



УТВЕРЖДАЮ
Директор МБОУСОШ №2
С.Р. Шолохова
от 01.09.2022г.

ПЕРЕЧЕНЬ МЕР, ПРЕПЯТСТВУЮЩИХ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ И ОБЕСПЕЧИВАЮЩИХ СОХРАННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Перечень мер, направленных на предотвращение неправомерного использования персональных данных (далее - Перечень мер). МБОУСОШ №2 (далее - Школа) определяет порядок противодействия несанкционированному использованию персональных данных сотрудниками, имеющими доступ к такой информации, а также их ответственность, в случае совершения ими действий, повлекших неправомерное использование персональных данных.

1.2. Целью настоящего документа является установление в учреждении процедур, позволяющих исключить возможность несанкционированного доступа к персональным данным и их использования работниками учреждения и третьими лицами в собственных интересах в ущерб интересам граждан.

2. ОСНОВНЫЕ МЕРЫ (ПРОЦЕДУРЫ), ПРЕПЯТСТВУЮЩИЕ НЕСАНКЦИОНИРОВАННОМУ ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Под процедурами, препятствующими несанкционированному использованию персональных данных, в целях реализации настоящего документа, понимаются мероприятия по предупреждению несанкционированного использования, оперативному и последующему контролю использования персональных данных, проводимые сотрудниками Школы.

2.2. В Школе применяются следующие меры, препятствующие несанкционированному доступу к персональным данным:

- ограничение доступа к персональным данным в специализированных программных средствах;
- защита персональных данных при их обработке и архивировании;
- ограничение доступа посторонних лиц в помещения учреждения, предназначенные для осуществления работы с ПД;
- защита рабочих мест работников, осуществляющих операции с программными средствами;
- контроль за соблюдением работниками Школы требований законодательства РФ и иных нормативных правовых актов.

2.3. В целях противодействия несанкционированному использованию персональных данных, предотвращения утечки и обеспечения сохранности

персональных данных, Школой используется следующий комплекс мероприятий.

2.3.1. Ограничение доступа к служебной информации в программных средствах:

- обеспечение доступа к данным только в пределах полномочий, представленных непосредственно исполнителям, обеспечивающим ведение, обработку и учет информации с ПД;

- установление индивидуальных кодов и паролей доступа к данным для каждого исполнителя;

- контроль за соблюдением режима обращения персональных данных осуществляется ответственным за организацию работы по обеспечению защиты информации, а также директором Школы.

2.3.2. Защита персональных данных при ее обработке и архивировании:

- обеспечение дублирования данных в процессе их ввода, предусматривающее сохранность первичного носителя информации;

- установка программных средств для создания резервных копии, способствующих быстрому восстановлению данных;

- использование систем защиты информационно-технических систем и каналов связи от утечки персональных данных;

- осуществление резервного копирования (восстановления) только уполномоченными сотрудниками;

2.3.3. Ограничение доступа посторонних лиц в помещение Школы, предназначенное для осуществления сбора, обработки и хранения информации ПД осуществляются за счёт:

- соблюдения порядка и правил доступа в служебные помещения в соответствии с Положением о защите ПД;

- ограничением доступа работников и посторонних лиц в помещение, в котором размещены персональные компьютеры, вычислительные системы и системы телекоммуникации для осуществления операций с ПД.

2.3.4. Защита рабочих мест работников, осуществляющих сбор и обработку ПД:

- эффективное размещение рабочих мест сотрудников для исключения возможности несанкционированного просмотра документов и информации на мониторах;

- соблюдение сотрудниками правил по обеспечению защиты информации при работе с персональными компьютерами.

2.3.5. Ограничение доступа к персональным данным:

- доступ работников к необходимым документам, только для выполнения своих обязанностей;

- проведение инвентаризации мест хранения документов, содержащих персональные данные.

2.3.6. При приеме на работу, работник дает расписку о неразглашении персональных данных.

2.3.7. Контроль за соблюдением работниками требований законодательства РФ и иных нормативных правовых актов, регулирующих работу с ПД, внутренними документами, возложен на ответственного за организацию обработки персональных данных.

3. ОСУЩЕСТВЛЕНИЕ ПРОЦЕДУР, ПРЕПЯТСТВУЮЩИХ НЕСАНКЦИОНИРОВАННОМУ ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ, И КОНТРОЛЯ ЗА ИХ ИСПОЛНЕНИЕМ

3.1. Проведение процедур, препятствующих несанкционированному использованию персональных данных, и осуществление контроля включают в себя:

3.1.1. Установление требований о неразглашении персональных данных.

3.1.2. Контроль за выполнением работниками требований действующего законодательства РФ и внутренних документов.

3.1.3. Уведомление работников, имеющих доступ к информации о ПД, о недопустимости осуществления операций с ПД как в своих интересах, так и в интересах третьих лиц.

3.1.4. Проведение оперативных проверок на предмет возможной утечки персональных данных в случаях, предполагающих несанкционированное использование персональных данных.

3.1.5. Направление сведений директору об установленных (обнаруженных) случаях несанкционированного использования персональных данных.

4. ОТВЕТСТВЕННОСТЬ

4.1 Ответственный за организацию обработки персональных данных отвечает за:

- осуществление контроля исполнения положений нормативных документов по вопросам организации и эффективного функционирования системы внутреннего контроля;

- контроль исполнения внутренних нормативных документов учреждения по вопросам обеспечения конфиденциальности персональных данных:

- проведение служебных расследований по фактам возможного неправомерного использования работниками персональных данных, о результатах которых незамедлительно уведомляет директора.

4.2. Работники, которым стали известны факты неправомерного использования персональных данных при осуществлении профессиональной деятельности, должны незамедлительно доложить об этом директору школы.

4.3. Ответственность сотрудников и должностных лиц школы за нарушения режима обращения с персональными данными и порядок наложения взыскания:

4.3.1. Виды взысканий, применяемых к сотрудникам и должностным лицам, нарушившим режим обращения с персональными данными:

- предупреждение;

- выговор;

- увольнение с работы;

4.3.2. Взыскание на сотрудника школы налагается директором.