

УТВЕРЖДАЮ

Директор МБУ ДО
«СШОР по баскетболу»



Годзинский А.Н.

12

2022 г.

**Разрешительная система доступа к персональным данным,
содержащимся в базах данных
Муниципального бюджетного учреждения
дополнительного образования
«Спортивная школа олимпийского резерва по баскетболу»
(МБУ ДО «СШОР по баскетболу»)**

РАЗРАБОТАЛ

Администратор информационной
безопасности

Лапутина И.И.

подпись

расшифровка подписи

" 07 "

12

2022 г.

г. Мытищи

1. Общие положения

1.1. Разрешительная система доступа к персональным данным, содержащимся в базах данных является локальным нормативным актом Муниципального бюджетного учреждения дополнительного образования «Спортивная школа олимпийского резерва по баскетболу» (МБУ ДО «СШОР по баскетболу») устанавливает правила доступа сотрудников и сторонних организаций к персональным данным, содержащимся в базах данных (далее соответственно – положение, организация, персональные данные).

1.2. В настоящем положении используются следующие основные понятия в соответствии, в том числе с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъект 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.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Информационные ресурсы организации, содержащие персональные данные – отдельные документы и массивы документов, а также документы и массивы документов в информационных системах (базах данных, архивах), доступ к которым ограничен в соответствии с законодательством Российской Федерации и локальными нормативными актами организации, и которые содержат персональные данные.

Доступ пользователя к информационным ресурсам – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

2. Порядок предоставления доступа

2.1. Предоставление доступа сотрудникам к любым информационным ресурсам должно осуществляться только на основании заявок, оформленных в соответствии с приложением 1 к настоящему положению.

2.2. Перед предоставлением сотруднику доступа к информационным ресурсам организации, содержащим персональные данные, необходимо:

отразить в трудовом договоре с сотрудником обязательства о неразглашении персональных данных, которые будут ему известны при исполнении служебных обязанностей, и о соблюдении требований локальных нормативных актов, регулирующих порядок обращения с персональными данными;

а) перечень персональных данных организации;
б) инструкция по обеспечению безопасности обрабатываемых персональных данных;

в) инструкции пользователей информационных систем персональных данных (для всех ИСПДн, используемых в организации).

2.3. На основании распорядительного акта руководителя организации (при необходимости) осуществляется допуск пользователя к персональным данным, объеме, необходимом для выполнения им своих функциональных обязанностей.

2.4. При переводе на другую должность основанием для допуска служит распорядительный акт руководителя, при этом допуск работника по предыдущей должности прекращается, и он допускается к сведениям по новой должности.

2.5. Перечень персональных данных организации необходимо поддерживать актуальном состоянии.

3. Порядок получения разрешения на предоставление доступа

3.1. Предоставление пользователям доступа к персональным данным организации осуществляется следующим образом:

заявка на предоставление доступа к ресурсу, подписанная непосредственным руководителем, направляется ответственному за этот ресурс лицу;

подписанная ответственным за ресурс лицом заявка согласовывается администратором информационной безопасности и направляется системному администратору для предоставления доступа пользователю к запрашиваемому ресурсу.

3.2. Срок рассмотрения заявки на предоставление доступа пользователей информационным ресурсам не должен превышать одного рабочего дня.

4. Порядок прекращения доступа

4.1. Прекращение предоставления доступа пользователям к персональным данным организации осуществляется следующим образом:

в случае увольнения (перевода на другую должность) сотрудника заявка на отключение доступа к ресурсу, подписанная непосредственным руководителем, направляется ответственному за этот ресурс лицу;

подписанная ответственным за ресурс лицом заявка направляется системному администратору и администратору информационной безопасности для отключения доступа пользователя к ресурсу.

4.2. В случае компрометации аутентификационных данных пользователей руководитель подразделения извещает в письменном виде администраторов информационной безопасности о факте компрометации.

4.3. Администратор информационной безопасности должен уведомить в письменном виде ответственного за ресурс и лицо, выполняющее функции системного администратора, о необходимости отключения доступа пользователя к ресурсу и инициировать служебное расследование.

5. Контроль доступа к информационным ресурсам

5.1. Контроль правомерности предоставления доступа пользователей информационным ресурсам возлагается на администратора информационной безопасности.

6. Ответственность

6.1. Сотрудники организации, допущенные к работе с персональными данными несут ответственность за разглашение персональных данных в соответствии с законодательством Российской Федерации.

7. Перечень локальных нормативных актов, ознакомление с которыми рекомендуется в целях соблюдения требований настоящего положения

- Перечень защищаемой информации в организации.
- Инструкция пользователя ИСПДн.
- Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций.
- Инструкция администратора ИБ.

Заявка на доступ к информационным ресурсам

Наименование информационного ресурса	
ФИО сотрудника, получающего доступ	
Права	
Основание получения доступа	

Подпись непосредственного руководителя сотрудника, запрашивающего доступ:

Должность _____ подпись _____ Инициалы, фамилия

СОГЛАСОВАНО:

Администратор информационной безопасности

(подпись)

(инициалы, фамилия)

Доступ предоставлен:

Администратор ИСПДн

(название ИСПДн)

(подпись)

(инициалы, фамилия)

Положение о порядке организации и проведения работ по защите персональных данных организации.

Инструкция пользователя

[illegible]

(цифрами и прописью)

Годзинский А.Н./

