**Администрация Петрозаводского городского округа**

**Муниципальное бюджетное учреждение**
**Петрозаводского городского округа**
**«Дирекция спортивных сооружений и спортивной подготовки»**
**(МУ «Дирекция спорта»)**

# ПРИКАЗ

09.06.2025 № 250 - ОД

**«О применении мер по обеспечению безопасности персональных данных при их обработке»**

Руководствуясь ч.ч. 1 и 2 ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»,

**ПРИКАЗЫВАЮ:**

1. Утвердить Перечень информационных систем персональных данных муниципального бюджетного учреждения Петрозаводского городского округа «Дирекция спортивных сооружений и спортивной подготовки» (Приложение № 1).
2. Утвердить Перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение № 2).
3. Утвердить Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей (Приложение № 3).
4. Утвердить Правила доступа работников в помещения, в которых ведется обработка персональных данных (Приложение № 4).
5. Утвердить Порядок обращения со съемными машинными носителями персональных данных (Приложение № 5).
6. Утвердить Инструкцию пользователя информационной системы (Приложение № 6).
7. Утвердить Инструкцию по организации парольной защиты (Приложение № 7).
8. Утвердить Инструкцию по организации антивирусной защиты (Приложение № 8).
9. Утвердить Инструкцию по организации обновления программного обеспечения и средств защиты информации (Приложение № 9).
10. Утвердить Инструкцию о порядке организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации (Приложение № 10).
11. Утвердить Положение о разрешительной системе доступа к ресурсам информационных систем (Приложение № 11).
12. Утвердить Политику конфиденциальности (Приложение № 12).
13. Ответственному за организацию обработки персональных данных обеспечить в установленном порядке сохранность носителей персональных данных, использование

средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

14. Ответственному за организацию обработки персональных данных обеспечить контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

15. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор А.М. Сандальнев

Приложение № 1
к приказу от 09.06. 2025 г. № 250-ОД

**Перечень информационных систем персональных данных МУ «Дирекция спорта»**

| № п/п | Наименование, ИСПДн | Назначение ИСПДн | Категории субъектов ПДн, обрабатываемых в ИСПДн | Категории ПДн, обрабатываемых в ИСПДн | Необходимый уровень защищенности |
|---|---|---|---|---|---|
| 1. | Информационная система бухгалтерского и кадрового учета 1С | Ведение кадрового делопроизводства и бухгалтерского учета | Работники, родственники работников, уволенные работники | фамилия, имя, отчество;<br>пол;<br>год рождения;<br>месяц рождения;<br>дата рождения;<br>место рождения;<br>гражданство;<br>данные документа, удостоверяющего личность;<br>адрес места жительства;<br>адрес регистрации;<br>номер телефона;<br>адрес электронной почты;<br>СНИЛС;<br>ИНН;<br>семейное положение;<br>сведения о близких родственниках (фамилия, имя, отчество; степень родства; год рождения);<br>доходы;<br>реквизиты банковской карты;<br>номер лицевого счета;<br>профессия;<br>должность;<br>сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);<br>отношение к воинской обязанности, сведения о воинском учете;<br>сведения об образовании;<br>сведения об удержаниях по исполнительным документам;<br>сведения о доходе с предыдущего места работы | **4-ый уровень защищенности персональных данных**:<br>не обрабатываются специальные и биометрические категории персональных данных,<br>не обрабатываются только общедоступные персональные данные;<br>категория обрабатываемых персональных данных: иные ПДн;<br>обрабатываются персональные данные менее чем 100 000 субъектов;<br>определены угрозы 3 типа |

| | | | | | |
|---|---|---|---|---|---|
| | | | Контрагенты, представители контрагентов | фамилия, имя, отчество;<br>адрес электронной почты;<br>адрес места жительства;<br>адрес регистрации<br>номер телефона;<br>ИНН;<br>СНИЛС;<br>данные документа, удостоверяющего личность;<br>реквизиты банковской карты;<br>номер лицевого счета;<br>номер расчетного счета;<br>данные документа, подтверждающего полномочия представителя контрагента;<br>данные пенсионного удостоверения;<br>данные удостоверения инвалида | |

Приложение № 2
к приказу от 09.06.2025 г. № 250-ОД

**Перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных**

1. Настоящий Перечень определяет угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных МУ «Дирекция спорта».

