|  |  |
| --- | --- |
|  | Утверждено  приказом директора МОУ СОШ № 60  №\_\_\_\_\_ от\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.Л. Саматоева |

**ПОЛИТИКА**

**МОУ СОШ № 60**

**В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧАСТНИКОВ ОБРАЗОВАТЕЛЬНЫХ ОТНОШЕНИЙ**

**г. Ярославль**

**2014 год**

**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.

**Школа** – Муниципальное образовательное учреждение средняя общеобразовательная школа № 60

**Субъект –** участник образовательных отношений

**1. Общие положения**

1.1. Настоящая Политика разработана на основании Конституции РФ, Гражданского Кодекса РФ, Трудового Кодекса РФ, и в соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящая Политика устанавливает порядок организации и проведения работ по защите информации в ИСПДн, создаваемых и эксплуатируемых в Школе.

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

1.4. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПДн Школы, 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. Настоящая политика утверждается директором Школы и является обязательной для исполнения всеми сотрудниками, имеющими доступ к персональным данным Субъекта.

**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 ответст-

венности 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. 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.

2.4. 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.

2.5. Совершенствование - предполагает постоянное совершенствование мер и средств защиты информации.

2.6. Персональная ответственность - предполагает возложение ответственности за обеспечение безопасности ПДн и ИСПДн на каждого исполнителя в пределах его полномочий.

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

2.8. Обязательность контроля - предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации.

**3. Основные требования по защите информации, составляющей персональные данные**

3.1. Защита информации в ИСПДн является неотъемлемой составной частью деятельности Школы 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 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, исключающие 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. Обработка информации, составляющей ПДн, осуществляется на основании письменного разрешения (приказа или иного документа) директора Школы.

3.7. Ответственность за обеспечение выполнения установленных требо-

ваний по защите информации возлагается на директора Школы.

3.8. Все ИСПДн должны пройти оценку эффективности принимаемых

мер по обеспечению безопасности ПДн до начала обработки информации составляющей ПДн.

**4. Порядок организации и проведения работ по защите информации**

4.1. Организация работ по защите информации возлагается на директора Школы.

4.2. 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.

4.3. В случае невозможности или нецелесообразности выполнения работ по защите информации силами Школы к этим работам должна привлекаться специализированная организация, имеющая соответствующие лицензии на право выполнения работ и оказания услуг по ТЗКИ.

4.4. Стадии создания системы защиты информации:

* Предпроектная стадия включает предпроектное обследование создаваемой ИСПДн.
* 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.

**5. Порядок обеспечения защиты информации при эксплуатации ИСПДн**

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

5.2. Ответственность за обеспечение защиты информации в процессе эксплуатации ИСПДн возлагается на директора Школы.

5.3. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИСПДн возлагается на непосредственных исполнителей ИСПДн.

5.4. За нарушение установленных требований по защите информации ди-

ректор Школы, и (или) непосредственный исполнитель привлекаются к ответственности в соответствии с действующим в РФ законодательством.

**6. Порядок организации делопроизводства, хранения и обращения накопителей и носителей информации**

6.1. 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.

6.2. Организация и ведение учета накопителей и носителей ПДн, организация их хранения, обращения и уничтожения осуществляются ответственными за данный участок работы.

6.3. ПДн, должны обособляться от иной информации.

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

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

6.6. 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.

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

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

**7. Контроль состояния и эффективности защиты ИСПДн**

7.1. В ИСПДн должен осуществляться контроль соответст-

вия обработки ПДн действующим в РФ законодательству и требованиям к защите ПДн, а так же настоящей Политике и локальным актам Школы.

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

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

7.4. Контроль осуществляется 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.

7.5. 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.

7.6. Результаты контроля оформляются актами или заключениями.