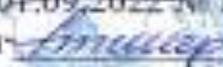


УТВЕРЖДАЮ
Приказ от 04.09.2022 № 227
Директор школы  Т.А. Пыкина



**Политика
в отношении обработки персональных данных
в МБОУ «Цинская СОШ №1»**

Обозначения и сокращения

ИСПДн – информационная система персональных данных.

НСД – несанкционированный доступ.

ПДн – персональные данные.

Политика – политика образовательном учреждении в отношении обработки персональных данных.

СЗИДн – система защиты персональных данных.

ТЗКИ – техническая защита конфиденциальной информации.

ТС – техническое средство.

Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность информации – состояние защищенности информации, характеризуемое способностью технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. **Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Накопитель информации – устройство, предназначенное для записи и (или) чтения информации на носитель информации. Накопитель информации конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначен для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке (в том числе техническими средствами) в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

Носитель информации – физический объект, предназначенный для хранения информации.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – МБОУ «Цнинская СОШ № 1», осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Система защиты персональных данных – комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПДн.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенноцифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Информация об операторе

Полное наименование Муниципальное бюджетное общеобразовательное учреждение «Цнинская общеобразовательная школа №1» (далее по тексту – образовательное учреждение).

Сокращенное наименование МБОУ «Цнинская СОШ №1».

Директор МБОУ «Цнинская СОШ №1» Пыкина Татьяна Александровна

Адрес местонахождения: 392525, Тамбовская область, Тамбовский район, поселок Строитель, микрорайон Северный, дом 19.

Почтовый адрес 392525, Тамбовская область, Тамбовский район, поселок Строитель, микрорайон Северный, дом 19.

Телефон 8(4752) 77-75-32

Е-mail sosh-cninskay-1@r00.tambov.gov.ru

Сайт <https://sh1-stroitel-r68.gosweb.gosuslugi.ru>

1. Основные положения

1.1. Настоящая Политика разработана в соответствии с положениями Конституции РФ, Трудового кодекса РФ от 30.12.2001 № 197-ФЗ, Гражданского кодекса РФ от 30.11.1994 № 51-ФЗ, Налогового кодекса РФ часть первая от 31.07.1998 № 146-ФЗ и часть вторая от 05.08.2000 № 117-ФЗ, Федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 27.07.2006 № 149-ФЗ "Об информации,

информационных технологиях и о защите информации" и иных нормативно-правовых актов, регулирующих вопросы защиты персональных данных.

1.2. Требования настоящей Политики распространяются на защиту информации с ограниченным доступом, отнесенной к информации, составляющей ПДн.

1.3. Персональные данные являются конфиденциальной, охраняемой информацией и на них распространяются все требования, установленные внутренними документами образовательного учреждения к защите конфиденциальной информации.

1.4. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПДн образовательных учреждений, а также нормативных и методических документов, обеспечивающих ее реализацию.

1.5. Политика определяет следующие основные вопросы защиты информации:

- основные принципы и требования по защите информации, составляющей ПДн,
- порядок организации и проведения работ по защите информации,
- порядок обеспечения защиты информации при эксплуатации ИСПДн,
- порядок организации делопроизводства, хранения и обращения накопителей и носителей информации.

1.6. Является общедоступным документом, декларирующим концептуальные основы деятельности оператора при обработке персональных данных.

2. Принципы обеспечения защиты информации, составляющей персональные данные

Защита информации, составляющей ПДн должна осуществляться в соответствии со следующими основными принципами:

2.1. Законность — предполагает обеспечение защиты ПДн в соответствии с действующим в РФ законодательством и нормативными актами в области защиты ПДн.

Пользователи и обслуживающий персонал ИСПДн должны быть осведомлены о правилах и порядке работы с защищаемой информацией и об ответственности за их нарушение.

2.2. Системность — предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн.

2.3. Комплексность — предполагает согласованное применение разнородных средств и систем при построении комплексной системы защиты информации, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей.

Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

2.4. Непрерывность — предполагает функционирование СЗПДн в виде непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны

находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры не допускающие переход ИСПДн в незащищенное состояние.

2.5.Своевременность — предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

2.6.Совершенствование — предполагает постоянное совершенствование мер и средств защиты информации на основе комплексного применения организационных и технических решений, квалификации персонала, анализа функционирования ИСПДн и ее системы защиты с учетом изменений условий функционирования ИСПДн, появления новых методов и средств перехвата информации, изменений требований нормативных документов по защите ПДн.

2.7.Персональная ответственность — предполагает возложение ответственности за обеспечение безопасности ПДн и ИСПДн на каждого исполнителя в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей исполнителей строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

2.8.Минимальная достаточность — предполагает предоставление исполнителям минимально необходимых прав доступа к ресурсам ИСПДн в соответствии с производственной необходимостью, на основе принципа «запрещено все, что не разрешено явным образом».

