо |
| 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 | Применимо |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |  | + | + | + | Да | Применимо |
| 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 | Нет |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + | + | Да | Нет |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + | + | Да | Нет |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + | + | Да | Нет |
| 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 | Применимо |
| **V. Регистрация событий безопасности (РСБ)** | | | | | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + | Да | Применимо |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + | Да | Применимо |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + | Да | Применимо |
| 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 | Применимо |
| **VI. Антивирусная защита (АВЗ)** | | | | | | | |
| АВЗ.1 | Реализация антивирусной защиты | + | + | + | + | Да | Применимо |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | + | + | + | Да | Применимо |
| **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 | Применимо |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + | + | Да | Применимо |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |  | + | + | + | Да | Применимо |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |  | + | + | + | Да | Применимо |
| 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 | Нет |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + | Да | Нет |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |  | + | + | + | Да | Нет |
| 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 | Нет |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей |  | + | + | + | Да | Нет |
| **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 | Применимо |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | + | + | + | Да | Применимо |
| 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 | Нет |
| 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 | Нет |
| **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 | Применимо |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |  | + | + | + | Да | Применимо |
| 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 | Применимо |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |  | + | + | + | Да | Применимо |

### 3.3.3 Уточнение адаптированного базового набора мер защиты информации

Уточнение адаптированного базового набора мер защиты информации проводится с целью оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все актуальные угрозы безопасности информации, включенные в модель угроз безопасности, или снизить вероятность их реализации исходя из условий функционирования ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Таблица 3 – Уточненный адаптированный базовый набор мер ЗИ

| **Условное обозначение и № меры** | **Содержание мер по обеспечению безопасности персональных данных** |
| --- | --- |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| **III. Ограничение программной среды (ОПС)** | |
| **IV. Защита машинных носителей персональных данных (ЗНИ)** | |
| 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 |
| **V. Регистрация событий безопасности (РСБ)** | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.7 | Защита информации о событиях безопасности |
| **VI. Антивирусная защита (АВЗ)** | |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| **VII. Обнаружение вторжений (СОВ)** | |
| **VIII. Контроль (анализ) защищенности персональных данных (АНЗ)** | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| **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)** | |
| 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 |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (3ИС)** | |
| **XIV. Выявление инцидентов и реагирование на них (ИНЦ)** | |
| **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 |
| 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 результате было установлено, что выбранный набор мер защиты перекрывает все актуальные угрозы безопасности ИСПДн, отраженные в Модели угроз безопасности информации Информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН».

### 3.3.4 Дополнение уточненного адаптированного базового набора мер защиты информации ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

Дополнение уточненного адаптированного базового набора мер защиты информации осуществляется с целью выполнения требований о защите информации, установленных иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

С целью выполнения требований документа «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119) в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» 3-го уровня защищенности персональных данных необходимо выполнение следующих требований:

– организация режима обеспечения безопасности помещений, в которых размещена ИСПДн «ВЛАДЕЛЕЦ ИСПДН», 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 ИСПДн «ВЛАДЕЛЕЦ ИСПДН», 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 ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

# 4. Основные технические решения

## 4.1 Анализ дополненного уточненного адаптированного базового набора мер защиты информации и описание вариантов их реализации

Для реализации мер защиты информации, связанных с обеспечением ИСПДн «ВЛАДЕЛЕЦ ИСПДН» программными средствами защиты, возможны следующие варианты их реализации:

- с помощью прикладных программных или программно-аппаратных средств защиты информации (комплексов средств защиты), прошедших в установленном порядке процедуру оценки соответствия по требованиям безопасности информации;

- с помощью специальных внешних служб и сервисов, предоставляемых по договору (сервис антивирусной защиты, межсетевого экранирования и др.), прошедших в установленном порядке процедуру оценки соответствия по требованиям безопасности информации;

- с помощью встроенных (штатных) функциональных возможностей и механизмов защиты информации операционной системы и прикладного программного обеспечения ИСПДн «ВЛАДЕЛЕЦ ИСПДН» (специальное (ключевое) функциональное программное обеспечение ИСПДн «ВЛАДЕЛЕЦ ИСПДН», далее Приложение), прошедших в установленном порядке прохождение процедуры оценки соответствия по требованиям безопасности информации.