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

3. Угрозами безопасности персональных данных (за исключением персональных данных, разрешенных субъектом персональных данных для их распространения), актуальными при их обработке в информационных системах персональных данных МУ «Дирекция спорта», являются:

угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе;

угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации;

угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем персональных данных;

угрозы воздействия вредоносного кода и (или) вредоносной программы, внешних по отношению к информационным системам персональных данных;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, обладающими полномочиями в информационных системах персональных данных, в том числе в ходе создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации информационных систем персональных данных, и дальнейшего хранения содержащейся в их базах данных информации;

угрозы использования методов воздействия на лиц, обладающих полномочиями в информационных системах персональных данных;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах персональных данных, с использованием уязвимостей в организации защиты персональных данных;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах персональных данных, с использованием уязвимостей в программном обеспечении информационных систем персональных данных;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем персональных данных;

угрозы физического доступа к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации;

угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием средств криптографической защиты информации персональных данных или создания условий для этого, определяемые оператором информационных систем персональных данных в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденным приказом Федеральной службы безопасности Российской Федерации от 10.08.2014 № 378.

4. Угрозами безопасности персональных данных, разрешенных субъектом персональных данных для их распространения, актуальными при их обработке в информационных системах персональных данных, являются в том числе угрозы нарушения целостности (подмены) и нарушения доступности персональных данных, разрешенных субъектом персональных данных для их распространения.

Приложение № 3
к приказу от 09.06.2025 г. № 250-ОД

**Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей**

1. Директор Сандальнев А.М.
2. Заместитель директора по техническим вопросам Федулов М.П.
3. Заместитель директора по спортивно-массовым мероприятиям Петровская З.В.
4. Начальник общего отдела Сухоросова Т.Ю.
5. Начальник отдела физкультуры и спорта Цветкова О.В.
6. Специалист по кадрам Иванова О.Г.
7. Специалист по планированию Веретенникова Л.Н.
8. Специалист по закупкам Сиротюк И.Р.
9. Инструктор-методист Осипова А.А.
10. Инструктор – методист Михеева Е.В.
11. Заведующий хозяйством Семенова М.Д.
12. Делопроизводитель Шумилова Т.И.
13. Инженер-программист Сень И.М.

Приложение № 4
к приказу от 09.06.2025 г. № 250-ОД

**Правила доступа работников в помещения, в которых ведется обработка персональных данных**

1. Настоящие Правила доступа работников в помещения, в которых ведется обработка персональных данных (далее – Правила) устанавливают единые требования к доступу работников в помещения, в которых ведется обработка персональных данных.

2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

3. Правила обязательны для исполнения всеми работниками, которые участвуют в обработке персональных данных.

4. Нарушение Правил влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

5. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, в которых ведется обработка персональных данных.

6. Размещение основных технических средств и систем обработки персональных данных осуществляется в охраняемых помещениях, расположенных в пределах границы контролируемой зоны.

7. В помещения, в которых ведется обработка персональных данных, допускаются только работники, уполномоченные осуществлять обработку и (или) защиту персональных данных.

8. Ответственными за организацию доступа в помещения являются руководители структурных подразделений, использующих помещения.

9. Нахождения лиц, не уполномоченных осуществлять обработку и (или) защиту персональных данных, в помещениях возможно только в сопровождении уполномоченного работника на время, ограниченное служебной необходимостью.

10. В целях обеспечения соблюдения требований к ограничению доступа в помещения Оператором обеспечивается:

1) использование помещений строго по назначению;

2) наличие на входах в помещения дверей, оборудованных запорными устройствами;

3) содержание дверей помещений в нерабочее время в закрытом на запорное устройство состоянии;

4) содержание окон в помещениях в нерабочее время в закрытом состоянии.

Приложение № 5
к приказу от 09.06.2025 г. № 250-ОД

**Порядок обращения со съемными машинными носителями персональных данных**

1. Настоящая Порядок обращения со съемными машинными носителями персональных данных (далее – Порядок), разработан в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных при их обработке в информационных системах.

2. Настоящий Порядок определяет:

1) правила обращения со съемными машинными носителями персональных данных;

2) порядок организации учета съемных машинных носителей персональных данных;

3) порядок уничтожения съемных машинных носителей персональных данных.

3. Порядок обязателен для исполнения всеми работниками муниципального бюджетного учреждения Петрозаводского городского округа «Дирекция спортивных сооружений и спортивной подготовки» (далее - Организация), непосредственно участвующими в обработке персональных данных в информационных системах.

