Приложение
к приказу **МБУ ДО «ДЮСШ» МО Черноморский район РК**

от «28» 12.2023 г. № 66

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных МБУ ДО «ДЮСШ» МО Черноморский район РК

22. Термины и определения

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

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

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.

Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.

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.

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

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

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

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.

23. Общие положения

– Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных **МБУ ДО «ДЮСШ» МО Черноморский район РК**

– (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

– Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

– Положение обязательно для исполнения всеми работниками **МБУ ДО «ДЮСШ» МО Черноморский район РК** (далее – Учреждение), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

24. Цели и задачи обеспечения безопасности персональных данных

4.1. Основной целью обеспечения безопасности ПДн, при их обработке в ИСПДн, является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

4.2. Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью системы защиты персональных данных (далее – СЗПДн).

4.3. СЗПДн включает в себя организационные, физические и (или) технические меры, используемых в ИСПДн.

25. Основные принципы построения системы защиты информации

5.1. СЗПДн основывается на следующих принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости;
- простоты применения средств защиты информации (далее – СЗИ).

5.2. Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

5.3. Принцип комплексности – предполагает, что СЗПДн должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ПДн от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

5.4. Принцип непрерывности защиты – это процесс обеспечения безопасности ПДн, осуществляемый руководством, ответственным за обеспечение безопасности ПДн в ИСПДн и работниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность СЗИ, сколько процесс, который должен постоянно идти на всех уровнях внутри Учреждения, и каждый работник должен принимать участие в этом процессе.

5.5. Принцип разумной достаточности – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

5.6. Принцип гибкости – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.

5.7. Принцип простоты применения СЗИ – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

26. Основные мероприятия по обеспечению безопасности персональных данных

1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, проводятся следующие мероприятия:

6.1. определение ответственных лиц за обеспечение защиты ПДн;
6.2. определение уровня защищенности ПДн;
6.3. реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн;
6.4. ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ПДн;
6.5. учет и хранение съемных машинных носителей ПДн;
6.6. организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ;
6.7. организация парольной защиты;
6.8. организация антивирусной защиты;
6.9. организация обновления программного обеспечения и СЗИ;
6.10. использование СЗИ;
6.11. обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
6.12. контроль за принимаемыми мерами по обеспечению безопасности ПДн;
6.13. планирование мероприятий по защите ПДн в ИСПДн;
6.14. управление (администрирование) СЗПДн;
6.15. управление конфигурацией ИСПДн и СЗПДн;
6.16. реагирование на инциденты;
6.17. информирование и обучение персонала ИСПДн.

2. Определение ответственных лиц за обеспечение безопасности ПДн

2.1. За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:

6.18. Директор.

6.19. Ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн.

6.20. Ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн.

6.21. Администратор ИСПДн – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.

3. Определение уровня защищенности ПДн

3.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется в соответствии с 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» и оформляется в виде «Акта об определения уровня защищенности персональных данных».

4. Реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн

4.1. Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПДн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных

МБУ ДО «ДЮСШ» МО Черноморский район РК , утвержденным приказом Директора Учреждения.

4.2. Основные технические средства и системы ИСПДн располагаются в помещениях, находящихся в пределах границы контролируемой зоны, определенной приказом Директора Учреждения, с максимальным удалением от её границ.

4.3. Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных в **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденными приказом Директора Учреждения.

5. Учет и хранение съемных машинных носителей ПДн

5.1. Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Порядком обращения со съемными машинными носителями персональных данных в **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденным приказом Директора Учреждения.

6. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ.

6.1. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в

информационных системах персональных данных **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденной приказом Директора Учреждения.

7. Организация парольной защиты

7.1. Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденной приказом Директора Учреждения.

8. Организация антивирусной защиты

8.1. Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты в **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденной приказом Директора Учреждения.

9. Организация обновления программного обеспечения и СЗИ

9.1. Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных **МБУ ДО «ДЮСШ» МО Черноморский район РК** и «Инструкцией администратора информационных систем персональных данных **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденные приказом Директора Учреждения.

10. Применение СЗИ

10.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, применяются СЗИ, прошедшие оценку соответствия.

10.2. Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.

11. Обнаружение фактов несанкционированного доступа к ПДн и принятие мер

11.1. Ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн должны сообщаться любые инциденты информационной безопасности, в которые входят:

6.22. факты попыток и успешной реализации несанкционированного доступа в ИСПДн;

6.23. факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ПДн;

6.24. факты сбоя или некорректной работы систем обработки ПДн;

6.25. факты сбоя или некорректной работы СЗИ;

6.26. факты разглашения ПДн, обрабатываемых в ИСПДн;

6.27. факты разглашения информации о методах и способах защиты и обработки ПДн в ИСПДн.

11.2. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденным приказом Директора Учреждения.

12. Контроль за принимаемыми мерами по обеспечению безопасности ПДн

12.1. Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в **МБУ ДО «ДЮСШ» МО Черноморский район РК** утвержденным приказом Директора Учреждения.

27. Ответственность

- Все работники, допущенные в установленном порядке к работе с ПДн, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за необеспечение сохранности и несоблюдение правил работы с ПДн.
- Ответственность за доведение требований настоящего Положения до работников Учреждения и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.