Утверждаю:

Заведующий МБДОУ ДС №1

_____ Т.А. Кирсанова

«15» 01 2018 г

Политика
в отношении обработки персональных данных и сведений о реализуемых требованиях к защите персональных данных в МБДОУ ДС №1

1. Общие положения.

1.1. В целях обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных МБДОУ ДС №1, в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ, определяется политика в области обеспечения безопасности персональных данных, содержащая основные правила и порядок обработки персональных данных граждан.

1.2. Политика заключается в выполнении требований и норм обработки персональных данных, установленных в Постановлении Правительства Российской Федерации от 1 ноября 2012 года № 1119.

2. Лица, ответственные за обеспечение безопасности персональных данных

2.1. Заведующий МБДОУ ДС №1:

2.1.1. Является ответственным за организацию работ по обеспечению безопасности персональных данных, на которого возлагается:

- утверждение списка лиц, доступ которых к персональным данным, необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;
- принятие решения о распространении (передаче) персональных данных;
- проведение разбирательств по фактам 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;
- приостановка предоставления персональных данных пользователям информационной системы при обнаружении нарушений порядка предоставления персональных данных;
- руководство работами по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.

2.1.2. Назначает ответственного пользователя криптосредств.

2.1.3. На ответственного пользователя криптосредств возлагается:

- организация парольной защиты;

• организация учета средств защиты информации, эксплуатационной и технической документации к ним;

• администрирование средств и систем защиты персональных данных в информационной системе персональных данных, включая средства антивирусной защиты (за исключением средств криптографической защиты информации);

• учет лиц, допущенных к работе с персональными данными в информационной системе;

• учет носителей персональных данных, используемых в информационной системе персональных данных (как с использованием средств автоматизации, так и без их использования);

• периодическая (не реже одного раза в квартал) проверка электронного журнала обращений пользователей информационной системы к персональным данным;

• инструктаж пользователей информационной системе персональных данных о порядке и правилах использования средств защиты информации, включая средства антивирусной защиты;

• контроль за соблюдением условий использования средств защиты информации (за исключением средств криптографической защиты информации).

3. Организация резервирования и восстановления программного обеспечения, баз персональных данных информационной системе персональных данных

3.1. В информационной системе персональных данных резервированию подлежат:

• базы персональных данных;

• специальное программное обеспечение;

• средства защиты информации;

• общее программное обеспечение;

• средства вычислительной техники;

• средства обеспечения функционирования информационных систем.

3.2. Резервные носители персональных данных хранятся в подразделении, эксплуатирующем ИСПДн.

3.3. Резервные носители персональных данных не могут быть переданы за пределы подразделения, эксплуатирующего ИСПДн.

3.4. Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, ***запрещается***.

3.5. Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения машинных носителей дистрибутивов данных программ и машинных носителей обновлений к ним в подразделениях, отвечающих за их установку, настройку и сопровождение.

3.6. Машинные носители обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны быть маркированы датой их получения (датой выхода обновления).

3.7. В случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения осуществляется обязательное восстановление работоспособности ИСПДн.

4. Учет лиц, допущенных к работе с персональными данными в информационной системе персональных данных

4.1. Лица, допущенные к работе с персональными данными в информационной системе персональных данных МБДОУ ДС №1 утверждаются приказом заведующего МБДОУ ДС №1.

4.2. Основанием для допуска сотрудника к персональным данным, обрабатываемым в информационной системе персональных данных, является необходимость обработки персональных данных в связи с выполнением должностных обязанностей, а также соответствующий приказ, утвержденный заведующим МБДОУ ДС №1.

4.3. Основанием для прекращения допуска сотрудника к персональным данным, обрабатываемым в информационной системе персональных данных, может служить приказ об его увольнении (переводе на другую должность, не требующую работы с персональными данными).

5. Организация парольной защиты в информационной системе персональных данных

5.1. Защите паролем подлежит доступ к:

- базовым системам ввода вывода компьютеров;
- настройкам сетевого оборудования;
- настройкам операционных систем;
- настройкам средств защиты информации (в том числе средств антивирусной защиты);
- запуску специализированного программного обеспечения, предназначенного для обработки персональных данных;
- ресурсам АРМ и баз данных ИСПДн.

