

Муниципальное бюджетное общеобразовательное учреждение средняя  
общеобразовательная школа № 12 имени Ивана Иосифовича Вирченко  
станции Павловской

Введено в действие приказом  
от 31 августа 2020 года № 127  
Директор МБОУ СОШ № 12  
им. И.И.Вирченко ст. Павловской  
С.С.Приходько  
«31» августа 2020 года

УТВЕРЖДАЮ  
Директор МБОУ СОШ № 12  
им. И.И.Вирченко ст. Павловской  
С.С.Приходько  
«31» августа 2020 года

**Перечень мер,  
направленных на исключение несанкционированного доступа и  
обеспечивающих сохранность персональных данных**

**1. Общие положения**

1.1. Настоящий Перечень мер, направленных на исключение несанкционированного доступа и обеспечивающих сохранность персональных данных (далее - Перечень мер) МБОУ СОШ № 12 им. И.И.Вирченко ст. Павловской далее - образовательная организация) 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 образовательной организации процедур, позволяющих:

- исключить возможность несанкционированного доступа к персональным данным и их использования работниками образовательной организации и третьими лицами в собственных интересах в ущерб интересам граждан.

**2. Термины и определения**

В настоящем Перечне мер применяются следующие термины и определения:

2.1. Персональные данные (ПД) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.2. Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

2.3. Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и



технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без наличия таких средств.

2.4. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.5. Применяемые в Перечне мер понятия и определения, не приведенные в настоящем разделе, используются в соответствии с понятиями и определениями, содержащимися в законодательстве Российской Федерации.

### **3. Общие положения о персональных данных и порядке их использования**

3.1. Персональные данные могут быть представлены в различном виде, в том числе в бумажном или электронном.

3.2. Персональные данные могут передаваться только тем лицам, которым они необходимы для исполнения ими своих прямых должностных обязанностей.

3.3. Сотрудники образовательной организации, осуществляющие проведение, обработку и учет персональных данных не имеют права передавать данную информацию третьим лицам и работникам образовательной организации, режим доступа которых не предусматривает возможности обладания такой информацией, либо использовать ее в личных целях.

3.4. За использование и разглашение персональных данных, сотрудник образовательной организации несет персональную ответственность в соответствии с должностной инструкцией и действующим законодательством РФ.

### **4. Основные меры, препятствующие несанкционированному использованию персональных данных**

4.1. Под мерами, 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 образовательной организации.

4.2. В образовательной организации 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 образовательной организации требований законодательства РФ и иных нормативных правовых актов.

4.3. В целях противодействия несанкционированному использованию персональных данных, предотвращения утечки и обеспечения сохранности персональных данных, образовательная организация использует следующий



комплекс мероприятий.

4.3.1. 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;
- осуществление административных и технических мер, направленных на исключение несанкционированного доступа к данным: блокирование доступа пользователя в систему, в случае обнаружения попыток несанкционированного доступа, установка программных средств, оповещающих ответственного за организацию работы по обеспечению защиты информации о попытке несанкционированного доступа, блокировка рабочего места нарушителя;
- контроль за соблюдением режима обращения персональных данных осуществляется ответственным за организацию работы по обеспечению защиты информации, а так же директором образовательной организации.

4.3.2. 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:

4.3.3. Ограничение доступа посторонних лиц в помещении образовательной организации, предназначенные 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 в образовательной организации, утвержденном директором;
- ограничением доступа работников и посторонних лиц в помещение, в котором размещены персональные компьютеры, вычислительные системы и системы телекоммуникации для осуществления операций с ПД.

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

- защита окон в служебных помещениях от внешне дистанционного наблюдения жалюзи и шторами;
- эффективное размещение рабочих мест сотрудников для исключения возможности несанкционированного просмотра документов и информации на мониторах;
- соблюдение сотрудниками подразделений правил по обеспечению защиты информации при работе с персональными компьютерами.

4.3.5. Ограничение доступа к персональным данным:

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



- проведение инвентаризации мест хранения документов, содержащих персональные данные;
  - контроль за соблюдением утвержденных внутренних регламентов.
- 4.3.6. При оформлении на работу в образовательной организации, работник дает расписку о неразглашении персональных данных.
- 4.3.7. Контроль за соблюдением работниками образовательной организации требований законодательства РФ и иных нормативных правовых актов, регулирующих работу с ПД, внутренними документами образовательной организации, возложен на директора.

## **5. Осуществление процедур, препятствующих несанкционированному использованию персональных данных и контроля за их исполнением**

- 5.1. Проведение процедур, препятствующих несанкционированному использованию персональных данных и осуществление контроля включают в себя:
- 5.1.1. Установление требований о неразглашении персональных данных.
- 5.1.2. Контроль за выполнением работниками образовательной организации требований действующего законодательства РФ и внутренних документов образовательной организации.
- 5.1.3. Уведомление работников образовательной организации, имеющих доступ к информации о ПД, о недопустимости осуществления операций с ПД как в своих интересах, так и в интересах третьих лиц.
- 5.1.4. Проведение оперативных проверок на предмет возможной утечки персональных данных в случаях, предполагающих несанкционированное использование персональных данных.
- 5.1.5. Направление сведений директору образовательной организации об установленных (обнаруженных) случаях несанкционированного использования персональных данных.

## **6. Ответственность**

- 6.1. Ответственный за организацию работы по обеспечению защиты информации отвечает за:
- осуществление контроля исполнения положений нормативных документов по вопросам организации и эффективного функционирования системы внутреннего контроля образовательной организации;
  - контроль исполнения внутренних нормативных документов по вопросам обеспечения конфиденциальности персональных данных в образовательной организации;
  - проведение служебных расследований по фактам возможного неправомерного использования работниками образовательной организации персональных данных, о результатах которых незамедлительно уведомляет директора.
- 6.2. Работники образовательной организации, которым стали известны факты неправомерного использования персональных данных при осуществлении профессиональной деятельности, должны незамедлительно доложить об этом директору.

6.3. Ответственность сотрудников и должностных лиц образовательной организации за нарушения режима обращения с персональными данными и порядок наложения взыскания:

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

- предупреждение;
- выговор;
- увольнение с работы.

6.3.2. Взыскание на сотрудника образовательной организации налагается директором.

## **7. Места хранения персональных данных**

7.1. Для исключения несанкционированного доступа к ПД в образовательной организации приказом директора определяются места хранения персональных данных (материальных носителей) в отношении каждой категории персональных данных и устанавливается перечень лиц, осуществляющих обработку персональных данных.

7.2. Ответственный за организацию работы по обеспечению защиты информации осуществляет ознакомление сотрудников образовательной организации с настоящим Перечнем мер не позднее одного месяца со дня его вступления в силу. Факт ознакомления подтверждается подписью сотрудника.

7.3. Ответственный за организацию работы по обеспечению защиты информации, в случае принятия в штат образовательной организации нового сотрудника, осуществляет ознакомление с настоящим Перечнем мер не позднее одной недели со дня его зачисления в штат.

7.4. Работники образовательной организации должны предпринимать все необходимые меры, позволяющие предотвратить неправомерное распространение и использование персональных данных при проведении операции, связанных с осуществлением профессиональных видов деятельности.