УТВЕРЖДАЮ
Директор МБУДО «ЦДМШ»
М.Г.Даровская
Пр.№ 96-ОД от 12.04.2018 г.

ПОЛОЖЕНИЕ
О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТРАЛЬНОЙ ДЕТСКОЙ МУЗЫКАЛЬНОЙ ШКОЛЫ ГОРОДА ЮЖНО-САХАЛИНСКА»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение о мерах по организации защиты информационных систем персональных данных в МБУДО «ЦДМШ» (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Школы на протяжении всего цикла их создания и эксплуатации.

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой Школой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

2. Настоящее Положение является внутренним локальным актом МБУДО «ЦДМШ» (далее – Школа).

Настоящее Положение вступает в силу с момента его утверждения директором Школы и действует бессрочно, до замены его новым Положением.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий обработки ПДн.

Изменения к Положению утверждаются директором Школы.

3. Все работники Школы должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

Настоящее Положение является обязательным для исполнения всеми работниками Школы, имеющими доступ к персональным данным.

4. Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм Положения возлагается на назначаемого приказом по Школе уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защите персональных данных.

5. Положение разработано с учетом требований принятой в Школе Политики по защите персональных данных в МБУДО «ЦДМШ». Школа учитывает требования настоящего Положения при разработке и утверждении внутренних локальных актов и иных документов Школы, связанных с обработкой ПДн.

2. ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ.

В Положении используются следующие понятия, определения и сокращения:

ПДн - персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - субъекту персональных данных.

Обработка ПДн - любое действие с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств.

ИСПДн – информационная система персональных данных, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Обработка ПДн без использования средств автоматизации - обработка персональных данных, содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Система защиты персональных данных – СЗПДн - организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Закон «О персональных данных» - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Приказ ФСТЭК №21 - Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической и видео информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Для обеспечения защиты информации, содержащейся в информационной системе, Школой назначается работник, ответственный за защиту информации.

Система защиты персональных данных включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Выбор средств защиты информации для системы защиты персональных данных

осуществляется Школой в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

Определение типа угроз безопасности персональных данных, актуальных для информационных систем, производится Школой с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18^1 Закона «О персональных данных».

В связи с этим Школой необходимо классифицировать информационные системы в зависимости от того, какие категории персональных данных в ней обрабатываются и какие типы угроз актуальны для ИСПДн Школы. По результатам требуется определить набор требований, которые необходимо выполнить для обеспечения того уровня защищенности ПДн, который был определен при классификации ИСПДн Школы.

4. ОСНОВНЫЕ МЕРЫ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.

1. Состав и содержание организационных мер по обеспечению безопасности ПДн

Для обеспечения необходимого уровня защищенности персональных данных при их обработке в информационных системах Школы необходимо принятие следующих основных организационных мер:

а) ввести режим обеспечения безопасности помещений, в которых размещены ИСПДн Школы, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечить безусловную сохранность носителей персональных данных;

в) назначить уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защиту персональных данных;

г) утвердить перечень персональных данных и иных объектов, подлежащих защите в ИСПДн Школы;

д) утвердить перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн Школы, необходим для выполнения ими служебных обязанностей;

ж) провести классификацию ИСПД Школы, по результатам определить набор требований, которые необходимо выполнить для обеспечения необходимого уровня защищенности ПДн;

з) обеспечить использование только таких средств защиты информации, которые прошли процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

и) обеспечить проведение не реже 1 раза в 3 года проверки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и регулярный контроль за выполнением требований к защите ПДн при обработке их в ИСПДн.

1.1. Мероприятия по реализации организационных мер по обеспечению безопасности ПДн

С учетом требований, перечисленных в п.1. статьи 6. Положения, необходимо организовать и провести ниже следующие мероприятия:

1. Назначить приказом директора уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защиту персональных данных в информационных системах Школы. Разработать и ввести в действие должностную инструкцию, регламентирующие права и обязанности такого уполномоченного сотрудника.

