|  |
| --- |
| Конфиденциально |
| Экз. № \_\_ |

|  |
| --- |
| **УТВЕРЖДАЮ** |
| Генеральный директор  ООО «ВЛАДЕЛЕЦ ИСПДН» |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ген. директор |

**ТЕХНИЧЕСКИЙ ПАСПОРТ**

**информационной (автоматизированной) системы  
«ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН»**

**1. Общие сведения об информационной (автоматизированной) системе.**

**1.1. Наименование и назначение информационной (автоматизированной) системы:**

Информационная система персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее по тексту – ИС) является автоматизированной системой, обрабатывающей персональные данные как сотрудников, так и субъектов, не являющихся сотрудниками. Примерная тематика и (или) специализация ИС: предназначена для автоматизации процессов экономической и организационной деятельности.

**1.2. Расположение информационной (автоматизированной) системы персональных данных:**

**1.3. Установленный класс защищенности информационной (автоматизированной) системы (категория значимого объекта, уровень защищенности персональных данных):**

Уровень защищенности персональных данных – 3 (третий)(Акт установления уровня защищенности персональных данных информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» от 27.02.2024).

**1.4. Сведения о вводе информационной (автоматизированной) системы в эксплуатацию:**

Приказ ООО «ВЛАДЕЛЕЦ ИСПДН» «О вводе информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» в эксплуатацию».

**2. Условия эксплуатации информационной (автоматизированной) системы.**

**2.1. Сведения об архитектуре информационной (автоматизированной) системы, включающие описание структуры и состава (типовых компонентов), структурную (топологическую) схему с указанием информационных связей между компонентами информационной (автоматизированной) системы и иными информационными системами, в том числе с сетью Интернет.**

ИС имеет сосредоточенную структуру и состоит из одного АРМ с подключением к сети Интернет.

Схема общей архитектуры ИС, топологии и размещение относительно границ контролируемой зоны приведена на рисунках 1 и 2.

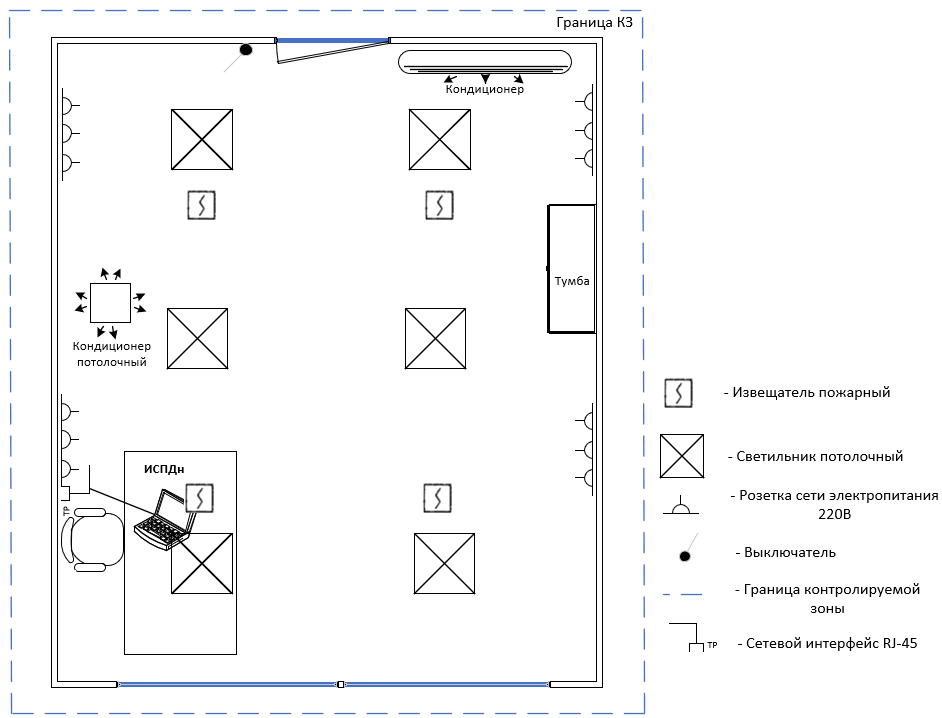


Рисунок 2 - Схема размещения ИСПДн относительно границ контролируемой зоны

**2.2. Описание технологического процесса обработки информации и режимы доступа к информационным ресурсам, включающее описание всех типов внешних, внутренних пользователей (привилегированных, непривилегированных), полномочий пользователей и тип доступа к информационным ресурсам.**