4. При обращении со съемными машинными носителями персональных данных в информационной системе, выполняются следующие основные правила:

1) съемные машинные носители персональных данных учитываются и выдаются пользователям под подпись;

2) съемные машинные носители персональных данных, срок эксплуатации которых истек, уничтожаются в установленном порядке;

3) для выноса съемных машинных носителей персональных данных за пределы контролируемой зоны, запрашивается специальное разрешение, а факт выноса фиксируется;

4) право на перемещение съемных машинных носителей информации за пределы контролируемой зоны, имеют только те лица, которым оно необходимо для выполнения своих трудовых обязанностей (функции);

5) все съемные машинные носители персональных данных хранятся в безопасном месте в соответствии с требованиями по их эксплуатации.

5. Ответственным за хранение, учет и выдачу съемных машинных носителей персональных данных, является ответственный за обработку персональных данных.

6. Все находящиеся на хранении и в обращении съемные машинные носители персональных данных учитываются ответственным в Журнале учета съемных машинных носителей персональных данных (Приложение № 1).

7. Пользователи информационных систем для выполнения работ получают съемные машинные носители персональных данных у ответственного. При получении делаются соответствующие записи в Журнале учета съемных машинных носителей персональных данных.

8. Допускается хранение съемных машинных носителей персональных данных в личных сейфах, закрываемых шкафах, при условиях исключения возможности несанкционированного ознакомления с содержанием информации, хранящейся на съемных машинных носителей персональных данных.

9. Съемные машинные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

10. Уничтожение съемных машинных носителей персональных данных осуществляется комиссией по уничтожению, назначенной приказом руководителя Организации.

11. Уничтожение магнитных, оптических, магнитооптических и электронных съемных машинных носителей персональных данных производится путем их физического разрушения.

12. По результатам уничтожения комиссией составляется Акт уничтожения съемных машинных носителей персональных данных.

**Приложение № 1**
к Порядку обращения со съемными машинными носителями персональных данных

**Журнал учета съемных машинных носителей персональных данных**

Начат: «09» июня 2025 г.

Окончен: «___» _____ 20__ г.

На _____ листах

| № п/п | Тип носителя | Номер (серийный/ инвентарный) | Расписка в получении | | | Подпись ответственного лица | Место хранения | Примечание | Дата и номер акта уничтожения |
|---|---|---|---|---|---|---|---|---|---|
| | | | ФИО | Дата | Подпись | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Приложение № 6
к приказу от 09.06.2025 г. № 250-ОД

**Инструкция пользователя информационной системы**

1. Настоящая инструкция определяет обязанности, права и ответственность пользователя информационной системы.

2. Пользователь информационной системы в своей работе руководствуется настоящей инструкцией.

3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

4. Пользователь обязан:

1) знать и выполнять требования настоящей инструкции, а так же действующих нормативных и руководящих документов регламентирующих порядок действий по защите информации;

2) выполнять на автоматизированном рабочем месте только те процедуры, которые требуются для выполнения его должностных обязанностей;

3) работать в сетях общего доступа, только при служебной необходимости;

4) соблюдать установленные правила разграничения доступа к информации, обрабатываемой в информационной системе;

5) покидая свое рабочее место на кратковременный срок блокировать доступ к операционной среде автоматизированного рабочего места;

6) знать и выполнять правила работы со средствами защиты информации, установленными в информационной системе;

7) немедленно ставить в известность ответственного администратора информационной системы, об обнаруженных инцидентах, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы средств защиты информации;
- факты разглашения информации, содержащей персональные данные;
- факты разглашения информации о методах и способах защиты и обработки информации.

8. Пользователю запрещается:

1) разглашать сведения ограниченного доступа, ставшие известными ему по роду работы;

2) производить действия в информационной системе в обход процедур идентификации и аутентификации в операционной системе;

3) использовать неучтенные внешние машинные носители информации;

4) подключать к автоматизированному рабочему месту мобильные устройства;

5) самостоятельно устанавливать или модифицировать программное и (или) аппаратное обеспечение информационной системы;

6) отключать средства защиты информации;

7) использовать компоненты программного и аппаратного обеспечения информационной системы в неслужебных (личных) целях;

8) оставлять автоматизированное рабочее место без присмотра, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

9) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инцидентам информационной безопасности.

