Муниципальное учреждение дополнительного образования
«Детско-юношеская спортивная школа «РИТМ»

СОГЛАСОВАНО:
Представитель трудового коллектива
МУДО «ДЮСШ «РИТМ»

Логинова С.А.

УТВЕРЖДАЮ:
Директор МУДО «ДЮСШ «РИТМ»

Шафигулина И.Л.
Приказ №46 от 24.04.2017 года

Политика
в отношении обработки персональных данных
МУДО «ДЮСШ «РИТМ»

2017г.
г.Качканар

1. Назначение

1.1. Целью настоящей Политики в отношении обработки персональных данных (далее Политика) является обеспечение соответствия обработки и защиты персональных данных, обрабатываемых в муниципальном учреждении дополнительного образования «Детско-юношеской спортивной школе «РИТМ» (далее – учреждение), требованиям Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных», нормативных правовых актов, принятых в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных».

1.2. Политика разработана в соответствии с требованиями:

- Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных»;

- Постановление Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановления Правительства РФ от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановления Правительства РФ от 6 июля 2008г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Приказа Федеральной службы по техническому и экспортному контролю РФ, Федеральной службы безопасности РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

- Приказа Федеральной службы по техническому и экспортному контролю РФ от 5 февраля 2010г. №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;

- «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Федеральной службой по техническому и экспортному контролю РФ 15 февраля 2008г.;

- «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Федеральной службой по техническому и экспортному контролю РФ 15 февраля 2008г.;

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Федеральной службой безопасности РФ 21 февраля 2008г. №149/6/6-622;

- «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных Федеральной службой безопасности РФ 21 февраля 2008г. №149/54-144.

1.3. Политика содержит сведения о реализуемых требованиях к защите персональных данных.

1.4. Политика должна быть опубликована или иным образом должен быть обеспечен неограниченный доступ к ней.

2. Определения

2.1. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

2.2. **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.

2.3. Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

2.4. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.5. 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.

2.6. Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

2.7. Доступ к информации – возможность получения информации и ее использования.

2.8. Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

2.9. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.10. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.11. Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

2.12. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытие третьим лицам или их распространение без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.13. Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.14. Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

2.15. Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

2.16. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

2.17. Носитель персональных данных – материальный объект, в котором информация, содержащая персональные данные, находит свое отражение в виде символов, образов, сигналов, количественных характеристик физических величин. Выделяются следующие типы носителей персональных данных:

- бумажный носитель персональных данных – носитель на бумажной основе, содержащий персональные данные;

- машинный носитель персональных данных – электронный, магнитный, магнитооптический, оптический носитель, содержащий персональные данные (дискета, CD-диск, DVD-диск, жесткий диск, USB устройства, позволяющие хранить информацию, и т.д.).

2.18. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.19. 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.

2.20. 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.

2.21. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.22. Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

2.23. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.24. Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

2.25. Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

2.26. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.27. Технические средства – 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).

2.28. Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

2.29. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

2.31. 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.

2.32. Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

2.33. Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

2.34. Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.35. Шифровальные (криптографические) средства – криптосредства:

средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

ключевые документы (независимо от вида носителя ключевой информации).

3. Перечень условных обозначений и сокращений

ИСПД – информационные системы персональных данных учреждения
ПД – персональные данные
СЗПД - система защиты персональных данных, обрабатываемых в информационных системах персональных данных учреждения
СЗИ - средство защиты информации

4. Построение защиты персональных данных

4.1. В локальном акте учреждения – «Положении об обработке и защите персональных данных», определяются:

- порядок взаимодействия с Роскомнадзором;
- перечень оснований для обработки персональных данных (далее ПД);
- порядок получения ПД;
- порядок поручения обработки ПД;
- порядок предоставления, распространения ПД;
- порядок трансграничной передачи ПД;
- порядок прекращения обработки ПД, уничтожения ПД;
- порядок рассмотрения запросов субъектов ПД на предоставление информации;

- порядок рассмотрения запросов на уточнение ПД;
- порядок рассмотрения запросов на устранение нарушений законодательства, допущенных при обработке ПД, блокирование или уничтожение ПД;
- порядок принятия решений на основании исключительно автоматизированной обработки ПД;
- порядок защиты ПД.

4.2. Защита ПД, обрабатываемых без использования средств автоматизации, строится на основании требований Постановления Правительства РФ от **15 сентября 2008г. №687** «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.3. Система защиты ПД, обрабатываемых в информационных системах персональных данных учреждения (далее СЗПД), строится на основании требований нормативных правовых актов, принятых в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», а также:
- Перечня ПД, обрабатываемых в информационных системах персональных данных учреждения (далее ИСПД);
- Актов классификации ИСПД;
- Модели угроз безопасности ПД при их обработке в ИСПД.