ИС предназначена для обработки информации ограниченного доступа, которая относится к конфиденциальной в соответствии с Перечнем информационных систем персональных данных (ИСПДн), в которых должна быть обеспечена безопасность информации, Перечнем защищаемых ресурсов, в том числе персональных данных и листом ознакомления к нему, утверждённым Генеральным директором ООО «ВЛАДЕЛЕЦ ИСПДН».

ИС реализует следующие функции по работе с информацией ограниченного доступа, составляющей сведения конфиденциального характера:

- ввод (создание) информации;

- обработка (редактирование) информации;

- хранение информации;

- удаление (уничтожение) информации.

Ответственный за защиту информации сотрудник (далее – ответственный сотрудник) в соответствии с приказом «О назначении должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе» несет ответственность и обеспечивает с помощью имеющихся на объекте инженерно-технических средств и систем:

- физическую защиту помещения и находящихся в нем технических средств;

- контроль доступа в помещение;

- надежные препятствия против несанкционированного проникновения в помещение и доступа к хранилищу защищаемых носителей информации посторонних лиц, особенно в нерабочее время, исключающее хищение и порчу документов и информационных носителей, самих средств информатизации;

- противодействие нахождение внутри контролируемой зоны технических средств разведки и промышленного шпионажа.

Предусмотрен следующий режим доступа в помещение с компонентами ИС:

1) Ответственный сотрудник, руководствуясь разрешительной системой доступа, осуществляет контроль доступа лиц, допущенных к нахождению в помещении с компонентами ИС.

2) Ответственный сотрудник обеспечивает контроль доступа и защиту от несанкционированного доступа в помещение с ИС путем запирания помещения дверью на механический замок по факту его покидания сотрудниками.

3) Ответственный сотрудник ведет журнал регистрации доступа в помещение с ИС.

4) В случае выявления попытки или факта доступа посторонних лиц в помещение с компонентами ИС инициирует разбирательство с оповещением и привлечением руководства, органов исполнительной власти и иных заинтересованных лиц с последующим выявлением, предотвращением и восстановлением возможных повреждений компонентов ИС, выявление факта утечки, разглашения и несанкционированного доступа к хранимой и обрабатываемой в ИС конфиденциальной информации.

Работа на АРМ из состава ИС осуществляется в соответствии с утвержденным перечнем «Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей».

Предусмотрен следующий режим работы субъектов доступа в ИС:

1) В начале сеанса, включив АРМ из состава ИС и войдя в операционную систему с использованием персонального идентификатора (логина) и аутентификатора (пароля), субъект доступа ИС получает установленные Администратором информационной безопасности ИС (далее - Администратор) права доступа к информационным и техническим ресурсам.

2) субъект доступа ИС с помощью штатных средств системного и прикладного программного обеспечения выполняет заданные ему ролевой моделью и должностной инструкцией работы и обязанности, с учетом положений документа «Инструкция пользователя …», обращается к защищаемой информации и компонентам, и ресурсам ИС в соответствии с разрешительной системой доступа.

3) Все данные, полученные в результате работы программ, а также исходные данные, необходимые для их корректной работы, пользователь вводит (выводит) на учтенные машинные носители данных.

4) В конце рабочего дня АРМ из состава ИС отключается от питания.

Компоненты ИС расположены в пределах контролируемой зоны. Помещение оборудовано дверью с одним надежным запирающим механическим замком и СКУД, препятствующими против несанкционированного доступа в помещение и компонентам ИС. Допуск лиц в указанное помещение осуществляется только по утвержденному перечню, в соответствии с приказом «Перечень лиц, имеющих право доступа в помещения …».