9. Пользователь информационной системы несет ответственность в соответствии с действующим законодательством за разглашение сведений ограниченного доступа, ставших известными ему по роду работы.

Приложение № 7
к приказу от 09.06.2025 г. № 250-ОД

**Инструкция по организации парольной защиты**

1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей пользователей абонентского пункта информационной системы.

2. Пользователь информационной системы в своей работе руководствуется настоящей инструкцией.

3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

4. Личные пароли доступа к автоматизированному рабочему месту из состава информационной системы создаются пользователем самостоятельно.

5. Личные пароли доступа к автоматизированному рабочему месту из состава информационной системы должны соответствовать следующим требованиям:

1) длина пароля не менее 6 символов;

2) алфавит пароля не менее 60 символов;

3) максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;

4) блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут;

5) смена паролей не более чем через 120 дней;

6) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также общепринятые сокращения (anonymous, user, пользователь и т.п.).

6. Правила хранения парольной информации:

1) запрещается записывать пароли на бумажные носители, в файл, в электронную записную книжку и другие носители информации, в том числе на предметы;

2) запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

3) хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

7. Правила ввода пароля:

1) ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

2) во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

8. Правила смены паролей:

1) в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, пользователи обязаны сразу после исчерпания инцидента сменить пароль или запросить изменение пароля у администратора информационной системы;

2) внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри Организации и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой;

3) внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора информационной системы.

9. Владельцы паролей обязаны своевременно сообщать администратору информационной системы об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

10. Ответственность за соблюдение пользователями правил настоящей инструкции возлагается на администратора информационной системы.

11. Ответственность за хранение и ввод парольной информации возлагается персонально на владельца пароля.

Приложение № 8
к приказу от 09.06.2025 г. № 250-02

**Инструкция по организации антивирусной защиты**

1. Настоящая инструкция определяет порядок применения средств антивирусной защиты абонентского пункта информационной системы.

2. Пользователь информационной системы в своей работе руководствуется настоящей инструкцией.

3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

4. Средства антивирусной защиты должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в информационной системе.

5. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

6. Реализация антивирусной защиты должна предусматривать:

1) проведение периодических проверок автоматизированных рабочих мест на наличие вредоносных компьютерных программ (вирусов);

2) проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

3) оповещение в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

4) определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

7. При резервном копировании информации, файлы, помещаемые в электронный архив, должны проходить антивирусный контроль с целью выявления вредоносных компьютерных программ.

8. Обновление базы данных признаков вредоносных компьютерных программ (вирусов) производится один раз в сутки в автоматическом режиме.

9. Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

1) получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

2) получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

3) контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

10 Пользователям запрещается:

1) отключать средства антивирусной защиты во время работы;

2) использовать средства антивирусной защиты, отличные от установленных средств;

3) без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

11. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения ответственного администратора информационной системы.

12. В случае появления подозрений на наличие программных вирусов пользователи должны немедленно проинформировать об этом ответственного администратора информационной системы.

13. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в информационной системе, пользователь должен:

1) приостановить процесс приема-передачи информации;

2) сообщить ответственному администратору информационной системы о факте обнаружения программного вируса;

3) принять по согласованию с ответственным администратором информационной системы меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;

4) в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку;

5) по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

14. За нарушение требований настоящей Инструкции ответственный за защиту информации в информационной системе и пользователи несут ответственность, установленную действующим законодательством Российской Федерации и нормативными правовыми актами.

Приложение № 9
к приказу от 09.06.2025 г. № 250-ОД

**Инструкция по организации обновления программного обеспечения и средств защиты информации**

1. Настоящая инструкция регламентирует процессы обновления программного обеспечения и средств защиты информации.

2. Пользователь информационной системы в своей работе руководствуется настоящей инструкцией.

3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

4. Установке обновлений должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

5. В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно.

6. Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

7. Установка протестированных обновлений может быть произведена только администратором информационной системы.

8. Установка новых версий программного обеспечения или внесение изменений и дополнений в действующее программного обеспечения может быть произведено только администратором информационной системы.

9. Ответственность за соблюдение пользователями правил настоящей инструкции возлагается на ответственного за обработку персональных данных.

10. Ответственность за организацию обновления программного обеспечения и средств защиты информации в информационной системе несет администратор информационной системы.

Приложение № 10
к приказу от 09.06.2025 г. № 250-ОД

**Инструкция о порядке организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации**

1. Настоящая инструкция регламентирует процессы организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации информационной системы.