5.2. Базовые системы ввода вывода, сетевое оборудование, операционные системы, средства защиты информации и файловые массивы (далее – объекты парольной защиты) должны быть настроены таким образом, чтобы:

- исключить возможность просмотра ранее вводимых паролей;
- блокировать доступ пользователей после пятикратной ошибки при вводе пароля и сигнализировать о наступлении данного события.

5.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями

возлагается на сотрудников отдела инженерно-технического обеспечения МБДОУ ДС №1.

5.4. Пользователь обязан запомнить личные пароли и никому их не передавать, и не записывать их на местах, где их могут увидеть другие лица.

5.5. Информация о паролях пользователей является информацией ограниченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к ресурсам ИСПДн согласно разрешительной системы доступа.

5.6. **ЗАПРЕЩАЕТСЯ:**

- умышленное и неумышленное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;
- передача личного пароля сослуживцам или посторонним лицам;
- запись личного пароля на бумагу и хранение его в потенциально доступном для ознакомления посторонними лицами и другими сотрудниками месте;
- вход в систему с использованием чужих идентификаторов или паролей;
- оставление без присмотра рабочего места при работе в ИСПДн.

5.7. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.8. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора.

6. Антивирусная защита в информационной системе персональных данных

6.1. К использованию в ИСПДн допускаются только лицензионные и сертифицированные по требованиям безопасности информации антивирусные средства.

6.2. Установка и настройка средств антивирусного контроля на компьютерах осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

6.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

6.4. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в 3 месяца.

6.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения, должна быть выполнена антивирусная проверка на всех компьютерах ИСПДн.

6.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно должен провести внеочередной антивирусный контроль своего компьютера.

6.7. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на сотрудников отдела инженерно-технического обеспечения и администраторов баз данных в территориальных отделах.

6.8. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на сотрудников отдела инженерно-технического обеспечения и администраторов баз данных в территориальных отделах и всех сотрудников, являющихся пользователями ИСПДн.

6.9. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований по антивирусной защите осуществляется ответственным за организацию работ по обеспечению безопасности персональных данных при их обработке в ИСПДн.

7. Перечень персональных данных, обрабатываемых в информационной системе персональных данных и подлежащих защите

7.1. В информационной системе персональных данных защите подлежит:

- любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:
  - фамилия, имя, отчество;
  - год рождения;
  - месяц рождения;
  - дата рождения;
  - адрес;
  - образование;
  - профессия;
  - доходы;
  - фотография;
  - контактный номер;
  - сведения о документе, удостоверяющем личность;
  - реквизиты ИНН, СНИЛС, пенсионного удостоверения, расчетных счетов.

Фамилия, имя и отчество не являются информацией, позволяющей определить субъекта персональных данных.

8. Порядок предоставления персональных данных

8.1. Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц.

8.2. Персональные данные могут быть распространены только на основании решения субъекта персональных данных.

8.3. До передачи любых персональных данных за пределы организации от каждого субъекта персональных данных должно быть получено письменное согласие на распространение его персональных данных, оформленное в соответствии с требованиями статьи 9 Федерального закона «О персональных данных», в каждом конкретном случае.

8.4. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8.5. Решение на предоставление персональных данных принимается ответственным за организацию обработки персональных данных.

8.6. Персональные данные, обрабатываемые в ИСПДн, могут быть предоставлены органам власти и органам местного самоуправления без согласия субъекта персональных данных, если данные действия осуществляются в соответствии с федеральными законами Российской Федерации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом решение на распространение персональных данных должно содержать ссылку на соответствующую статью федерального закона Российской Федерации.

9. Порядок приостановки предоставления персональных данных, в случае обнаружения нарушений порядка их предоставления, и порядок разбирательств по фактам, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям.

9.1. При обнаружении нарушений порядка предоставления персональных данных предоставление персональных данных пользователям информационной системы незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

9.2. Принятие решения на приостановку обработки персональных данных принимается ответственным за организацию обработки персональных данных.

