МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
«СВЕРДЛОВСКИЙ ЦЕНТР ОБРАЗОВАНИЯ»

Принято
на заседании
педагогического совета
Протокол № 1 от 29.08.2022 г.

Утверждено
приказом директора
МОУ «СОШ «Свердловский ЦО»
№ 187-ОД от 31.08.2022 г.

Подписано цифровой
подписью: Медведева Т.В.
Дата: 2022.09.13 20:32:25 +03'00'

Инструкция по обеспечению безопасности обработки персональных данных в МОУ «СОШ «Свердловский ЦО»

2022 г.

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с требованиями ст. 19 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», на основании Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», письма Федерального агентства по образованию № ФАО- 6748/52/17-02-09/72 «Об обеспечении безопасности персональных данных», внутренних документов, определяющих политику МОУ «СОШ «Свердловский ЦО» (далее - Учреждение) в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

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. В целях обеспечения безопасности персональных данных создается система зашиты персональных данных, которая должна обеспечивать конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных во всех структурных элементах, на технологических участках обработки и во всех режимах функционирования информационной системы.

1.4. Система зашиты персональных данных включает в себя организационные и технические меры, средства зашиты информации. средства предотвращения несанкционированного доступа. утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в информационных системах персональных данных информационные технологии.

1.5. 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.

1.6. Помещения, в которых размещены объекты информатизации, содержащие информационные системы персональных данных должны соответствовать требованиям по обеспечению их сохранности, пожарной безопасности, а также защиты от несанкционированного проникновения посторонних лиц

1.7. Ответственность за безопасность персональных данных возлагается на лиц, допущенных к их обработке.

2. Организация работ по обеспечению безопасности персональных данных при их обработке с использованием средств

2.1. Обеспечение безопасности перед началом обработки персональных данных

2.1.1 К обработке персональных данных допускаются сотрудники, которые ознакомились с документами, определяющими политику Учреждения в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений прошедшие или которые прошли обучение.

2.1.2. Перед началом обработки персональных данных необходимо обеспечить:

- соответствие средств защиты персональных данных классу информационной системы;
- отсутствие посторонних лиц в помещении, в котором ведется работа с персональными данными;
- сохранность и целостность носителей персональных данных;
- отсутствие возможности несанкционированного доступа к персональным данным;
- исправное состояние технических средств автоматизированной обработки и защиты персональных данных;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.2. Обеспечение безопасности во время обработки персональных данных

2.2.1. 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;

- работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных;
- конфиденциальность персональных данных.

2.3. Обеспечение безопасности в экстремальных ситуациях

2.3.1. При модификации или уничтожения персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.

2.3.2. При нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление.

2.3.3. При обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.

2.3.4. 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.

2.3.5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность директора образовательного учреждения и произвести разбирательство.

2.4. Обеспечение безопасности при завершении обработки персональных данных

2.4.1. После завершения сеанса обработки персональных данных необходимо обеспечить:

- корректное закрытие программ и приложений;
- сохранность и целостность всех носителей персональных данных;
- выключение средств автоматизации.

3. Контроль обеспечения безопасности персональных данных

3.1. Целью контроля является соблюдение пользователями информационных системах персональных данных требований по обеспечению безопасности персональных данных при их обработке.

3.2. Задачами контроля являются:

- установление фактического положения дел в Учреждении по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- выявление проблемных вопросов в организации обеспечения безопасности персональных данных;
- обеспечение соблюдения законодательства российской Федерации в сфере персональных данных;
- выработка мер по оказанию методической и практической помощи;
- повышение ответственности пользователей за выполнение возложенных задач, соблюдение законности в их деятельности.

3.3. Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах Учреждения оценивается не реже одного раза в три года.

4. Заключительные положения

4.1. Проверка и пересмотр настоящей инструкции осуществляются в следующих случаях:

- при изменении законодательства Российской Федерации в области персональных данных и пересмотре отраслевых требований обеспечения безопасности персональных данных;
- при внедрении новой техники и (или) технологий;
- по результатам анализа материалов расследования нарушений требований законодательства по обеспечению безопасности персональных данных;
- по требованию представителей органов исполнительной власти, осуществляющих контроль 9надзор) в установленной сфере.

4.1. Ответственность за своевременную корректировку настоящей инструкции возлагается на лицо, назначенное ответственным за организацию обработки персональных данных в Учреждении.