2. Пользователь информационной системы в своей работе руководствуется настоящей инструкцией.

3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

4. Резервирование программного обеспечения и баз данных, средств защиты информации информационной системы выполняется администратором информационной системы в том числе в целях обеспечения возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5. Определяется 2 вида резервирования баз данных:

1) полное резервирование – резервное копирование всех данных;

2) неполное резервирование– резервное копирование части данных.

6. Целью неполного резервирования является сохранение изменений в информационной системе с момента полного резервирования баз данных.

7. Периодичность проведения работ по резервированию баз данных должна составлять не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

8. Для организации резервирования и восстановления работоспособности программного обеспечения, должно быть обеспечено ведение двух копий программных средств и их периодическое обновление и контроль работоспособности.

9. Для организации резервирования и восстановления работоспособности программного обеспечения, перед каждым обновлением программного обеспечения необходимо делать контрольную точку восстановления операционной системы.

10. При организации резервирования и восстановления работоспособности программного обеспечения сначала осуществляется резервное копирование баз данных, затем производится полная деинсталляция некорректно работающего программного обеспечения.

11. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты информации.

12. Ответственность за проведение мероприятий по восстановлению программного обеспечения и баз данных, средств защиты информации возлагается на администратора информационной системы.

Приложение № 11
к приказу от 09.06.2025 г. № 250-ОД

**Положение о разрешительной системе доступа к ресурсам информационных систем**

## I. Основные термины и определения

**Дискреционный метод управления доступом -** метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа.

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

**Матрица доступа** – таблица, отображающая правила разграничения доступа.

**Объект доступа** – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Ролевой метод управления доступом** – метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

**Субъект доступа** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Типы доступа** – операции, разрешенные к выполнению субъектом доступа при доступе к объектам доступа.

## II. Общие положения

2.1 Настоящее Положение о разрешительной системе доступа (далее – Положение) к ресурсам абонентского пункта информационной системы, разработано в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных при их обработке в информационных системах.

2.2 Настоящее Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа.

## III. Субъекты и объекты доступа

3.1 К субъектам доступа в информационной системе, относятся работники оператора, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными инструкциями и которым в информационной системе присвоены учетные записи.

3.2 К объектам доступа в информационной системе, относятся:

- основные конфигурационные файлы операционной системы;
- средства настройки и управления операционной системой;
- основные конфигурационные файлы средств защиты информации;
- средства настройки и управления средств защиты информации;
- прикладное программное обеспечение;
- периферийные устройства;
- съемные машинные носители информации;
- обрабатываемые, хранимые данные.

## IV. Методы управления доступом

4.1 Методы управления доступом реализованы в соответствии с особенностями функционирования информационной системы и с учетом угроз безопасности информации и включают комбинацию следующих методов:

- ролевой метод управления доступом;
- дискреционный метод управления доступом.

4.2 Реализация ролевого метода управления доступом в информационной системе представлена в таблице 1.

Таблица 1

| № п/п | Роль субъекта доступа | Уровень доступа к объектам доступа |
|---|---|---|
| 1 | Администратор информационной системы | - обладает полной информацией о системном и прикладном программном обеспечении информационной системы;<br>- обладает полной информацией о технических средствах и конфигурации информационной системы;<br>- обладает правами конфигурирования и административной настройки технических средств информационной системы;<br>- обладает правами внесения изменений в программное обеспечение информационной системы на стадии ее разработки, внедрения и сопровождения |
| 2 | Ответственный за защиту информации | - обладает правами администратора информационной системы;<br>- обладает полной информацией об используемых в информационной системе средствах защиты;<br>- обладает правами конфигурирования средств защиты используемых в информационной системе |
| 3 | Пользователь | - обладает всеми необходимыми атрибутами и правами обеспечивающими доступ к обрабатываемой информации |

4.2 Дискреционный метод управления доступом в информационной системе реализован с помощью Матрицы доступа работников, к ресурсам информационной системы (Приложение № 1).

## V. Типы доступа

5.1 В информационной системе определены следующие типы доступа субъектов доступа к объектам доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) - субъекту доступа разрешено сканирование;
- полный (F) - субъект доступа имеет полный доступ к объектам доступа.

5.2 Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в информационной системе, типы доступа, определены в Матрице доступа работников, к ресурсам информационной системы.