Для защиты информации от несанкционированного доступа в ИС используется сертифицированный СЗИ от НСД. Настройку системного обеспечения в части защиты информации, настройку СЗИ от НСД для идентификации и аутентификации субъектов доступа, регистрации их действий, контроля целостности системных файлов, и файлов СЗИ НСД, а также контроль работоспособности, периодического тестирования и восстановления СЗИ НСД осуществляет Администратор информационной безопасности.

Обязанности и порядок работы субъектов доступа, в виде Администраторов информационной безопасности и Администраторов операционных систем/сети, принятых ролевой моделью, регламентируется документами: «Разрешительная система доступа объектов информатизации…», «Инструкция по эксплуатации системы защиты персональных данных информационной системы персональных данных», «Инструкция администратора информационной безопасности информационной системы персональных данных…».

Учет машинных носителей конфиденциальной информации ведется ответственным за защиту информации, выдача и сдача съемных носителей осуществляется строго с занесением записей в «Журнал учета машинных носителей конфиденциальной информации (персональных данных)» с указанием даты, времени и ФИО сотрудника, получившего/сдавшего съемный носитель конфиденциальной информации.

В качестве объектов доступа (объектов, содержащих защищаемую информацию), определены ресурсы ИС указанные в таблице 1.

Таблица 1 – Объекты доступа, содержащие защищаемую информацию в ИС

| №  п/п | Наименование (тип) защищаемого ресурса | Гриф конфиденциальности | Место хранения защищаемого ресурса  Windows |
| --- | --- | --- | --- |
| 1 | Программные компоненты, конфигурационные файлы и журналы событий безопасности операционной системы | Конфиденциально | Каталог внутреннего носителя:  C:\Windows\System32 |
| 2 | Программные компоненты, конфигурационные файлы и журналы безопасности СЗИ от НСД | Конфиденциально | Каталог внутреннего носителя:  C:\Windows\  C:\Program files\ |
| 3 | Программные компоненты и конфигурационные файлы антивирусного средства | Конфиденциально | Каталог внутреннего носителя:  C:\Windows\  C:\Program files\ |
| 4 | Программные компоненты и конфигурационные файлы средств обработки конфиденциальных документов | Конфиденциально | Каталог внутреннего носителя:  C:\Program files\ |
| 5 | Файлы с информацией и разрабатываемые документы, хранящиеся на ЖМД ПЭВМ | Конфиденциально | Каталог внутреннего носителя:  C:\Users\<имя пользователя> |

Субъектами доступа к защищаемой в ИС информации являются:

* администратор информационной безопасности,
* системный администратор;
* пользователи.

Для администраторов и пользователей в качестве штатных средств доступа в ИС предусмотрены:

* технические средства (компоненты) ИС в соответствии с таблицей п.3.1;
* программные компоненты системного программного обеспечения в соответствии с таблицей п. 3.2;
* телекоммуникационное оборудование в соответствии с таблицей п. 3.3.

В ИС используются средства защиты информации в соответствии с таблицей п.3.4.

**2.3. Сведения об аттестате соответствия информационно-телекоммуникационной инфраструктуры центра обработки данных, на базе которой функционирует информационная (автоматизированная) система, а также о модели услуг, по которой предоставляются вычислительные услуги (заполняется при условии аттестации информационной (автоматизированной) системы на базе аттестованной на соответствие требованиям по защите информации информационно-телекоммуникационной инфраструктуры центра обработки данных):**

Не применимо.

**3. Состав информационной (автоматизированной) системы.**

3.1. Состав программно-технических средств информационной (автоматизированной) системы:

(указываются типы технических средств, их наименования и модели)

| № п/п | Тип технического средства | Наименование и модели |
| --- | --- | --- |
| 1. | Ноутбук | lenovo t460 i5 |

3.2. Состав общесистемного и прикладного программного обеспечения информационной (автоматизированной) системы:

(указываются типы программного обеспечения, их наименования и основные (мажорные) версии)

| № п/п | Тип программного обеспечения | Наименование | Основная (мажорная) версия |
| --- | --- | --- | --- |
| 1. | Операционная система | Windows | 10 Pro |