## 4.2 Критерии выбора средств защиты информации

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 соответствии с требованиями технического задания на создание СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» выбираемые средства защиты информации, помимо стоимости выбирались по следующим критериям:

- в составе СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должно использоваться только лицензионное программное обеспечение средств защиты информации,

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

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

- в составе СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, N 52, ст. 5140; 2007, N 19, ст. 2293; N 49, ст. 6070; 2008, N 30, ст. 3616; 2009, N 29, ст. 3626; N 48, ст. 5711; 2010, N 1, ст. 6; 2011, N 30, ст. 4603; N 49, ст. 7025; N 50, ст. 7351; 2012, N 31, ст. 4322; 2012, N 50, ст. 6959)

- в СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должны применяться средства защиты информации 6 класса и 6 уровня доверия, а также средства вычислительной техники не ниже 5 класса (РД СВТ);

- при выборе средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, необходимо руководствоваться пунктом 2 Информационного сообщения ФСТЭК «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 г. № 240/24/4669;

- преимущество должны применяться средства защиты информации, имеющие сертификаты (свидетельства) совместимости со средствами защиты информации, также применяемыми в СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- преимущество должны применяться средства защиты информации, прошедшие функциональное тестирование, оценку качества и (или) надежности независимыми от производителей исследовательскими и испытательными организациями;

# 5 Мероприятия по подготовке объекта автоматизации к вводу в действие

## 5.1 Мероприятия по сбору и приведению входной информации к виду, пригодному для обработки на ЭВМ

Входную информацию для средств защиты информации из состава СЗИ формирует назначенный приказом Генерального директора ООО «ВЛАДЕЛЕЦ ИСПДН» администратор информационной безопасности ИСПДн, который определяет необходимые режимы и конфигурации средств защиты информации, обеспечивающие неизменность условий функционирования и обработки защищаемой информации.

## 5.2 Мероприятия по обучению и проверке квалификации персонала

Подготовка и проверка квалификации администратора безопасности информации осуществляется в соответствии с внутренними планами обучения и проверок сотрудников ООО «ВЛАДЕЛЕЦ ИСПДН».

Первичная подготовка и обучение администраторов и конечных пользователей предполагается с использованием соответствующих инструкций, руководств и эксплуатационной документацией на средства защиты, а также консультаций исполнителя работ по созданию СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

## 5.3 Мероприятия по изменению объекта автоматизации и созданию необходимых подразделений и рабочих мест

Мероприятия по изменению объекта автоматизации и созданию необходимых подразделений и рабочих мест в ООО «ВЛАДЕЛЕЦ ИСПДН» не проводятся, так как СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» создается на базе уже введенного в эксплуатацию помещении и оборудования, функционирующих в штатных режимах, предусмотренных в «ВЛАДЕЛЕЦ ИСПДН».

Штатного персонала достаточно для обслуживания объекта информатизации и СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

## 5.4 Другие мероприятия, исходящие из специфических особенностей создаваемой СЗПДн ИСПДн

Для обслуживания СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» необходим один администратор информационной безопасности.

Администратор информационной безопасности:

– осуществляет контроль за целевым использованием автоматизированной системы, а также всех ее внешних устройств;

– осуществляет контроль за правильностью настроек средств защиты информации;

– осуществляет контроль за физическим доступом к компонентам ИСПДн;

– осуществляет настройку и сопровождение подсистемы управления доступом;

– реализует полномочия доступа пользователя к элементам защищаемых информационных ресурсов ИСПДн на основе утвержденной разрешительной системы доступа;

– проводит периодическую проверку работоспособности системы защиты от НСД, а также при изменении программной среды и полномочий пользователей ИСПДн;

– один раз в три месяца, а также в случае необходимости (компрометация пароля) производит смену паролей пользователей для доступа в систему. Периодически уточняет список прав доступа и полномочия сотрудников по доступу к средствам вычислительной техники, которые используются для обработки конфиденциальных сведений;

– проводит периодический контроль принятых мер по защите.

Администратор информационной безопасности обязан:

– обеспечивать функционирование и поддерживать работоспособность средств защиты автоматизированной системе в пределах, возложенных на него функций.

– в случае отказа работоспособности технических средств и программного обеспечения СВТ ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности, в своей части по согласованию с ответственным за эксплуатацию ИСПДн.

– информировать ответственного за защиту информации о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

– знать состав технических средств и программных ресурсов ИСПДн, предназначенных для обработки информации, и перечень задач (прикладных программ), решаемых с их использованием.

– в случае выявления каких-либо несанкционированных действий пользователя, несущих в себе угрозу для безопасности информации, поставить в известность об этом ответственного за защиту информации, временно заблокировать возможность работы пользователя в ИСПДн и принять меры по исключению таких действий.