## VI. Правила разграничения доступа

6.1 В информационной системе правила разграничения доступа реализованы совокупностью правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы:

- разделение обязанностей и назначение минимально необходимых прав пользователям, администратору информационной системы и лицу, обеспечивающему функционирование системы защиты информационной системы;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- контроль использования в информационной системе технологий беспроводного доступа;
- контроль использования в информационной системе мобильных технических средств;
- управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

6.2 В информационной системе реализовано разделение обязанностей и назначение минимально необходимых прав пользователям, администратору информационной системы и лицу, обеспечивающему функционирование системы защиты информационной системы, в соответствии с их должностными функциями.

6.3 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей.

6.3.1 Управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей в информационной системе, осуществляет администратор информационной системы.

6.3.2 В информационной системе реализованы следующие функции управления учетными записями пользователей:

- определение типа учетной записи (пользователь, администратор, системная);
- объединение учетных записей в группы (пользователи, администраторы);
- верификация пользователя при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и корректировка учетных записей пользователей;
- порядок заведения и контроля использования временных учетных записей пользователей;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
- предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

6.3.3 Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

6.3.4 В информационной системе осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

6.3.5 Администратор информационной системы ведет учет пользователей в Журнале учета пользователей абонентского пункта информационной системы (Приложение № 2).

6.4 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

6.4.1 При передаче информации между устройствами, сегментами в рамках информационной системы, осуществляется управление информационными потоками, включающее:
- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в информационной системе только по установленному маршруту;
- изменение (перенаправление) маршрута передачи информации только в установленных случаях;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в установленных случаях.

6.4.2 Управление информационными потоками обеспечивает разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

6.4.3 Управление информационными потоками блокирует передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, не санкционированно исходящие из информационной системы и (или) входящие в информационную систему.

6.5 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

6.5.1 В информационной системе установлено и зафиксировано в Инструкции по организации парольной защиты:
- количество неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени;

- блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) в информационной системе.

6.5.2 В информационной системе обеспечивается блокирование сеанса доступа пользователя по запросу пользователя.

6.5.3 Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).

6.5.4 Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

6.6 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.

6.6.1 Администратору информационной системы и ответственный за защиту информации в информационной системе разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

6.7 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

6.7.1 В информационной системе исключен удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

6.8 Контроль использования в информационной системе технологий беспроводного доступа.

6.8.1 В информационной системе исключено использование технологий беспроводного доступа.

6.9 Контроль использования в информационной системе мобильных технических средств.

6.9.1 В информационной системе в качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства).

6.9.2 Регламентация и контроль использования съемных машинных носителей информации, описаны в Порядке обращения со съемными машинными носителями персональных данных.

6.10 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

6.10.1 В информационной системе при взаимодействии с внешними информационными системами, взаимодействие с которыми необходимо для функционирования информационной системы, предоставление доступа к информационной системе осуществляется только авторизованным (уполномоченным) пользователям в соответствии с Матрицей доступа работников, к ресурсам информационной системы.

Приложение № 1 к Положение о разрешительной системе доступа к ресурсам информационных систем

**Матрица доступа к ресурсам абонентского пункта информационной системы**

| Субъект доступа | Объект доступа | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Основные конфигурационные файлы операционной системы | Средства настройки и управления операционной системой | Основные конфигурационные файлы средств защиты информации | Средства настройки и управления средств защиты информации | Прикладное программное обеспечение | Периферийные устройства | Съемные машинные носители информации | Обрабатываемые, хранимые данные |
| Администратор информационной системы | F | F | - | - | F | P/S | - | - |
| Ответственный за защиту информации | F | F | F | F | F | P/S | F | F |
| Пользователь | R-E | - | - | - | R-E | P/S | F | F |

**Типы доступа:**

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) - субъекту доступа разрешено сканирование;
- полный (F) - субъект доступа имеет полный доступ к объектам доступа.

Приложение № 2 к Положение о разрешительной системе доступа к ресурсам информационных систем

**Журнал учета пользователей абонентского пункта информационной системы**

| № п/п | Фамилия имя отчество | Должность | Информационная система | Имя компьютера (или домен)/ учетная запись | Типовая роль | Создан/ Удален | Дата создания/ удаления | Подпись администратора |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Приложение № 12
к приказу от 09.06.2025 г. № 250-ОД

# ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Настоящая Политика конфиденциальности персональной информации (далее – Политика) разработана в целях соблюдения требований статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и регулирует правоотношения по обработке персональной информации между Пользователем сайта https://sportptz.ru (далее – Сайт) сети «Интернет» и Администрацией сайта.

