



Принято педагогическим советом
МОУ Большесельской СОШ
Протокол №5 от 24.05.2013
Утверждаю
Приказ № 202 от 27.05.2013
Директор МОУ Большесельская СОШ

Е.Ю. Дьячкова
Дьячкова Е.Ю./

Положение по обеспечению безопасности информации, содержащей персональные данные

1. Общие положения

- 1.1. Настоящее Положение разработано в соответствии со статьёй 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) 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».
- 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 так же 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 настоящее Положение.
- 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:
- Недопущение 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 уничтожении персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.
- 4.2. При нарушении порядка предоставления персональных данных пользователем 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**
- 5.1. После завершения сеанса обработки персональных данных необходимо обеспечить:
- 5.2. Исключение возможности несанкционированного проникновения или нахождения в помещении, в котором размещены информационные системы и ведется работа с персональными данными;
- 5.3. Работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных;
- 5.4. Фиксацию всех случаев нарушения в журнале.
- 6. Заключительные положения**
- 6.1. Проверка и пересмотр настоящего Положения осуществляются в следующих случаях:
- При введении новой техники и (или) технологий;

- По результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности персональных данных;
- По требованию представителей Федеральной службы безопасности.