

Приложение 7  
к Приказу «О проведении работ по защите  
персональных данных» от «08» июня 2023 г.  
№ 224

**УТВЕРЖДАЮ**

Директор МАУ ДО г. Нягань  
«СШОР «ЦСП»

\_\_\_\_\_ Вараксина Т.Р.  
«\_\_\_» 20 \_\_\_ г.

**ИНСТРУКЦИЯ**  
**администратора безопасности**  
**информационной системы персональных данных**  
**МАУ ДО г. Нягань «СШОР «ЦСП»**

2023г.

**СОДЕРЖАНИЕ**

1. Общие положения.....	3
2. Должностные обязанности.....	4

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Администратором безопасности (АБ) ИСПДн является штатный сотрудник МАУ ДО г. Нягань «СШОР «ЦСП» (далее - Оператор), назначенный приказом директора.
- 1.2. АБ ИСПДн в своей работе руководствуется:
  - Положением по защите персональных данных;
  - Политикой информационной безопасности;
  - Инструкциями по обеспечению безопасности персональных данных;
  - настоящей инструкцией;
  - нормативными документами ФСТЭК России.
- 1.3. АБ ИСПДн осуществляет проведение и контроль мероприятий по обеспечению безопасности персональных данных.
- 1.4. АБ ИСПДн осуществляет методическое руководство работой пользователей ИСПДн.
- 1.5. АБ ИСПДн отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.
- 1.6. АБ ИСПДн несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

## 2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Администратор безопасности ИСПДн обязан:

- 2.1. 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.
- 2.2. Обеспечивать контроль за установкой, настройкой и своевременным обновлением элементов ИСПДн:
  - программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
  - аппаратных средств;
  - аппаратных и программных средств защиты.
- 2.3. Контролировать работоспособность элементов ИСПДн и локальной вычислительной сети.
- 2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
- 2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.
- 2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
- 2.7. Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.
- 2.8. Хранить, осуществлять прием и выдачу логинов пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.
- 2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.
- 2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
- 2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.
- 2.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.
- 2.13. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.