**Муниципальное казенное учреждение дополнительного образования**

**«Районная станция юных техников»**

**Чегемского муниципального района КБР**

**Принят** на общем собрании **Утверждена**

трудового коллектива Директор МКУ ДО «РСЮТ»

Протокол № \_\_\_

от «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2015 г  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**М.З.Кяров

Приказ № от «\_\_\_»\_\_\_\_\_\_\_2015 г.

в отношении обработки персональных данных

 МКУ ДО «РСЮТ»

г.п.Чегем

2015 г.

**Содержание**

|  |  |
| --- | --- |
| Обозначения и сокращения.………………………………………………… | 2 |
| Термины и определения…………………………………………………….. | 2 |
| 1. Основные положения……………………………………………………... | 9 |
| 2. Принципы обеспечения защиты информации, составляющей персональные данные ……………………………………………………. | 10 |
| 3. Основные требования по защите информации составляющей персональные данные……………………….............................................. | 13 |
| 4. Порядок организации и проведения работ по защите информации...…... | 15 |
| 5. Порядок обеспечения защиты информации при эксплуатации ИСПДн... | 16 |
| 6. Порядок организации делопроизводства, хранения и обращения накопителей и носителей информации……………………………………. | 17 |
| 7. Контроль состояния и эффективности защиты ИСПДн…………………. | 19 |

**Обозначения  и  сокращения**

**ИСПДн**–  информационная система персональных данных.

**НСД –**несанкционированный доступ.

**ПДн** – персональные данные.

**Политика**– политика образовательных учреждений в отношении обработки персональных данных.

**СЗПДн**– 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 предназначению 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** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие 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 буквенно-цифровой 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.

# ****1.**   **Основные  положения****

**1.1.            Настоящая  Политика устанавливает** **порядок организации и проведения работ по** **защите информации в ИСПДн, создаваемых  и** **эксплуатируемых в образовательном учреждении.**

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

**1.3.    Политика  является дополнением к действующим в РФ нормативным документам по вопросам  обеспечения информационной безопасности ПДн, и не исключает обязательного  выполнения их требований.**

**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.**

# **2.   П**ринципы 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 неразрешено 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 правило 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****

* 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.
  2. Защита информации является составной частью работ по созданию и эксплуатации ИСПДн и осуществляется в установленном настоящей Политикой порядке и реализовывается в виде системы (подсистемы) защиты ПДн.
  3. Защита информации осуществляется 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.
  4. В ИСПДн должны использоваться сертифицированные по требованиям безопасности информации средства защиты информации и (или) технические и организационные решения, исключающие утечку информации по техническим каналам, за счет НСД, предупреждающие нарушение целостности информации и ее санкционированной доступности.
  5. Защита информации дифференцирована в зависимости от применяемых технических средств, обрабатывающих информацию, составляющую ПДн, установленного класса ИСПДн и утвержденной для ИСПДн модели угроз.
  6. Все используемые в ИСПДн средства защиты информации проверены на соответствие ограничениям и условиям эксплуатации, изложенным в сертификате соответствия, эксплуатационной документации или формуляре (для технических и программных средств защиты информации соответственно).
  7. Обработка информации составляющей ПДн осуществляется на основании письменного разрешения (приказа) руководителя образовательного учреждения, в котором эксплуатируется ИСПДн.
  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.

# Порядок организации и проведения работ по защите информации

* 1. Организация работ по защите информации возлагается на руководителя образовательного учреждения, осуществляющего разработку (модернизацию) и эксплуатацию ИСПДн.
  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.
  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.
  4. Стадии создания системы защиты информации:
* Пред проектная стадия — включает пред проектное обследование создаваемой ИСПДн, разработку аналитического обоснования необходимости создания системы защиты информации и технического задания на ее создание.
* Стадия проектирования (разработки проектов) и реализации ИСПДн — включает разработку СЗПДн в составе ИСПДн.
* Стадия ввода в действие системы СЗПДн — включает опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку эффективности принимаемых мер по обеспечению безопасности ПДн.

# Порядок обеспечения защиты информации при эксплуатации ИСПДн

* 1. Эксплуатация ИСПДн должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией ИСПДн.
  2. Ответственность за обеспечение защиты информации в процессе эксплуатации ИСПДн возлагается на руководителя образовательного учреждения, в ведении которого находится эта ИСПДн.
  3. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИСПДн возлагается на непосредственных исполнителей ИСПДн (пользователей, администраторов, обслуживающий персонал).
  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.