2. Разработать, утвердить и внедрить систему организации доступа в помещения Школы, где осуществляется обработка ПДн, исключающую возможность несанкционированного доступа к техническим средствам обработки ПДн, хищения и нарушения работоспособности ИСПДн, хищения носителей информации ПДн.

3. Определить состав и категории обрабатываемых в Школе персональных данных. Результат оформить в виде локального нормативного акта с перечнем персональных данных и иных объектов, подлежащих защите в Школе. Разработать и ввести в действие должностную инструкцию пользователя ИСПДн, регламентирующую права и обязанности работника Школы при работе с ИСПДн.

Разработать и ввести в действие локальный нормативный акт, регламентирующий разграничение прав доступа к обрабатываемым в ИСПДн персональным данным.

4. Разработать и ввести в действие инструкцию о порядке учета, использования, транспортировки, хранения и уничтожения в Школе съемных носителей персональных данных.

5. Провести учет съемных носителей ПДн, по результатам ввести в действие журнал учета съемных носителей ПДн.

6. В рамках внутренних локальных актов, регламентирующих обработку и защиту персональных данных работников и клиентов Школы, утвердить перечни подразделений и работников Школы, допущенных к обработке ПДн работников и учащихся.

7. Разработать и ввести локальный нормативный акт об ответственности работников Школы за разглашение персональных данных и несанкционированный доступ к персональным данным.

8. Провести внутреннюю проверку и классификацию ИСПДн Школы. Разработать модель угроз ИСПДн и определить возможный ущерб, который может быть нанесен субъектам ПДн компрометацией их персональных данных. Результаты оформить в виде письменных отчетов, на основании которых разработать план мероприятий по обеспечению безопасности ПДн в ИСПДн Школы.

9. Обеспечить в рамках реализации плана мероприятий по обеспечению безопасности ПДн в ИСПДн Школы использование только таких средств защиты информации, которые прошли процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации. Ввести в действие журнал учета применяемых технических средств защиты ИСПДн.

10. Разработать и утвердить план мероприятий по обеспечению безопасности ПДн в Школе. Ввести в действие журнал учета мероприятий по контролю соблюдения режима защиты персональных данных в информационных системах Школы.

2. Технические меры по обеспечению безопасности ПДн в ИСПДн

Школа должна принимать технические меры по обеспечению безопасности информационных систем персональных данных. Применение технических мер защиты, их количество и степень защиты зависят от того, какой уровень защищенности персональных данных при их обработке в ИСПДн необходимо обеспечить.

План мероприятий по обеспечению безопасности персональных данных в Школе должен включать в себя следующие этапы работы:

- определение на основании Приказа ФСТЭК №21 базового набора мер по обеспечению

безопасности персональных данных в ИСПДн Школы;

- адаптация базового набора мер под ИСПДн Школы с учетом особенностей их функционирования, исключая те меры, которые связаны с информационными технологиями, не используемыми в ИСПДн;

- уточнение списка мер с выключением в него не выбранных ранее мер для нейтрализации актуальных угроз;

- внедрение дополнительных мер, обеспечивающих выполнение требований к защите персональных данных, установленных нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

В составе мер, входящих в план мероприятий по обеспечению безопасности персональных данных в Школе, должно быть, в том числе, предусмотрено:

- внедрение системы парольной аутентификация работников Школы, допущенных к работе с ИСПДн, предусматривающей определение минимальной длинны пароля, управление сроком действия и периодической сменой паролей; ограничение числа неудачных попыток входа в систему и использование программных генераторов паролей;

- установление инструктивных и технических правил, обеспечивающих разграничение прав доступа работников к различным ПДн, находящимся в ИСПДн Школы;

- разработка и внедрение регламента обеспечивающего установку и запуск в ИСПДн только разрешенного к использованию в информационной системе программного обеспечения, и исключающего возможность использования запрещенного к использованию в информационной системе программного обеспечения;