Использование Сайта означает безоговорочное согласие Пользователя с настоящей Политикой и указанными в ней условиями обработки его персональной информации. В случае несогласия с этими условиями Пользователь должен воздержаться от использования Сайта.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Основные понятия, используемые в Политике:

1.1.1. «Администрация сайта» – Муниципальное бюджетное учреждение Петрозаводского городского округа «Дирекция спортивных сооружений и спортивной подготовки» (ОГРН 1141001009270, ИНН 1001286516, КПП 100101001, адрес: 185035, Республика Карелия, г. Петрозаводск, Неглинская наб., 52).

1.1.2. «Персональная информация» Пользователя.

Персональная информация, которую Пользователь предоставляет о себе самостоятельно в процессе использования Сайта, включая персональные данные Пользователя. Обязательная для предоставления информация помечена специальным образом. Иная информация предоставляется Пользователем на его усмотрение. В число персональных данных Пользователя входят данные, которые Пользователь может предоставить о себе: фамилия, имя, отчество; номер телефона; адрес электронной почты; иная информация, указываемая самостоятельно Пользователем на Сайте.

Данные, которые автоматически передаются сервисам Сайта в процессе их использования с помощью установленного на устройстве Пользователя программного обеспечения, в том числе IP-адрес, данные файлов cookie, информация о браузере Пользователя (или иной программе, с помощью которой осуществляется доступ к сервисам), технические характеристики оборудования и программного обеспечения, используемых Пользователем, дата и время доступа к сервисам, адреса запрашиваемых страниц и иная подобная информация.

1.1.3. «Автоматизированная обработка персональных данных» – обработка персональных данных с помощью средств вычислительной техники.

1.1.4. «Блокирование персональных данных» – временное прекращение обработки персональных данных (за исключением случаев, если обработка

необходима для уточнения персональных данных).

1.1.5. «Информационная система персональных данных» — совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств.

1.1.6. «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), блокирование, удаление, уничтожение персональных данных.

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

1.1.8. «Уничтожение персональных данных» – любые действия, в результате которых персональные данные уничтожаются безвозвратно с невозможностью дальнейшего восстановления содержания персональных данных в информационной системе персональных данных и (или) уничтожаются материальные носители персональных данных.

1.2. Настоящая Политика конфиденциальности применяется только к Сайту https://sportptz.ru. Сайт не контролирует и не несет ответственности за сайты третьих лиц, на которые Пользователь может перейти по ссылкам, доступным на Сайте.

## 2. ЦЕЛЬ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЕЙ

2.1. Сайт собирает и хранит только ту персональную информацию, которая необходима для предоставления сервисов или исполнения соглашений и договоров с Пользователем, за исключением случаев, когда законодательством предусмотрено обязательное хранение персональной информации в течение определенного законом срока.

2.2. Персональную информацию Пользователя Сайт обрабатывает с целью осуществления гражданско-правовых отношений, в том числе подготовки, заключения и исполнения гражданско-правовых договоров.

2.3. Правовыми основаниями обработки Персональной информации Пользователя Сайта является согласие Пользователя на обработку его персональных данных.

## 3. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЕЙ. РЕАЛИЗУЕМЫЕ ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Сайт хранит персональную информацию Пользователей в соответствии с внутренними регламентами Администрации сайта.

3.2. В отношении персональной информации Пользователя сохраняется ее конфиденциальность.

3.3. Сайт вправе передать персональную информацию Пользователя третьим лицам в следующих случаях:

3.3.1. Пользователь выразил согласие на такие действия.

3.3.2. Передача необходима для использования Пользователем определенного сервиса либо для исполнения определенного соглашения или договора с Пользователем.

3.3.3. Передача предусмотрена законодательством в рамках установленной законодательством процедуры.

3.4. Обработка персональных данных Пользователя осуществляется любым законным способом, в том числе в информационных системах персональных данных с использованием средств автоматизации или без использования таких средств. Обработка персональных данных Пользователей осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3.5. При утрате или разглашении персональных данных Администрация сайта информирует Пользователя об утрате или разглашении персональных данных.