– не реже 1 раза в неделю выполнять работу по администрированию ИСПДн в части делегированных ему полномочий роли системного администратора, проверять данные в системном журнале, в журнале учёта носителей информации и в случае необходимости распечатывать системные журналы СЗИ. В случае выявления попыток НСД к защищаемой информации представлять журнал ответственному за защиту информации.

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения конфиденциальной информации (в том числе диски корпоративной системы хранения данных (СХД)). Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие проверку.

– присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн.

– контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн (в т.ч. реальной конфигурации информационных связей).

– хранить, осуществлять прием и выдачу персональных идентификаторов пользователей, осуществлять контроль за правильностью использования персонального идентификатора пользователем ИСПДн.

– проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам АС. При выявлении таких каналов сообщать о них ответственному за защиту информации и принимать меры по исключению вмешательства в работу ИСПДн.

– проводить инструктаж пользователя ИСПДн по правилам работы с используемой СЗИ.

– не реже одного раза в год проводить тестирование всех функций СЗИ с помощью специальных программных средств.

СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» вводится в эксплуатацию приказом Генерального директора ООО «ВЛАДЕЛЕЦ ИСПДН» по результатам ее разработки или доработки.

В случае сбоев средств защиты информации из СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» администратор информационной безопасности предпринимает все необходимые меры по восстановлению их работоспособности в максимально короткие сроки в соответствии с инструкцией администратора информационной безопасности и эксплуатационной документацией на средства.

В случае необходимости внесения каких-либо изменений в систему защиты персональных данных ИСПДн ответственный представитель ООО «ВЛАДЕЛЕЦ ИСПДН» обязан согласовать изменения с проводившей оценку соответствия в форме аттестации по требованиям безопасности информации организацией – лицензиатом ФСБ и ФСТЭК России.

## 5.5 Разработка эксплуатационной и организационно-распорядительной документации

Для обеспечения безопасности и аттестации СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должен быть разработан следующий пакет ОРД:

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 (при необходимости).

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 (при необходимости).

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. Приказ о назначении оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям (при необходимости).

10. Технический паспорт информационной системы.

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

12. Описание технологического процесса обработки информации в информационной системе.

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

14. Инструкция администратору безопасности информации информационной системы.

15. Инструкция по эксплуатации системы защиты информации.

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

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

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

19. Акт классификации / установления уровня защищенности.

# ЗАКЛЮЧЕНИЕ

На основе анализа актуальных угроз безопасности информации ИСПДн «ВЛАДЕЛЕЦ ИСПДН», приведенных в Модели угроз и нарушителя, функциональных характеристик рассмотренных средств защиты информации и частного технического задания на СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН» были разработаны технические решения, реализующие предлагаемую модель защиты и функции назначения СЗПДн ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Для защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» были выбраны следующие средства защиты информации:

* СЗИ от НСД «Secret Net Studio»;

Места установки СЗИ указаны в таблице 4.

Таблица 4 - сводный перечень средств защиты информации и мест их установки для ИСПДн «ВЛАДЕЛЕЦ ИСПДН»

| **№ п/п** | **Наименование и тип СЗИ** | **Сведения о сертификате** | **Место**  **установки** |
| --- | --- | --- | --- |
|  | **Средство защиты информации Secret Net Studio 8.**  Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к САВЗ, Профиль защиты САВЗ(А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ), Профиль защиты САВЗ(Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ), Профиль защиты САВЗ(В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ), Профиль защиты САВЗ(Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ), Требования к СКН, Профиль защиты СКН(контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ), Требования к СОВ, Профили защиты СОВ(узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ), ЗБ, РД СВТ(5) | Сертификат соответствия ФСТЭК России № 3745,  действителен до 16.05.2025 | АРМ  ИСПДн «ВЛАДЕЛЕЦ ИСПДН» |

Спецификация закупаемых средств защиты информации приведена в таблице 5.

Таблица 5 – Спецификация закупаемых средств защиты информации

| **№ п/п** | **Наименование и тип СЗИ** | **Кол- во** | **Цена рублей за ед.**  **(на один объект)** | **Стоимость**  **(рублей)** |
| --- | --- | --- | --- | --- |
|  | **Средство защиты информации Secret Net Studio 8.** | 1 | 7169,00  (Максимальная защита) | 7200 |

Стоимость составляет 14 369,00 рублей (Четырнадцать тысяч триста шестьдесят девять рублей 00 копеек).

# ЛИСТ СОГЛАСОВАНИЯ

СОСТАВИЛИ

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

СОГЛАСОВАНО

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