

ПРИНЯТО:
Педагогическим советом
МБОУДОД
КДЮСШ «Ямбург»

Протокол № 1 от 31 августа 2015 г.

УТВЕРЖЕНО:
Директор МБОУДОД КДЮСШ
«Ямбург»
О.Б. Жмуркова
О.Б. Жмуркова

Приказ № 77 от 31 августа 2015г.



ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных
при их обработке в информационных системах
в муниципальном бюджетном образовательном учреждении
дополнительного образования детей
«Кингисеппская детско-юношеская спортивная школа «Ямбург»

Содержание

- I. Общие положения
- II. Документы, содержащие сведения, составляющие персональные данные
- III. Требования, предъявляемые при обработке персональных данных
- IV. Хранение и использование персональных данных
- V. Обеспечение безопасности персональных данных при их обработке в информационных системах

I. Общие положения

1.1. Настоящее Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в муниципальном бюджетном образовательном учреждении дополнительного образования детей «Кингисеппская детско-юношеская спортивная школа «Ямбург» (далее – Учреждение) разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от №781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных», уставом и иными локальными нормативными (правовыми) актами Учреждения.

1.2. Основными принципами обработки персональных данных являются:

- принцип законности целей и способов обработки персональных данных;
- принцип соответствия объема и характера обрабатываемых персональных данных, способам их обработки и целям обработки персональных данных;
- принцип достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к заявленным при их сборе целям;
- принцип недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- принцип защиты персональных данных от неправомерного доступа и их использования или утраты.

II. Документы, содержащие сведения, составляющие персональные данные

2.1. Документы работников Учреждения, документы, предъявляемые работником при заключении трудового договора: - паспорт или документ, удостоверяющий личность; трудовая книжка; страховое свидетельство государственного пенсионного страхования; документы воинского учета; документ об образовании и т.п.; документы о составе семьи работника, необходимые для предоставления гарантий, связанных с выполнением семейных обязанностей; документы о состоянии здоровья, когда с их наличием связано предоставление каких-либо гарантий и компенсаций; документы, подтверждающие право на дополнительные гарантии и компенсации по основаниям, предусмотренным законодательством РФ.

2.2. Документы обучающихся Учреждения: документы, предъявляемые в приёмную комиссию; документы, подтверждающие право на дополнительные гарантии и компенсации в соответствии с законодательством РФ; договоры; квитанции об оплате по договору.

III. Требования, предъявляемые при обработке персональных данных

3.1. При определении объема и содержания обрабатываемых персональных данных, директор должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3.2. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств, в порядке, установленном Трудовым кодексом РФ и иными федеральными законами;

3.3. Собственники персональных данных (их представители) должны быть ознакомлены с документами Учреждения, устанавливающими требования к обработке и обеспечению безопасности персональных данных, они не должны отказываться от своих прав на сохранение и защиту тайны.

3.4. Учреждение и собственники персональных данных (их представителями) должны совместно вырабатывать меры по защите персональных данных.

IV. Хранение и использование персональных данных

4.1. Документы, содержащие информацию о персональных данных, хранятся на бумажном и (или) электронном носителях.

4.2. Доступ к персональным данным, без получения специального разрешения имеет директор Учреждения; в пределах своей компетенции, в установленном порядке и в рамках выполнения должностных обязанностей. Доступ к персональным данным без получения специального разрешения имеют: - заместитель директора, работник кадрового подразделения, педагогические работники, программисты, члены приемной комиссии Учреждения, члены иных комиссий (советов), созданных приказом Учреждения, специалист по охране труда. Иные работники Учреждения могут иметь доступ к персональным данным в случае, если они получили разрешение директора в виде визы на служебной записке, обосновывающей необходимость доступа к персональным данным.

4.3. Со сторонними работниками (сопровождающими работу информационных систем, оказывающими бухгалтерские услуги и т.п.) заключаются договоры с обязательством о неразглашении персональных данных.

V. Обеспечение безопасности персональных данных при их обработке в информационных системах

5.1. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

5.2. Безопасность персональных данных 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 иных несанкционированных действий.

5.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

5.4. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

5.5. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения в эти помещения посторонних лиц.

5.6. При обработке персональных данных в информационной системе должны быть обеспечены:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

5.7. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию 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;
- организацию учета лиц, допущенных к работе с персональными данными в информационной системе на основании служебных записок, дополнительных трудовых соглашений;
- контроль за 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 персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

5.8. Контроль за организацией доступа к персональным данным возлагается на работников Учреждения, наделенных соответствующими полномочиями. При обнаружении