3.6. Администрация сайта принимает необходимые организационные и технические меры для защиты персональной информации Пользователя от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий третьих лиц, в том числе реализует следующие требования к защите персональных данных:

3.6.1. назначение ответственного за организацию обработки персональных данных;

3.6.2. издание документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3.6.3. осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике в отношении обработки персональных данных, локальным актам оператора;

3.6.4. оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

3.6.5. ознакомление работников, непосредственно осуществляющих

обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных работников;

3.6.6. определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

3.6.7. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3.6.8. применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

3.6.9. учет машинных носителей персональных данных;

3.6.10. обнаружение фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

3.6.11. восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

3.6.12. установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

3.6.13. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

3.6.14. применение для уничтожения персональных данных прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации.

3.7. Срок обработки персональных данных Пользователя: с момента предоставления согласия до момента его отзыва в письменной форме или прекращения договора.

После достижения цели обработки персональных данных Администрация сайта прекращает обработку персональных данных (обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Администрации сайта) и уничтожает персональные данные (обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом,

действующим по поручению Администрация сайта) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Пользователь, иным соглашением между Администрацией сайта и Пользователем либо если Администрация сайта не вправе осуществлять обработку персональных данных без согласия Пользователя на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

3.8. Пользователь вправе изменить свои персональные данные на Сайте или потребовать их удаления, направив электронное письмо по адресу: sk-lumi@mail.ru.

## 4. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Администрация сайта не осуществляет трансграничную передачу персональных данных.

## 5. ОБЯЗАТЕЛЬСТВА СТОРОН

5.1. Пользователь обязан:

5.1.1. Предоставить информацию о персональных данных, необходимую для пользования Сайтом.

5.1.2. Обновлять, дополнять предоставленную информацию о персональных данных в случае изменения данной информации.

5.2. Администрация сайта обязана:

5.2.1. Использовать полученную информацию исключительно для цели, указанной в настоящей Политике конфиденциальности.

5.2.2. Обеспечить хранение конфиденциальной информации в тайне, не разглашать без предварительного письменного разрешения Пользователя, а также не осуществлять продажу, обмен, опубликование либо разглашение иными возможными способами переданных персональных данных Пользователя.

5.2.3. Принимать меры предосторожности для защиты конфиденциальности персональных данных Пользователя согласно порядку, обычно используемому для защиты такого рода информации в существующем деловом обороте.

5.2.4. Осуществить блокирование персональных данных, относящихся к соответствующему Пользователю, с момента обращения или запроса Пользователя или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных на период проверки в случае выявления недостоверных персональных данных или неправомерных действий.

## 6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Администрация сайта, не исполнившая свои обязательства, несет ответственность за убытки, понесенные Пользователем в связи с неправомерным использованием персональных данных, в соответствии

с законодательством Российской Федерации.

6.2. В случае утраты или разглашения конфиденциальной информации Администрация сайта не несет ответственности, если данная конфиденциальная информация:

6.2.1. Стала публичным достоянием до ее утраты или разглашения.

6.2.2. Была получена от третьей стороны до момента ее получения Администрацией сайта.

6.2.3. Была разглашена с согласия Пользователя.

## 7. РАЗРЕШЕНИЕ СПОРОВ

7.1. До обращения в суд с иском по спорам, возникающим из отношений между Пользователем Сайта и Администрацией сайта, обязательным является предъявление претензии (письменного предложения о добровольном урегулировании спора).

7.2. Получатель претензии в течение 10 дней со дня получения претензии письменно уведомляет заявителя претензии о результатах рассмотрения претензии.

7.3. При недостижении соглашения спор будет передан на рассмотрение в суд в соответствии с действующим законодательством Российской Федерации.

7.4. К настоящей Политике конфиденциальности и отношениям между Пользователем и Администрацией сайта применяется действующее законодательство Российской Федерации.

## 8. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

8.1. Администрация сайта вправе вносить изменения в настоящую Политику конфиденциальности без согласия Пользователя.

8.2. Новая Политика конфиденциальности вступает в силу с момента ее размещения на Сайте, если иное не предусмотрено новой редакцией Политики конфиденциальности. Политика действует бессрочно до замены ее новой Политикой.

8.3. Все предложения или вопросы по настоящей Политике конфиденциальности следует направлять по адресу: sk-lumi@mail.ru.

8.4. Действующая Политика конфиденциальности размещена на Сайте по адресу: https://sportptz.ru сети «Интернет».