|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | **УТВЕРЖДАЮ**  Генеральный директор  ООО «ВЛАДЕЛЕЦ ИСПДН» | | \_\_\_\_\_\_\_\_\_\_\_ | |  | | | |
|  | | |
|  | | |
| **Описание технологического процесса обработки персональных данных в**  **информационной системе персональных данных «ВЛАДЕЛЕЦ ИСПДН»**  **ООО «ВЛАДЕЛЕЦ ИСПДН»** | | |
|  | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  | | |
| **2024 г.** | | |

**1. Описание объекта информатизации**

**1.1. Общие сведения**

Объект информатизации информационная система персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее – ИСПДн «ВЛАДЕЛЕЦ ИСПДН», ИС), функционирует на базе объектов вычислительной техники, указанных в документе «Технический паспорт информационной (автоматизированной) системы …».

**1.2. Назначение и решаемые задачи**

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

В ходе функционирования ИС осуществляется обработка информации ограниченного доступа, которая относится к конфиденциальной в соответствии с «Перечень защищаемых информационных ресурсов …» и «Акт установления уровня защищенности персональных данных…, утверждённых Генеральным директором ООО «ВЛАДЕЛЕЦ ИСПДН».

ИСПДн «ВЛАДЕЛЕЦ ИСПДН» решает следующие задачи, связанные с автоматизированной обработкой информации ограниченного доступа, составляющей сведения конфиденциального характера:

- ввод (создание) информации;

- обработка (редактирование) информации;

- хранение информации;

- удаление (уничтожение) информации.

**1.3. Состав программного обеспечения, участвующего в технологическом процессе обработки информации**

Таблица 1 Перечень программных средств обработки конфиденциальной информации ИС

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

**1.4. Уровень защищенности автоматизированной системы**

Уровень защищенности ИСПДн «ВЛАДЕЛЕЦ ИСПДН» - **3 УЗ.**

**2. Организация работы с конфиденциальной информацией**

**2.1. Доступ пользователя к работе в ИС**

Допуск к работе в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется строго в соответствии с утвержденным приказом Генерального директора ООО «ВЛАДЕЛЕЦ ИСПДН» «О перечне лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных «ВЛАДЕЛЕЦ ИСПДН», необходим для выполнения ими служебных (трудовых) обязанностей».

Ответственный за защиту информации в «ВЛАДЕЛЕЦ ИСПДН» сотрудник (далее – ответственный сотрудник) в соответствии с разрешительной системой доступа и перечнем сотрудников, допущенных в помещение с ИСПДн «ВЛАДЕЛЕЦ ИСПДН», несет ответственность и обеспечивает с помощью имеющихся по месту расположения ИС 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.

**2.2. Настройка средств защиты информации от несанкционированного доступа для конкретных пользователей**

Настройку средств защиты информации от несанкционированного доступа (СЗИ от НСД) и контроль их работоспособности осуществляет администратор информационной безопасности.

Настройки СЗИ от НСД выполнены таким образом, что ввод пароля возможен только не менее шести буквенно-цифровых символов. Смена пароля для пользователей осуществляется администратором информационной безопасности.

СЗИ от НСД не позволяет использовать для входа в систему незарегистрированные пароли и идентификаторы. При несоответствии вводимого имени или пароля, зарегистрированного для данного субъекта доступа, вход в операционную систему невозможен.

**2.3. Обработка информации, содержащей конфиденциальные сведения**

Предусмотрен следующий режим обработки информации, содержащей конфиденциальные сведения субъектами доступа в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»:

- в начале сеанса, включив ПК из состава клиентского сегмента ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и войдя в операционную систему с использованием персонального идентификатора (логина) и аутентификатора (пароля), субъект доступа ИСПДн «ВЛАДЕЛЕЦ ИСПДН» получает установленные администратором информационной безопасности права доступа к информационным и техническим ресурсам.

- 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.

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

**2.4. Хранение документов конфиденциального характера**

Информация хранится в специальных каталогах, контроль и защита которых осуществляется установленным в ИС, сертифицированным СЗИ от НСД.

**2.5. Хранение съемных носителей**

Учет съемных носителей конфиденциальной информации ведется администратором информационной безопасности, выдача и сдача съемных носителей осуществляется строго с занесением записей в журнал учета съемных носителей конфиденциальной информации с указанием даты, времени и ФИО сотрудника, получившего/сдавшего съемный носитель конфиденциальной информации.

**2.6. Удаление электронных документов, содержащих конфиденциальную информацию, со съемных носителей и жестких дисков**

Удаление электронных документов, содержащих конфиденциальную информацию, со съемных носителей и жестких дисков производится только в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» средствами сертифицированного СЗИ от НСД, без помещения удаляемых документов средствами операционной системы в корзину.

**2.7. Уничтожение съемных носителей**

Факт уничтожения носителей, содержащих конфиденциальную информацию, фиксируется администратором информационной безопасности в журнале учета уничтоженных носителей конфиденциальной информации.

**3. Описание технологического процесса обеспечения информационной безопасности**

**3.1. Защита от несанкционированного доступа**

Компоненты ИСПДн «ВЛАДЕЛЕЦ ИСПДН» расположены в пределах контролируемой зоны.

Доступ в помещение осуществляется только в соответствии с утвержденным «Перечень лиц, имеющих право доступа в помещения …».

Для защиты информации от несанкционированного доступа в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» используется сертифицированное программное обеспечение СЗИ от НСД.

Настройку СЗИ от НСД для идентификации и аутентификации субъектов доступа, регистрации их действий осуществляет администратор информационной безопасности в соответствии с «Разрешительной системой доступа …» и эксплуатационной документацией СЗИ от НСД.

**3.2. Антивирусная защита**

Вся входящая информация в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» в соответствии с утвержденным документом «Инструкция по проведению антивирусного контроля…» проверяется на отсутствие вирусов с помощью сертифицированного антивирусного средства.

Установку и настройку антивирусного средства, и обновление антивирусных баз осуществляет администратор информационной безопасности в соответствии с «Инструкцией по проведению антивирусного контроля …» и эксплуатационной документацией на антивирусное средство.

Каждый субъект доступа ежедневно при работе в ИС контролирует работоспособность антивирусного средства и регулярность (наличие актуальности) обновления антивирусных баз.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа приложений, появление посторонних графических и прочих эффектов, искажение или исчезновение файлов, частое появление сообщений о системных ошибках) субъект доступа ИС, руководствуясь «Инструкцией по проведению антивирусного контроля …»:

- прекращает работу в ИС;

- ставит в известность администратора информационной безопасности;

- действует согласно указаниям администратора информационной безопасности.

**3.3. Обеспечение целостности и доступности информации**

Для обеспечения целостности и доступности обрабатываемой информации, а также неизменности программной среды в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» используется СЗИ от НСД и средство анализа защищенности.

Целостность данных, передаваемых из/в ИС (на уровне сети), обеспечивается с помощью сертифицированного межсетевого экрана.

Администратором информационной безопасности проводится периодическое тестирование функций СЗИ от НСД при изменении программной среды и персонала ИС.

Ежемесячно администратором информационной безопасности проводится проверка наличия обновлений и их установка в случае наличия, а также контроль работоспособности используемых в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» средств защиты информации.