|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **УТВЕРЖДАЮ**   |  | | --- | | Генеральный директор  ООО «ВЛАДЕЛЕЦ ИСПДН» | | \_\_\_\_\_\_\_\_\_\_\_\_ | |  | | | |
|  | | |
|  | | |
| **Инструкция пользователя системы защиты персональных данных**  **информационной системы персональных данных**  **«ВЛАДЕЛЕЦ ИСПДН»**  **ООО «ВЛАДЕЛЕЦ ИСПДН»** | | |
|  | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  | | |
| **2024 г.** | | |

# Общие положения

Пользователь системы защиты персональных данных (далее по тексту – Пользователь) назначается приказом руководителя ООО «ВЛАДЕЛЕЦ ИСПДН».

Пользователь системы защиты персональных данных ИСПДн осуществляет обработку персональных данных в информационной системе персональных данных «ВЛАДЕЛЕЦ ИСПДН» (далее – ИСПДн «ВЛАДЕЛЕЦ ИСПДН»).

Пользователь в своей работе руководствуется настоящей Инструкцией, требованиями законов и иных нормативно-правовых актов Российской Федерации по вопросам защиты персональных данных, руководящими и нормативными документами ФСБ и ФСТЭК России, и локальными нормативными актами ООО «ВЛАДЕЛЕЦ ИСПДН».

Пользователем является каждый сотрудник организации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки конфиденциальной информации, в том числе персональных данных.

Пользователь несет персональную ответственность за свои действия.

Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

# Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования внутренних инструкций, руководств по защите информации и распоряжений.

2.2. Знать и соблюдать установленные требования по режиму обработки персональных данных (далее - ПДн), учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.3. Соблюдать требования парольной инструкции.

2.4. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

2.5. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к администратору безопасности ИСПДн.

2.6. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору системы защиты персональных данных (далее по тексту – Администратор безопасности).

2.7. Пользователям запрещается:

Разглашать [защищаемую информацию](../../../../Documents%20and%20Settings/dss/Мои%20документы/Загрузки/Prilozheniya/Приложения/Приложение%206%20Перечень%20персональных%20данных,%20подлежащих%20защите.doc) третьим лицам.

Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

Отключать (блокировать) средства защиты информации.

Обрабатывать в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

Привлекать посторонних лиц для производства ремонта или настройки оборудования ИСПДн «ВЛАДЕЛЕЦ ИСПДН», без согласования с ответственным за обеспечение защиты персональных данных.

2.8. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

2.9. Правила хранение пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

**Лист ознакомления**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Дата** | **Подпись** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |