

**Инструкция  
по обеспечению безопасности персональных данных**

**1. Общие положения**

- 1.1. Настоящая Инструкция разработана в соответствии со ст. 19 Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», на основании Федерального закона РФ от 27.07.2007 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства РФ от 17.01.2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности РФ (ФСБ России), Министерства информационных технологий и связи РФ (Мининформсвязи России) от 13.02.2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», Письма Федерального агентства по образованию № ФАО-6748/52/17-02-09/72 «Об обеспечении безопасности персональных данных», Положения о работе с персональными данными работников и учащихся.
- 1.2. Для обеспечения безопасности персональных данных необходимо исключить несанкционированный, в том числе случайный, доступ к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.
- 1.3. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.
- 1.4. Ответственность за безопасность персональных данных возлагается на лиц, допущенных к их обработке.

**2. Обеспечение безопасности перед началом обработки персональных данных**

- 2.1. Перед началом обработки персональных данных необходимо изучить настоящую Инструкцию.
- 2.2. Перед началом обработки персональных данных необходимо убедиться в том, что:
  - средства защиты персональных данных соответствуют классу информационной системы;
  - в помещении, в котором ведется работа с персональными данными, отсутствуют посторонние лица;
  - носители персональных данных не повреждены;
  - к персональным данным не был осуществлен несанкционированный доступ;
  - персональные данные не повреждены;
  - технические средства автоматизированной обработки и защиты персональных данных находятся в исправном состоянии.

**3. Обеспечение безопасности во время обработки персональных данных**

- 3.1. Во время обработки персональных данных необходимо обеспечить:

- недопущения воздействия на технические средства автоматизированной обработки персональных данных, способного нарушить их функционирование;
- 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.

#### **4. Обеспечение безопасности в экстремальных ситуациях**

- 4.1. При модификации или уничтожения персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.
- 4.2. При нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление.
- 4.3. При обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.
- 4.4. 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.
- 4.5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность директора школы и произвести разбирательство.

#### **5. Обеспечение безопасности при завершении обработки персональных данных**

- 3.1. 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.

#### **6. Заключительные положения**

- 6.1. 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.

Ответственность за своевременную корректировку настоящей инструкции возлагается на директора школы.