2.9.Гибкость системы защиты — предполагает наличие возможности варьирования уровнем защищенности при изменении условий функционирования ИСПДн.

2.10.Обязательность контроля — предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации. Контроль за деятельностью каждого пользователя, каждого средства защиты и в отношении каждого объекта защиты должен осуществляться на основе применения средств контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

3. Основные требования по защите информации составляющей персональные данные

3.1.Защита информации в ИСПДн является неотъемлемой составной частью управленческой и научной деятельности образовательного учреждения и должна осуществляться во взаимосвязи с другими мерами по защите информации, составляющей ПДн.

3.2.Защита информации является составной частью работ по созданию и эксплуатации ИСПДн и должна осуществляться в установленном настоящей Политикой порядке и реализовываться в виде системы (подсистемы) защиты ПДн.

3.3.Защита информации должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счет НСД к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее санкционированной доступности и работоспособности ТС.

3.4.В ИСПДн должны использоваться сертифицированные по требованиям безопасности информации средства защиты информации и (или) технические и организационные решения, исключаяющие утечку информации по техническим каналам, за счет НСД, предупреждающие нарушение целостности информации и ее санкционированной доступности.

3.5.Защита информации должна быть дифференцированной в зависимости от применяемых технических средств, обрабатывающих информацию, составляющую ПДн, установленного уровня защищенности ИСПДн, установленного класса ИСПДн и утвержденной для ИСПДн модели угроз.

3.6.Все используемые в ИСПДн средства защиты информации должны быть проверены на соответствие ограничениям и условиям эксплуатации, изложенным в сертификате соответствия, эксплуатационной документации или формуляре (для технических и программных средств защиты информации соответственно).

3.7.Обработка информации составляющей ПДн осуществляется на основании письменного разрешения (приказа) руководителя образовательного учреждения, в котором эксплуатируется ИСПДн.

3.8.Ответственность за обеспечение выполнения установленных требований по защите информации возлагается на руководителя образовательного учреждения, в котором создается (совершенствуется) и эксплуатируется ИСПДн.

3.9.Все ИСПДн должны пройти оценку эффективности принимаемых мер по обеспечению безопасности ПДн до начала обработки информации составляющей ПДн.

4. Сведения об обеспечении безопасности персональных данных

4.1. Безопасность персональных данных достигается путем обеспечения их конфиденциальности, целостности и доступности.

4.2. В образовательном учреждении функционирует комплексная система защиты персональных данных, которая включает:

4.2.1. Организационные мероприятия:

- действующие организационно-распорядительные документы по защите ПДн, регламентирующие порядок обработки ПДн и ответственность должностных лиц;
- осуществление внутреннего периодического контроля;
- учет машинных носителей персональных данных;
- физическая охрана здания и помещений;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- обучение сотрудников вопросам защиты ПДн.

4.2.2. Технические меры защиты:

- подсистема парольной защиты;
- подсистема антивирусной защиты;
- сейфы и запирающиеся шкафы для хранения носителей персональных данных;
- пожарная сигнализация.

5. Доступ к ПДн

5.1. Сотрудники Оператора, которые в силу выполняемых служебных (трудовых) обязанностей постоянно работают с ПДн, получают доступ к необходимым категориям ПДн на срок выполнения ими соответствующих должностных

обязанностей на основании перечня лиц, допущенных к работе с ПДн, который утверждается директором Оператора.

5.2. Список лиц, имеющих доступ к ПДн для информационной системы, должен поддерживаться в актуальном состоянии.

5.3. Оператором установлен разрешительный порядок доступа к ПДн. Сотрудникам Оператора предоставляется доступ к работе с ПДн в пределах и объеме, необходимых для выполнения ими для выполнения служебных (трудовых) обязанностей.

5.4. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником Оператора по согласованию директора.

5.5. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с разрешения директора.

5.6. В случае если сотруднику сторонней организации необходим доступ к ПДн Оператора, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Оператора, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором с субъектом ПД.

5.7. Доступ сотрудника Оператора к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

6. Обработка персональных данных

6.1. При обработке персональных данных в образовательном учреждении соблюдаются конституционные права и свободы человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну.

