

## **Инструкция пользователя ИСПДн**

### 1 Общие положения

- 1.1. Настоящая инструкция определяет общие положения работы пользователей в защищенной от несанкционированного доступа информационных системах персональных данных (далее – ИСПДн).
- 1.2. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
- 1.3. Пользователем является каждый сотрудник ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица (далее – Учреждение), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
- 1.4. Пользователь отвечает за правильность функционирования ИСПДн, входа в систему и все действия при работе в ИСПДн.
- 1.5. Пользователь в своей работе руководствуется настоящей инструкцией и документами ФСТЭК России регламентирующими документами.
- 1.6. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

### 2 Должностные обязанности

- 2.1. Допуск пользователей для работы на АРМ осуществляется в соответствии со списком лиц допущенных к работе с персональными данными.
- 2.2. В процессе первичной регистрации пользователь заявляет перечень необходимых для работы ресурсов, перечень персональных данных, состав необходимого общесистемного программного обеспечения для решения поставленных задач.
- 2.3. Пользователь обязан:
  - Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
  - Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным в ИСПДн.
  - Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.
  - Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

- При работе со съемными носителями пользователь должен каждый раз перед началом работы проверить их на наличие вирусов с использованием штатных антивирусных программ.
- В случае обнаружения вирусов на машинных носителях информации (съемных носителях, жестком магнитном диске, твердотельном носителе) пользователь обязан немедленно принять меры.
- В случае оставления рабочей станции без визуального контроля доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>, либо комбинацией клавиш Win + L.

• Принимать меры по реагированию, в случае возникновения штатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

#### 2.4. Пользователям запрещается:

- Разглашать защищаемую информацию 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.
- Обращаться на АРМ информацию и выполнять другие работы, непредусмотренные перечнем прав пользователя по доступу к ИСПДн.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
- Самостоятельно вносить изменения в аппаратно-программную конфигурацию ИСПДн, изменять месторасположение средств отображения информации.

2.5. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

### 3 Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться в соответствии с требованиями законодательства Российской Федерации в области обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

3.2. При работе в Сети запрещается:

- Осуществлять работу при отключенных средствах защиты (антивирус и других).
- Передавать по Сети защищаемую информацию без использования механизмов защиты.
- Запрещается скачивать из Сети программное обеспечение и другие файлы.
- Запрещается посещение сайтов сомнительной репутации (порно сайты, сайты, содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к Сети.