

* недопущение нахождения в помещении, в котором ведется работа с персональными данными, посторонних лиц;
* постоянный контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
* недопущение несанкционированного доступа к персональным данным;
* конфиденциальность персональных данных.

1. **Обеспечение безопасности в экстремальных ситуациях**
   1. При модификации или уничтожения персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.
   2. При нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление.
   3. При обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.
   4. В случае несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных необходимо произвести разбирательство и составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
   5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность директора образовательного учреждения и произвести разбирательство.
2. **Обеспечение безопасности при завершении обработки персональных данных**
3. После завершения сеанса обработки персональных данных необходимо обеспечить:

* исключение возможности несанкционированного проникновения или нахождения в помещении, в котором размещены информационные системы и ведется работа с персональными данными;
* работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных;
* фиксацию всех случаев нарушения данной инструкции в журнале.

1. **Заключительные положения**
2. Проверка и пересмотр настоящей инструкции осуществляются в следующих случаях:

* при пересмотре межотраслевых и отраслевых требований обеспечения безопасности персональных данных;
* при внедрении новой техники и (или) технологий;
* по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности персональных данных;
* по требованию представителей Федеральной службы безопасности.

1. Ответственность за своевременную корректировку настоящей инструкции возлагается на заведующего ДОУ.