4.4. ИСПД классифицируются в соответствии с Приказом Федеральной службы по техническому и экспортному контролю РФ, Федеральной службы безопасности РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

4.5. На основании класса ИСПД, перечня актуальных угроз безопасности ПД, указанных в Модели угроз безопасности ПД при их обработке в ИСПД, готовится Описание СЗПД.

5. Состав подсистем СЗПД

5.1. СЗПД включает в себя следующие подсистемы:
- организационных мер защиты;
- физической защиты;
- защиты каналов связи;
- управления логическим доступом;
- защиты от воздействия вредоносных программ;
- межсетевого экранирования;
- защиты информационного взаимодействия через сети связи общего пользования;
- обнаружения вторжений;
- инструментального анализа защищенности;
- конфиденциального делопроизводства;
- обеспечения целостности;
- обеспечения непрерывности;
- защиты от утечки по техническим каналам;
- подтверждения соответствия требованиям по безопасности.

6. Подсистема организационных мер защиты

6.1. Состоит из лиц, выполняющих функции по:
- администрированию программных, программно-аппаратных, аппаратных средств ИСПД;
- администрированию средств защиты информации ИСПД (далее СЗИ);
- защите ПД.

6.2. Также в данную подсистему входят локальные акты учреждения по вопросам обработки и защиты ПД.

7. Подсистема физической защиты

7.1. Данная подсистема предназначена для обеспечения физической охраны технических средств ИСПД, эксплуатационной и технической документации к СЗИ, ключевых документов, носителей ПД.
7.2. Данная подсистема реализуется путем применения инженерно-технических средств охраны, надежных хранилищ, мер по обеспечению необходимого уровня физической укрепленности помещений.

8. Подсистема защиты каналов связи

8.1. Данная подсистема предназначена для исключения несанкционированного доступа к защищаемой информации ИСПД (ПД, служебная информация СЗИ) при ее передаче по каналам связи, выходящим за пределы контролируемой зоны учреждения.

8.2. Данная подсистема реализуется путем применения криптосредств, защищенных коробов и защищенных телекоммуникационных шкафов совместно со средствами контроля за их вскрытием.

9. Подсистема управления логическим доступом

9.1. Данная подсистема предназначена для идентификации, проверки подлинности пользователей и администраторов ИСПД, разграничения и контроля доступа в ИСПД, регистрации действий пользователей и администраторов ИСПД.

9.2. Данная подсистема реализуется путем применения СЗИ от несанкционированного доступа, встроенных механизмов защиты применяемых программных, программно-аппаратных, аппаратных средств ИСПД (операционных систем, систем управления базами данных, приложений).

10. Подсистема защиты от воздействия вредоносных программ

10.1. Данная подсистема предназначена для защиты от воздействия на ИСПД вредоносных программ.
10.2. Данная подсистема реализуется путем применения средств антивирусной защиты, периодического обновления антивирусных баз на рабочих местах и серверах ИСПДн, подключенных к сетям связи общего пользования, а также ИСПДн, при функционировании которых предусмотрено использование съемных носителей информации.

11. Подсистема межсетевого экранирования

11.1. Данная подсистема предназначена для фильтрации трафика, передаваемого в/из ИСПД.
11.2. Данная подсистема реализуется путем применения межсетевых экранов при подключении ИСПД к сетям связи общего пользования, локальным вычислительным сетям учреждения.

12. Подсистема защиты информационного взаимодействия через сети связи общего пользования

12.1. Данная подсистема предназначена для защиты ПД при подключении ПД к сетям связи общего пользования в целях:
- получения общедоступной информации;
- удаленного доступа к ИСПД через сети связи общего пользования,
- межсетевого взаимодействия отдельных ИСПД учреждения через сети связи общего пользования;
- межсетевого взаимодействии отдельных ИСПД учреждения с ИСПД других операторов через сети связи общего пользования.

12.2. Данная подсистема реализуется путем:
- применения электронных замков, носителей информации для надежной идентификации и проверки подлинности пользователей;
- применения средств централизованного управления СЗПД;
- анализа принимаемой по сетям связи общего пользования информации (в том числе на наличие компьютерных вирусов);
- проверки подлинности взаимодействующих ИСПД;
- проверки подлинности пользователей;
- проверки целостности данных, передаваемых по сетям связи общего пользования;
- предотвращения возможности отрицания пользователем факта отправки ПД другому пользователю;
- предотвращения возможности отрицания пользователем факта получения ПДн от другого пользователя.

13. Подсистема обнаружения вторжений

13.1. Данная подсистема предназначена для защиты от воздействия на ИСПД сетевых атак.
13.2. Данная подсистема реализуется путем применения средств обнаружения вторжений при подключении ИСПД к сетям связи общего пользования.

14. Подсистема инструментального анализа защищенности

14.1. Данная подсистема предназначена для периодического тестирования функций СЗПД в целях выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения ИСПД, которые могут быть использованы нарушителем для реализации атаки на ИСПД.

