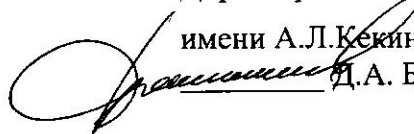


УТВЕРЖДАЮ:

Директор МОУ гимназии  
имени А.Л. Кекина г. Ростова  
Д.А. Бражников



« 7 » сент. 2015 год

## ПОЛИТИКА

муниципального образовательного учреждения

гимназии имени А.Л. Кекина г. Ростова

в отношении обработки персональных данных

### Содержание

1. Основные положения
2. Принципы обеспечения защиты информации, составляющей персональные данные
3. Основные требования по защите информации составляющей персональные данные
4. Порядок организации и проведения работ по защите информации
5. Порядок обеспечения защиты информации при эксплуатации ИСПДн
6. Порядок организации делопроизводства, хранения и обращения накопителей и носителей информации
7. Контроль состояния и эффективности защиты ИСПДн

### 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 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** – 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.

## **Основные положения**

Настоящая Политика устанавливает порядок организации и проведения работ по защите информации в ИСПДн, создаваемых и эксплуатируемых в МОУ гимназия имени А.Л. Кекина г.Ростова(далее Гимназия ).

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

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

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

## **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.

## **Принципы обеспечения защиты информации, составляющей персональные данные:**

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

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

#### **Основные требования по защите информации составляющей персональные данные:**

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



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).

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

Ответственность за обеспечение выполнения установленных требований по защите информации возлагается на директора Гимназии, в котором создается (совершенствуется) и эксплуатируется ИСПДн.

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:**

- Организация работ по защите информации возлагается на директора Гимназии, осуществляющего разработку (модернизацию) и (или) эксплуатацию ИСПДн.
- 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.
- Проведение работ по защите информации, составляющей ПДн, осуществляется силами Гимназии, в которой создается (совершенствуется) ИСПДн.

#### **Стадии создания системы защиты информации:**

- Предпроектная стадия — включает предпроектное 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:**

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

## **Порядок организации делопроизводства, хранения и обращения накопителей и носителей информации:**

- 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.
- Организация и ведение учета накопителей и носителей ПДн, организация их хранения, обращения и уничтожения осуществляются ответственными делопроизводителями конфиденциального делопроизводства.
- ПДн, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).
- При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.
- Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.
- 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.
- Должно обеспечиваться раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.
- При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключаяющие несанкционированный к ним доступ.

## **Контроль состояния и эффективности защиты ИСПДн**

- 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.
- Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению ПДн.
- Контроль подразделяется на оперативный и плановый (периодический).
- 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.
- 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.
- 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.
- Результаты контроля оформляются актами, заключениями и записями в эксплуатационной документации.