УТВЕРЖДЕНО
приказом заведующего
МБДОУ № 10 «Светлячок»
от 07.07.2021г. № 48-ОД

ПЕРЕЧЕНЬ МЕР,

направленных на исключение несанкционированного доступа и обеспечивающих сохранность персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий Перечень разработан в соответствии со ст. 19 Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных».
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.
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.
4. Ответственность за безопасность персональных данных возлагается на лиц, допущенных к их обработке.

2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕД НАЧАЛОМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Перед началом обработки персональных данных необходимо изучить настоящий Перечень.
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

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

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 руководителя образовательного учреждения и произвести разбирательство.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ЗАВЕРШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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.