«Утверждаю»

Заведующий МБДОУ № 19

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.В. Нетеса

**ИНСТРУКЦИЯ**

**пользователя информационных систем персональных данных**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1.Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) МБДОУ № 19 Предгорного муниципального района Ставропольского края (далее – Учреждение).

1.2.Субъектами доступа к ресурсам ИСПДн являются администратор безопасности (далее – АБ), пользователи и обслуживающий персонал.

1.3.Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4.Машинные носители информации имеют пометку «ПДн».

1.5.Пользователи получают свои права на доступ к ресурсам ИСПДн через АБ.

1.6.Пользователи имеют право письменно вносить предложения по изменению и дополнению данной Инструкции.

1.7.Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.8.Право толкования положений настоящей Инструкции возлагается на заведующего Учреждением.

**2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

2.1. Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.2. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.3. Доступ к информации – возможность получения информации и ее использования.

2.4. Защита информации — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.6. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.8. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.9. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.10. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1. **ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИСПДН**

Пользователь обязан:

* 1. При работе с документами, содержащими персональные данные, руководствоваться требованиями организационно-распорядительных документов ИСПДн. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПДн.
  2. Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией.
  3. Использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль.
  4. Хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн.
  5. Не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее АРМ.
  6. Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места.
  7. По всем вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПДн, обращаться к администратору информационной безопасности.
  8. Немедленно прекращать обработку персональных данных и ставить в известность администратора информационной безопасности при подозрении компрометации пароля, а также при обнаружении:

- нарушений целостности пломб, наклеек на ПЭВМ (персональные электронно-вычислительные машины), при наличии таковых, или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД);

- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования АРМ;

- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

* 1. Немедленно информировать ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн в случае обнаружения попыток несанкционированного доступа к ИСПДн.
  2. Немедленно информировать сотрудников, осуществляющихсетевое администрирование ОУ, при появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов ОУ.

**4. ДЕЙСТВИЯ, ЗАПРЕЩЕННЫЕ ПОЛЬЗОВАТЕЛЮ ИСПДН**

Пользователю ИСПДн запрещается:

* 1. Предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке.
  2. Записывать пароль на любые носители, в том числе бумажные.
  3. Сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам ИСПДн.
  4. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
  5. Работать с персональными данными в присутствии посторонних (не допущенных к данной информации) лиц.
  6. Самостоятельно изменять конфигурацию аппаратно-программных средств ИСПДн.
  7. Осуществлять действия по преодолению установленных ограничений на доступ к ИСПДн.
  8. Отключать или изменять конфигурацию средств защиты информации ИСПДн.
  9. Устанавливать на АРМ программное обеспечение, не связанное с исполнением служебных обязанностей.

1. **ПРАВА ПОЛЬЗОВАТЕЛЯ ИСПДН**

Пользователь ИСПДн имеет право:

* 1. Получать помощь по вопросам эксплуатации ИСПДн от ответственного за систему защиты информации (далее - СЗИ) ИСПДн.
  2. Обращаться ксотрудникам, осуществляющим сетевое администрированиеОУ, по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ и ИСПДн, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями.
  3. Подавать сотрудникам, осуществляющим сетевое администрирование ОУ, предложения по совершенствованию функционирования ИСПДн.

1. **ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИСПДН**

Пользователь ИСПДн несет ответственность за:

* 1. Обеспечение безопасности персональных данных при их обработке в ИСПДн.
  2. Нарушение работоспособности или вывод из строя системы защиты ИСПДн.
  3. Преднамеренные действия, повлекшие модификацию или уничтожение персональных данных в ИСПДн, и несанкционированный доступ к персональным данным в ИСПДн.
  4. Разглашение персональных данных.
  5. Пользователь, имеющий расширенные права «Опытный пользователь» или «Администратор», несет ответственность за корректное функционирование прикладного программного обеспечения ИСПДн.
  6. За нарушение настоящей Инструкции к пользователю могут применяться меры дисциплинарного воздействия.

1. **ПРАВИЛА РАБОТЫ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА**
   1. Работа в информационно-телекоммуникационных сетях международного информационного обмена - сети Интернет и других (далее – Сеть) на элементах ИСПДн должна проводиться только при служебной необходимости.
   2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусных и других);

- передавать по Сети защищаемую информацию без использования средств шифрования;

- скачивать из Сети программное обеспечение и другие файлы в неслужебных целях;

- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение (ПО), сайты знакомств, онлайн игры и другие).

1. **ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ, ИСПОЛЬЗОВАННЫХ ПРИ РАЗРАБОТКЕ ДАННОГО ПОРЯДКА.**

8.1. Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности (Инструкция пользователя на случай возникновения внештатных ситуаций).

8.2. Инструкция администратора информационной безопасности.

8.3.Разрешительная система доступа к персональным данным, содержащимся в базах данных ИСПДн.

8.4. Инструкция по использованию паролей.

8.5. Порядок резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и системы защиты информации (СЗИ).