- разработка инструкции, регламентирующей порядок резервирования и восстановления работоспособности программного обеспечения, баз данных и систем защиты ИСПДн;

- разработка инструкции, регламентирующей защиту машинных носителей персональных данных от несанкционированного доступа и использования;

- внедрение технологии, позволяющей осуществлять сбор, запись, хранение, анализ, просмотр и защиту информации о событиях безопасности в ИСПДн Школы;

- использование программного обеспечения по антивирусной защите, обеспечивающего обнаружение в ИСПДн вредоносных программ и либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования ПДн, другой информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;

- проведение систематических мероприятий по анализу защищенности ИСПДн и тестированию работоспособности системы защиты персональных данных;

- обеспечение защиты ИСПДн, ее средств, систем связи и передачи данных при взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;

5. ЛИЦА, ОТВЕТСТВЕННЫЕ В ШКОЛЕ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

1. Общее руководство деятельностью Школы по обеспечению безопасности ПДн осуществляет директор.

2. Директор приказом назначает уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защиту персональных данных в Школе.

2. Уполномоченный сотрудник, ответственный за обеспечение информационной безопасности и защиту персональных данных, получает указания непосредственно от

директора либо руководителя по общим вопросам и им подотчетно.

3. Уполномоченный сотрудник, ответственный за обеспечение информационной безопасности и защиту персональных данных, в частности, обязан:

осуществлять внутренний контроль по соблюдению Школой и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводить до сведения работников Школы положения законодательства Российской Федерации о персональных данных, внутренних локальных нормативных актов, принятых в Школе по вопросам обработки и защите персональных данных;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, и осуществлять контроль за приемом и обработкой таких обращений и запросов;

не реже одного раза в три года проводиться проверку состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных, при необходимости вносить предложения по доработке или модернизации системы защиты ПДн.

4. Директор приказом возлагает на ответственных по работе с персональными данными следующие обязанности:

реализации мероприятий, предусмотренных настоящим Положением;

осуществление внутреннего контроля и аудита соответствия практики обработки персональных данных в Школе тем требованиям и нормам, которые установлены Законом «О персональных данных», а также принятым в этой сфере иным нормативным правовым актам и требованиям к защите персональных данных, и локальным нормативным актам Школы;

организационное, методическое и научно-техническое руководство работами по созданию либо модернизации системы защиты ПДн.

5. Школа на договорной основе имеет право привлечь для разработки и внедрения систем защиты ПДн в ИСПДн Школы специализированные организации, имеющие лицензии ФСТЭК, ФСБ России на соответствующие виды деятельности.

6. ПОРЯДОК МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ПДн.

Для ИСПДн, находящихся в эксплуатации, модернизация или доработка системы защиты ПДн должна проводиться в следующих случаях:

изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

изменился состав угроз безопасности ПДн в ИСПДн;

изменился уровень защищенности, который необходимо обеспечить при защите ПДн.

Для определения необходимости доработки или модернизации систем защиты ПДн не реже одного раза в три года должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных. Проверка проводится лицом, ответственным за обеспечение безопасности ПДн. Результаты проверки оформляются актом и утверждаются директором.

7. КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ПДн.

1. Уполномоченный сотрудник, ответственный за обеспечение информационной безопасности и защиту персональных данных, и Комиссия по персональным данным периодический (не реже одного раза в год) должны проводится контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

2. В случае выявления фактов несоблюдения условий хранения носителей ПДн, или использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности ПДн, либо нарушения заданного уровня безопасности ПДн, должно в обязательном порядке проводиться разбирательство.

2.1. В процессе проведения разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

2.2. По окончании проведения разбирательства готовится заключение о лицах, виновных в выявленных нарушениях.

8. НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ.

При организации и проведении работ по обеспечению безопасности ПДн в Школе, работники должны руководствоваться следующими нормативными и методическими документами:

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматической обработке персональных данных»

Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»

Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Локальные нормативные акты Школы по вопросам работы с персональными данными.