УТВЕРЖДЕНО
приказом №59 о/д от 29 декабря 2017 г.
МУДО «Детская школа искусств
с.Горькая Балка Советского района»
Директор _____М.Ю.Васляева

Положение о работе с персональными данными
в информационной системе персональных данных
в муниципальном учреждении дополнительного образования
«Детская школа искусств с.Горькая Балка Советского района»

I. Общие положения

1.1. Настоящее Положение о работе с персональными данными в информационной системе персональных данных в муниципальном учреждении дополнительного образования «Детская школа искусств с.Горькая Балка Советского района» (далее – Положение) разработано в соответствии с Федеральным Законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными документами ФСТЭК и ФСБ России с целью обеспечения защиты прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных.

1.2. Для целей настоящего Положения применяются следующие термины и определения:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- оператор персональных данных – муниципальное учреждение дополнительного образования «Детская школа искусств с.Горькая Балка Советского района» (далее – Учреждение) - юридическое 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.
- информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- 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, 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, применяемые в информационных системах.

- пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.
- правила разграничения доступа к информационным системам персональных данных – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- 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.
- распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
- блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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.
- обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- конфиденциальность персональных данных – Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
- трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
- несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных – доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в

том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

- защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

а) разграничение полномочий доступа к данным;

б) авторизация, контроль и учет действий с данными (регистрация событий);

в) контроль копирования, печати, обмена данными по каналам связи;

г) межсетевое экранирование и защита от вирусов;

д) учет внешних носителей данных;

е) резервное копирование / восстановление данных;

ж) раздельное хранение носителей данных с резервными копиями;

з) контроль доступа в помещения и к компьютерам;

и) применение устройств идентификации пользователей для доступа.

1.3. Настоящим Положением определяется структура и составляющие безопасности информации в информационной системе персональных данных работников Учреждения, обучающихся и их родителей (законных представителей).

II. Обеспечение безопасности персональных данных

2.1. Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных – ИСПДн) достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

2.2. Мероприятия по обеспечению безопасности ПДн формулируются на основании анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

2.3. Структура, состав и основные функции СЗПДн определяются исходя из анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

2.4. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн; на восстановление нормального функционирования ИСПДн после

нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

2.5. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с ПДн в информационной системе;
- контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

2.6. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

2.7. Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

2.8. По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;
- угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования.

2.9. Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

- обследование и оформление документа о типе актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, определение способов и состава средств защиты информации (СЗИ), разработка технического задания (ТЗ) на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование;

- ввод в эксплуатацию – закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации.

3. Цели обеспечения информационной безопасности

3.1. Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъекто в информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

- целостности информации;

- доступности обрабатываемой информации для зарегистрированных пользователей;

- конфиденциальности информации.

3.2. Объект защиты:

3.2.1. Объектом защиты является информационная система персональных данных работников Учреждения, обучающихся и их родителей (законных представителей).

3.3. Информационные ресурсы:

- персональные данные работников Учреждения, обучающихся и их родителей (законных представителей) (исходная информация, информационные базы данных);

- инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;

- технические информационные системы и средства Учреждения, в которых обрабатывается, хранится и передается информация ПДн;

- помещения объектов Учреждения, в которых размещаются информационные ресурсы, и обрабатывается конфиденциальная информация;

- технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

3.4. Критичными свойствами объекта защиты являются:

- возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;

- возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;

- несанкционированная доступность информации, выражающаяся в возможности:

а) непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на носитель или транспортную среду с целью перлюстрации,

отчуждения, копирования, изменения, подмены и уничтожения информации;

б) прямого или косвенного доступа к оборудованию ИСПДн и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ);

в) перехвата речевой информации по акустическим и другим каналам утечки (подслушивание).

3.5. Субъекты информационных отношений

3.5.1. Субъектами информационных отношений являются:

- работники – физические лица, состоящие в трудовых и иных гражданско-правовых отношениях с Учреждением-оператором;

- обучающиеся – физические лица, родители (законные представители) которых состоят в договорных и иных гражданско-правовых отношениях с Учреждением-оператором по вопросам оказания услуг в сфере образования, предусмотренных Уставом.

3.5.2. Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;

- достоверности (полноты, точности, адекватности, целостности) информации;

- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);

- своевременного доступа (за приемлемое для них время) к необходимой им информации;

- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

- защиты информации от незаконного ее тиражирования (защиты персональных данных, защиты авторских прав, прав собственника информации).

4. Возможные угрозы и участки вторжения

4.1. Общая классификация угроз.

4.1.1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к программам, данным, каналам связи, при перехвате электромагнитных излучений, при анализе трафика.

4.1.2. Угрозы целостности данных, программ, аппаратуры. Реализуются при несанкционированном уничтожении, модификации данных, порождении фальсифицированных данных, задержке и нарушении маршрутизации данных в каналах связи.

4.1.3. Угрозы доступности данных. Реализуются при создании условий, когда законный пользователь или процесс не получает своевременного доступа к данным или ресурсам системы, каналам связи.

5. Заключительные положения.

5.1. Решение основных вопросов обеспечения защиты ПДн предусматривает осуществление постоянного контроля, подготовку кадров, выделение необходимых финансовых и материальных средств, закупку программного и аппаратного обеспечения, а также, при необходимости, привлечение сторонней организации при наличии лицензий ФСТЭК и ФСБ.