9.3. Основаниями для приостановки обработки ПДн в ИСПДн и проведения разбирательства являются:

- выявление недостоверных персональных данных в информационной системе персональных данных;
- предоставление персональных данных в нарушение установленных правил;
- допуск к ИСПДн лица, не имеющего на то разрешения;

• утрата носителя персональных данных;
• нарушение правил хранения носителей персональных данных;
• нарушение правил эксплуатации средств защиты информации;
• нарушение правил парольной защиты;
• нарушение правил антивирусной защиты;
• нарушение правил резервирования и восстановления общего и специального программного обеспечения, а также баз персональных данных;
• выявление в ИСПДн вредоносных программ (вирусов);
• выявление в электронных журналах средств защиты информации несанкционированных действий пользователей, нарушающих безопасность персональных данных или целостность (неизменность) программного обеспечения ИСПДн;
• выявление несанкционированного внесения изменений в состав технических средств и (или) программного обеспечения ИСПДн.

9.4. Разбирательство проводится структурным подразделением или должностным лицом (работником), ответственным за обеспечение безопасности персональных данных, с обязательным привлечением руководителя структурного подразделения, осуществляющего эксплуатацию ИСПДн.

9.5. В ходе разбирательства составляется заключение, в котором отражается:
• состав группы проводившей разбирательство;
• период времени, в который проводилось разбирательство;
• основание для проведения разбирательства;
• факты, выявленные в ходе разбирательства и имеющие значение в определении наличия нарушений конфиденциальности персональных данных или нарушений правил использования средств защиты информации, а также иные факты, которые могут привести к нарушению конфиденциальности персональных данных или к снижению уровня защищенности персональных данных;
• вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;
• рекомендации по совершенствованию обеспечения безопасности персональных данных, исключающие в дальнейшем подобные нарушения.

9.6. Заключение представляется ответственному за организацию обработки персональных данных, который принимает решение на возобновление обработки персональных данных и принятие дополнительных мер защиты.

10. Порядок взаимодействия по вопросам обеспечения безопасности персональных данных

10.1. Взаимодействие по вопросам обеспечения безопасности персональных данных может осуществляться с:
• организациями, оказывающими услуги по обеспечению безопасности персональных данных;

• подчиненными организациями и обособленными структурными подразделениями.

10.2. Взаимодействие с организациями, оказывающими услуги по обеспечению безопасности персональных данных, осуществляется на договорной основе. Такие организации в обязательном порядке должны иметь лицензию Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации, а в случае оказания ими услуг в области криптографической защиты информации – лицензии Федеральной службы безопасности Российской Федерации.

10.3. Существенным условием договора с организацией, оказывающей услуги по обеспечению безопасности персональных данных, является требование соблюдения конфиденциальности сведений о степени защищенности информационных систем персональных данных (внедренных методах и способах защиты и их эффективности).

10.4. Взаимодействие с подчиненными организациями и обособленными структурными подразделениями осуществляется в части методического руководства и контроля за полнотой и эффективностью принятых мер обеспечения безопасности персональных данных. Контрольные мероприятия в подчиненных организациях и обособленных структурных подразделениях осуществляются ответственным за организацию работ по обеспечению безопасности персональных данных, ответственным пользователем криптосредств (в части использования средств криптографической защиты информации) и сотрудниками службы информационного и программного обеспечения, осуществляющими работы по обеспечению безопасности персональных данных.

Политика безопасности в области защиты персональных данных

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Нормативно-правовые акты, регулирующие вопросы в области политики по защите персональных данных:

- Политика в области обеспечения безопасности персональных данных в МБДОУ ДС №1 (скачать)
- Положение о персональных данных …..(скачать)
- Положение……
- Положение….

- **Федеральный закон от** 27 июля 2006 г. N 152-ФЗ "О персональных данных" (скачать)
- **Постановление Правительства РФ** от 21 марта 2012 г. 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" (скачать)
- **Постановление Правительства РФ** от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

- **Приказ** Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (скачать).