6.2. Образовательное учреждение не вправе обрабатывать персональные данные субъектов ПДн об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

6.3. Источники получения персональных данных:

6.3.1. субъект ПДн;

6.3.2. законный представитель субъекта;

6.4. При наличии законных оснований получателем персональных данных субъекта могут являться:

- 6.4.1. налоговые органы;
- 6.4.2. Пенсионный Фонд РФ;
- 6.4.3. Фонд социального страхования РФ;
- 6.4.4. Федеральная служба государственной статистики РФ;
- 6.4.5. Фонд обязательного медицинского страхования РФ;
- 6.4.6. правоохранительные органы;
- 6.4.7. банки и иные кредитные организации.
- 6.5. Персональные данные субъектов в образовательном учреждении обрабатываются как на бумажных носителях, так и в электронном виде – в компьютерных программах и электронных базах данных (в ИСПДн) без передачи по незащищенным техническим каналам связи.
- 6.6. Обработка персональных данных по общему правилу происходит до утраты правовых оснований.
- 6.7. Срок хранения документов, содержащих персональные данные, определяется "Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения", утвержденный Приказом Министерства культуры РФ от 25.08.2010 № 558 и в иных случаях, предусмотренных законодательством РФ.
- 6.8. Трансграничная передача персональных данных не осуществляется.
- 6.9. Лицо, ответственное за организацию обработки ПДн в образовательном учреждении директор Пыкина Т.А.
- 6.10. Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- 6.11. Целями обработки персональных данных являются:
- организация кадрового учета, ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, исполнение налогового законодательства РФ в связи с исчислением и уплатой НДФЛ, а также пенсионного законодательства РФ при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнение первичной статистической документации;
 - заключение, исполнение и прекращение гражданско-правовых договоров;
 - защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;
 - в иных законных целях.
- 6.12. Обработка персональных данных в образовательном учреждении допускается в случаях:
- если обработка персональных данных осуществляется с согласия субъекта персональных данных;
 - если обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
 - если обработка персональных данных необходима для осуществления прав и законных интересов образовательного учреждения или третьих лиц, либо для

достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- если обработка персональных данных необходима для осуществления научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- если осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных, либо по его просьбе;

- если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законом.

7. Порядок организации и проведения работ по защите информации

7.1. Организация работ по защите информации возлагается на директора образовательного учреждения, который принимает решение по модернизации и/или эксплуатацию ИСПДн.

7.2. Организация и проведение работ по защите информации, составляющей ПДн на различных стадиях разработки, внедрения и эксплуатации ИСПДн определяется действующими в РФ нормативными документами и настоящим документом.

7.3. Проведение работ по защите информации, составляющей ПДн, осуществляется силами образовательного учреждения, в котором создается (совершенствуется) ИСПДн. В случае невозможности или нецелесообразности выполнения работ по защите информации силами образовательного учреждения к этим работам должна привлекаться специализированная организация, имеющая соответствующие лицензии на право выполнения работ и оказания услуг по ТЗКИ.

8. Порядок обеспечения защиты информации при эксплуатации ИСПДн

8.1. Эксплуатация ИСПДн должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией ИСПДн.

8.2. Ответственность за обеспечение защиты информации в процессе эксплуатации ИСПДн возлагается на руководителя образовательного учреждения, в ведении которого находится эта ИСПДн.

8.3. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИСПДн возлагается на непосредственных исполнителей ИСПДн (пользователей, администраторов, обслуживающий персонал).

8.4. За нарушение установленных требований по защите информации руководитель образовательного учреждения, в ведении которого находится ИСПДн и (или) непосредственный исполнитель привлекаются к ответственности в соответствии с действующим в РФ законодательством.

9. Порядок организации делопроизводства, хранения и обращения накопителей и носителей информации

9.1. Все накопители и носители информации содержащие ПДн на бумажной, магнитной, магнито-оптической и иной основе, используемые в технологическом процессе обработки информации в ИСПДн, подлежат учету, хранению и обращению в соответствии с требованиями конфиденциального делопроизводства.

9.2. Организация и ведение учета накопителей и носителей ПДн, организация их хранения, обращения и уничтожения осуществляются ответственными делопроизводителями конфиденциального делопроизводства.

9.3. ПДн, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

9.4. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

9.5. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

9.6. Обработка ПДн без использования средств автоматизации должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

9.7. Должно обеспечиваться раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

9.8. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

10. Контроль состояния и эффективности защиты ИСПДн

10.1. В ИСПДн должен осуществляться контроль и (или) аудит соответствия обработки ПДн действующим в РФ законодательству и требованиям к защите ПДн, а так же настоящей Политике и локальным актам образовательного учреждения.

10.2. Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению ПДн.

10.3. Контроль подразделяется на оперативный и плановый (периодический).

10.4. В процессе эксплуатации ИСПДн в целях защиты информации от НСД осуществляются оперативный контроль и периодический контроль за выполнением исполнителями требований действующих нормативных документов по вопросам обеспечения безопасности и защиты ПДн.

10.5. С целью своевременного выявления и предотвращения утечки информации, исключения или существенного затруднения НСД и предотвращения специальных воздействий (программно-технических и др.), вызывающих нарушение целостности информации или работоспособность технических средств, в ИСПДн образовательных учреждений проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

10.6. При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности ИСПДн от утечки ПДн по техническим каналам, выборочный контроль содержимого накопителей и носителей информации, и т.п.

10.7. Результаты контроля оформляются актами, заключениями и записями в эксплуатационной документации.