14.2. Данная подсистема реализуется путем применения средств анализа защищенности как периодически, так и при изменении программной среды или состава пользователей ИСПД.

15. Подсистема конфиденциального делопроизводства

15.1. Данная подсистема предназначена для исключения несанкционированного доступа к носителям ПД.
15.2. Данная подсистема реализуется путем учета носителей ПД, исключения хищения, подмены или уничтожения съемных носителей ПД.

16. Подсистема обеспечения целостности

16.1. Данная подсистема предназначена для обеспечения целостности программной среды ИСПД, программных компонент СЗИ.

16.2. Данная подсистема реализуется путем:
- обеспечения отсутствия средств модификации объектного кода программ в процессе обработки и (или) хранения ПД;
- проверки целостности программных компонентов СЗПД;
- оборудования аппаратных средств, с которыми осуществляется штатное функционирование программных криптосредств, а также аппаратных и аппаратно-программных криптосредств средствами контроля за их вскрытием.

17. Подсистема обеспечения непрерывности

17.1. Данная подсистема предназначена для обеспечения возможности восстановления ПД, работоспособности СЗПД.
17.2. Данная подсистема реализуется путем применения средств дублирования массивов ПД, ведения копий программных компонентов СЗПД.

18. Подсистема защиты от утечки по техническим каналам
18.1. Данная подсистема предназначена для исключения утечки ПД по техническим каналам.
18.2. Данная подсистема реализуется путем:
- размещения устройств вывода информации (мониторов) таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПД;
- применения методов и способов защиты акустической (речевой) информации при использовании в ИСПД класса К1 функции голосового ввода ПД в ИСПД или функции воспроизведения ПД акустическими средствами ИСПД;
- применения методов и способов защиты ПД от утечки за счет побочных электромагнитных излучений и наводок в ИСПД класса К1.

19. Подсистема подтверждения соответствия требованиям по безопасности

19.1. Данная подсистема предназначена для обеспечения соответствия требованиям по безопасности ПД.
19.2. Данная подсистема реализуется путем:
- применения СЗИ, прошедших в установленном порядке процедуру оценки соответствия;
- оценки эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию ИСПД.

20. Персонал

20.1. Выделяются следующие группы лиц, участвующих в обработке и защите ПД:

- ответственный за организацию обработки ПД;
- администратор информационной безопасности ИСПД;
- администратор ИСПД;
- пользователи ИСПД.

21. Ответственный за организацию обработки ПД

21.1. Ответственный за организацию обработки ПД – работник учреждения или специализированной организации, имеющей необходимые лицензии ФСТЭК России и ФСБ России, ответственный за:
- подготовку локальных актов учреждения по вопросам обработки и защиты ПД;
- осуществление внутреннего контроля за соблюдением учреждением и его работниками законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПД;
- проведение инструктажа работников в целях доведения до данных работников положений законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПД;
- организацию приема и обработки запросов (обращений, заявлений) субъектов ПД или их представителей.

21.2. Ответственным за организацию обработки ПД назначается лицо, имеющее высшее профессиональное образование и (или) переподготовку (повышение квалификации) в области информационной безопасности, а также производственный стаж в области информационной безопасности не менее одного года.

21.3. Ответственный за организацию обработки ПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией ответственного за организацию обработки ПД» или соответствующим договором со специализированной организацией.

22. Администратор информационной безопасности ИСПД

22.1. Администратором информационной безопасности ИСПД назначается лицо, имеющее высшее профессиональное образование и (или) переподготовку (повышение квалификации) в области информационной безопасности, а также производственный стаж в области информационной безопасности не менее одного года.

22.2. Администратор информационной безопасности ИСПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией администратора информационной безопасности ИСПД или соответствующим договором со специализированной организацией.

23. Администратор ИСПД.

23.1. Администратор ИСПД – работник учреждения или работник специализированной организации или физическое лицо, ответственное за установку, настройку и сопровождение программных, программно-аппаратных, аппаратных средств ИСПД.
23.2. Администратором ИСПД назначается лицо, имеющее производственный стаж в области создания, обслуживания локальных вычислительных сетей не менее одного года.
23.3. Администратор ИСПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией администратора ИСПД или соответствующим договором со специализированной организацией или соответствующим договором с физическим лицом.

24. Пользователь ИСПД

24.1. Пользователь ИСПД – работник учреждения, работник контрагента учреждения, физическое лицо, осуществляющее обработку ПД в ИСПД.

24.2. Пользователь ИСПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией пользователя ИСПД или соответствующим договором с контрагентом или соответствующим договором с физическим лицом.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 217702588042463165739188801430949850835526482765

Владелец Ольховикова Надежда Сергеевна

Действителен С 13.11.2023 по 12.11.2024