3.3. Состав телекоммуникационного оборудования информационной (автоматизированной) системы и используемые для передачи информации линии связи:

(указываются типы оборудования, их наименования и основные (мажорные) версии)

| № п/п | Тип оборудования | Наименование и основная (мажорная) версия |
| --- | --- | --- |
|  | Коммутатор | Keenetic Viva |

3.4. Состав средств защиты информации, используемых в информационной (автоматизированной) системе:

(указываются типы средств, их наименования и основные (мажорные) версии, сведения о сертификатах соответствия)

|  |  |  |
| --- | --- | --- |
| **Тип средства** | **Наименование и основная (мажорная) версия** | **Сведения**  **о сертификате соответствия** |
| Средство защиты информации от несанкционированного доступа | Средство защиты информации Secret Net Studio 8. | Сертификат соответствия ФСТЭК России № 3745 от 16.05.2017 действителен до 16.05.2025 |
| Антивирусное средство | Средство защиты информации Secret Net Studio 8. | Сертификат соответствия ФСТЭК России № 3745 от 16.05.2017 действителен до 16.05.2025 |
| МЭ, СОВ | Средство защиты информации Secret Net Studio 8. | Сертификат соответствия ФСТЭК России № 3745 от 16.05.2017 действителен до 16.05.2025 |

**4. Сведения о соответствии информационной (автоматизированной) системы требованиям по защите информации.**

4.1. Сведения о протоколах аттестационных испытаний информационной (автоматизированной) системы.

(реквизиты протоколов и дата их выдачи)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование документа** | **Организация, проводившая аттестацию** | **Уч. номер**  **документа** | **Дата** |
| 1. | Протокол аттестационных испытаний объекта информатизации «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» по требованиям защиты информации | ООО «ОРГАН ПО АТТЕСТАЦИИ» |  | \_\_.03.2024 |

4.2. Сведения о заключении по результатам аттестационных испытаний информационной (автоматизированной) системы.

(реквизиты заключения и дата выдачи)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование документа** | **Организация, проводившая аттестацию** | **Уч. номер**  **документа** | **Дата** |
| 1. | Заключение по результатам аттестационных испытаний объекта информатизации «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» по требованиям защиты информации | ООО «ОРГАН ПО АТТЕСТАЦИИ» |  | \_\_.03.2024 |

4.3. Сведения об аттестате соответствия информационной (автоматизированной) системы на соответствие требованиям о защите информации.

(реквизиты аттестата соответствия, дата выдачи)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование документа** | **Организация, проводившая аттестацию** | **Уч. номер**  **документа** | **Дата** |
| 1. | Аттестат соответствия  требованиям по защите информации | ООО «ОРГАН ПО АТТЕСТАЦИИ» |  | \_\_.03.2024 |

**5. Сведения о проведении контроля за обеспечением уровня защиты информации, содержащейся в информационной (автоматизированной) системе, приведены в таблице 1.**

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N п/п | Наименование организации (подразделения), проводившей контроль | Дата проведения контроля | Реквизиты документа с выводами о результатах контроля | Вывод по результатам контроля |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |

**6. Сведения об изменениях информационной (автоматизированной) системы и средств защиты информации приведены в таблице 2.**

Таблица 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N п/п | Дата внесения изменения | Документ, на основании которого внесены изменения | Пункт технического паспорта, в который внесены изменения | Краткая характеристика изменений | Подпись лица, внесшего изменения |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| 11 |  |  |  |  |  |
| 12 |  |  |  |  |  |
| 13 |  |  |  |  |  |
| 14 |  |  |  |  |  |
| 15 |  |  |  |  |  |
| 16 |  |  |  |  |  |
| 17 |  |  |  |  |  |
| 18 |  |  |  |  |  |
| 19 |  |  |  |  |  |
| 20 |  |  |  |  |  |

Ответственный за обеспечение защиты информации в ходе эксплуатации информационной (автоматизированной) системы

|  |  |
| --- | --- |
| Инженер-программист  (должность)  . | \_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия и инициалы) |