Подписан: Ворохова Анна Александровна
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Дата: 2022.06.22 16:52: 13+11'00'

Утверждено
приказом № 77-ОД
от 22.06.2022 г.
И.о. директора МБУДО
«ДШИ «Этнос»
_____ О.Н.Кузнецова

ПОЛОЖЕНИЕ
О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «ДЕТСКАЯ ШКОЛА ИСКУССТВ «ЭТНОС»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о мерах по организации защиты информационных систем персональных данных в МБУДО «ДШИ «Этнос» (далее – Положение, Школа) разработано в соответствии с требованиями действующего законодательства в области обработки и защиты персональных данных (далее – ПДн), Политики Школы в отношении обработки и защиты персональных данных и 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.

1.2. 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.

1.3. 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.

1.4. Настоящее Положение, все изменения и дополнения к нему утверждаются приказом директора.

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

3.1. 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 видеоинформации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

3.2. Для обеспечения защиты информации, содержащейся в информационной системе, Школой назначается администратор безопасности информационных систем персональных данных Администратор информационной безопасности).

3.3. 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.

3.4. 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.

4. ОСНОВНЫЕ МЕРЫ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Для обеспечения необходимого уровня защищенности ПДн при их обработке в информационных системах Школы необходимо принять следующие основные организационные меры:

- назначить сотрудника, ответственного за обеспечение информационной безопасности и защиту персональных данных в ИСПДн;
- разработать локальную нормативную правовую базу в отношении обработки и защиты ПДн;
- определить состав и категории обрабатываемых в Школе персональных данных;
- утвердить перечень лиц, допущенных к работе с персональными данными в ИСПДн;
- разграничить права доступа к обрабатываемым в ИСПДн данным в зависимости от должностных обязанностей работников;
- ознакомить работников с требованиями локальных нормативных документов по обработке и защите ПД; провести обучение (инструктаж) работников, допущенных к обработке персональных данных в ИСПДн;
- проводить служебные расследования по фактам нарушения требований безопасности ПД;
- обеспечить соблюдение пропускного режима и режима безопасности помещений, в которых размещены ИСПДн Школы, с целью исключения неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- разместить устройства отображения информации таким образом, чтобы был исключен ее несанкционированный просмотр;

- обеспечить учёт и хранение носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение;
- провести внутреннюю проверку ИСПДн, разработать модель угроз ИСПДн и определить возможный ущерб, который может быть нанесен субъектам ПДн компрометацией их персональных данных.

4.2. Для обеспечения необходимого уровня защищенности ПДн при их обработке в информационных системах Школы необходимо принять технические меры. Применение технических мер защиты, их количество и степень защиты зависят от того, какой уровень защищенности персональных данных при их обработке в ИСПДн необходимо обеспечить.

4.3. К техническим мерам относятся следующие:
- внедрение системы парольной аутентификация работников Школы, допущенных к работе с ИСПДн, предусматривающей определение минимальной длины пароля, управление сроком действия и периодической сменой паролей; ограничение числа неудачных попыток входа в систему;
- управление доступом к к объектам ИСПДн, разграничение доступа и контроль за его соблюдением;
- установление инструктивных и технических правил, обеспечивающих разграничение прав доступа работников к различным ПДн, находящимся в ИСПДн Школы;
- разработка инструкции, регламентирующей порядок резервирования и восстановления работоспособности программного обеспечения, баз данных и систем защиты ИСПДн;
- резервное копирование информации;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности ПД при передаче по открытым каналам связи и хранении на съемных машинных носителях информации;
- установка и запуск в ИСПДн только разрешенного к использованию в информационной системе программного обеспечения, использование только таких средств защиты информации, которые соответствуют требованиям законодательства Российской Федерации в области обеспечения безопасности информации, контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- использование программного обеспечения по антивирусной защите, обеспечивающего обнаружение в ИСПДн вредоносных программ и 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 мероприятий при обнаружении несанкционированного доступа к персональным данным, обрабатываемым с использованием

средств автоматизации, в том числе восстановление персональных данных, которые были модифицированы или уничтожены вследствие несанкционированного доступа к ним;
- обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

5. 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.

6. КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ПДн

6.1. Администратор информационной безопасности осуществляет контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

6.2. Работник, ответственный за организацию обработки ПДн совместно с администратором информационной безопасности осуществляют контроль выполнения организационных и технических мер по организации защиты ИСПДн.

6.3. 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 проводится служебное расследование, в ходе которого выявляются причины, устанавливаются виновные лица и разрабатываются меры по предотвращению возможных негативных последствий подобных нарушений.