УТВЕРЖДАЮ
Директор
ГАУ КО «Дирекция спортсооружений»

_____ Е.В. Филиппова
«___» _____ 2022 г.

м.п.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
государственного автономного учреждения Калининградской области «Дирекция спортивных сооружений»

Настоящая Политика информационной безопасности (далее – Политика) **государственного автономного учреждения Калининградской области «Дирекция спортивных сооружений»** (далее – Учреждение) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и является официальным документом.

Политика разработана в соответствии с требованиями:

- Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания 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 защищённости»;
- Гражданского кодекса Российской Федерации;

- Устава государственного автономного учреждения Калининградской области «Дирекция спортивных сооружений», утвержденного приказом заместителя Председателя Правительства Калининградской области – министра спорта Калининградской области от 22 ноября 2021 г. № 167.

В Политике определены требования к работникам Учреждения, допущенным для работы в информационных системах персональных данных (далее – ИСПДн), степень ответственности таких работников, структура и необходимый уровень защищенности ИСПДн Учреждения, статус и обязанности работников, ответственных за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн Учреждения.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является:

а) обеспечение безопасности объектов защиты Учреждения от всех видов угроз (внешних, внутренних; умышленных, непреднамеренных);

б) минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее – УБПДн).

Безопасность ПДн, обрабатываемых в Учреждении, достигается путем исключения несанкционированного, в том числе случайного доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей Учреждения (работников, допущенных для выполнения своих должностных обязанностей в информационных системах персональных данных).

Информация, размещаемая на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» без согласия субъекта персональных данных, не превышает перечня персональных данных, разрешенного для открытого опубликования, установленного нормативными правовыми актами Российской Федерации. Размещение дополнительной информации о субъектах персональных данных, выходящей за рамки перечня информации, разрешенной для открытого опубликования, производится только при письменном согласии субъекта персональных данных. Распространение персональных данных субъекта персональных данных неограниченному кругу лиц осуществляется с согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

В Учреждении осуществляется своевременное обнаружение и реагирование на УБПДн и предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты, перечень ПДн, обрабатываемых в ИСПДн и подлежащих защите, утверждается приказом директора Учреждения.

Настоящая Политика утверждена директором Учреждения.

Требования настоящей Политики распространяются на всех работников Учреждения, а также иных лиц, взаимодействующих с Учреждением.

2. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (далее – СЗПДн) Учреждения строится на основании:

- перечня персональных данных, подлежащих защите;
- актов обследования по результатам обследования информационных систем персональных данных;
- частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- актов определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных;
- локальных актов (приказов, распоряжений) по Учреждению;
- организационно-распорядительной документации, относящейся к системе защиты информации и персональных данных Учреждения;
- руководящих и нормативных документов Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора);
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения.

На основании анализа актуальных угроз безопасности ПДн, описанных в частных моделях угроз безопасности персональных данных, технических заданиях на разработку СЗПДн, делается заключение о необходимости использования технических средств и проведения организационных мероприятий для обеспечения безопасности ПДн Учреждения.

Избранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению безопасности информации и персональных данных.

План мероприятий по обеспечению безопасности информации и персональных данных утверждается приказом директора Учреждения.

В Учреждении, для ИСПДн, которые относятся к государственным информационным системам, проводятся мероприятия по аттестации ИСПДН требованиям безопасности информации.

При проведении работ в актах обследования составляется перечень используемых технических средств, программного обеспечения, участвующего в обработке ПДн на всех элементах ИСПДн, включающих в себя:

а) перечень основных технических средств и систем (далее – ОТСС);

б) перечень программного обеспечения, используемого в ИСПДн;

в) перечень работников Учреждения, допущенных для работы в соответствующей ИСПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз СЗПДн может включать следующие технические средства защиты информации (далее – ТСЗИ):

а) антивирусные средства для рабочих мест пользователей и серверов;

б) средства защиты информации от несанкционированного доступа;

в) средства межсетевого экранирования;

г) средства криптографической защиты информации, используемые при передаче защищаемой информации по открытым каналам связи (далее – СКЗИ).

Список используемых ТСЗИ отражается в «Журнале учета средств защиты информации». Список ТСЗИ должен поддерживаться в актуальном состоянии, а при изменении состава ТСЗИ соответствующие изменения должны быть внесены в журнал.

Список используемых СКЗИ отражается в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов». Список СКЗИ должен поддерживаться в актуальном состоянии, а при изменении состава СКЗИ соответствующие изменения должны быть внесены в журнал.

3. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДн

СЗПДн Учреждения включает в себя следующие подсистемы:

а) управления доступом, регистрацией и учетом;

б) обеспечения целостности и доступности;

в) антивирусной защиты;

г) криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от определенных уровней защищенности ИСПДн, определенных в актах определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных Учреждения.

4. ПОЛЬЗОВАТЕЛИ ИСПДн

Пользователи – работники Учреждения, осуществляющие обработку персональных данных.

Перечень пользователей, допущенных до работы с ПДн, уровень их доступа и информированности утверждаются директором Учреждения.

Пользователи имеют доступ к обработке ПДн, которая включает в себя: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн.

Пользователи не имеют полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователи ИСПДн обладают следующими уровнями доступа и знаний:

а) обладают всеми необходимыми знаниями для работы с ПДн;

б) имеют личный идентификатор (логин) и аутентификатор (пароль).

5. ТРЕБОВАНИЯ К РАБОТНИКАМ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

Все работники Учреждения, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдать принятый режим безопасности ПДн, а также быть ознакомленными с руководящими документами по информационной безопасности Учреждения.

При вступлении в должность нового работника, ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных Учреждения (далее – Ответственный) знакомит указанного работника с необходимыми документами, регламентирующими требования по защите ПДн, а также обучает его правилам работы с ПДн в ИСПДн.

Работники Учреждения под роспись знакомятся с должностными инструкциями, организационно-распорядительной документацией, относящейся к системе защиты ПДн Учреждения, настоящей Политикой, принятыми процедурами работы с элементами ИСПДн и СЗПДн, а также с Положением об обработке и защите персональных данных Учреждения.

Работники Учреждения, использующие технические средства аутентификации, в обязательном порядке обеспечивают сохранность идентификаторов (электронных ключей) и не допускают несанкционированного доступа (далее – НСД) к ним, исключают возможность их утери и вероятность использования третьими лицами.

Работники Учреждения проинструктированы о необходимости следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники Учреждения ознакомлены с правилами обеспечения надлежащей защиты оборудования ИСПДн, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Работники Учреждения как пользователи ознакомлены с требованиями по безопасности ПДн и процедурами защиты оборудования ИСПДн, оставленного без присмотра, а также знают свои обязанности по обеспечению такой защиты.

Работники Учреждения ознакомлены с требованиями обеспечения отсутствия возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест (далее – АРМ) или терминалов при работе с ПДн.

Работники Учреждения ознакомлены с правилами защиты АРМ с помощью блокировки **(комбинация Ctrl+Alt+Del, далее Блокировка компьютера; комбинация клавиш Win+L)** при завершении работы с ПДн.

Работники Учреждения проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

Работники Учреждения ознакомлены с дисциплинарными взысканиями при нарушении требований безопасности работы с ПДн в соответствии с действующим федеральным законодательством Российской Федерации в области защиты информации и персональных данных.

Контроль по соблюдению режима безопасности обработки ПДн возложен на Ответственного в соответствии с приказом директора Учреждения.

Работники Учреждения, допущенные к работам с техническими и криптографическими средствами защиты информации, проходят обучение по правилам работы, хранения и учета технических и криптографических средств защиты информации. Обучение проводит Ответственный.

Допуск работников Учреждения к работе со средствами криптографической защиты информации происходит на основании приказа директора Учреждения.

Работники Учреждения под роспись знакомятся с инструкциями, правилами, руководствами, принятыми процедурами работы с установленными средствами криптографической защиты информации.

Работники Учреждения, использующие средства криптографической защиты информации, в обязательном порядке обеспечивают их сохранность и не допускают НСД к ним, исключают возможность их утери и вероятность использования третьими лицами.

Работники Учреждения обязаны без промедления сообщать директору Учреждения и Ответственному обо всех случаях работы в ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам Учреждения **ЗАПРЕЩАЕТСЯ:**

а) устанавливать стороннее программное обеспечение;

б) подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию;

в) разглашать защищаемую информацию, которая стала им известна при работе в ИСПДн Учреждения, третьим лицам.

6. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ РАБОТНИКОВ (ПОЛЬЗОВАТЕЛЕЙ ИСПДн)

Должностные обязанности пользователей ИСПДн Учреждения описаны в следующих организационно-распорядительных документах:

- руководстве ответственного за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных;
- руководстве администратора информационной безопасности;
- руководстве пользователя;
- инструкции по организации режима доступа в помещения, о порядке действий при несанкционированном проникновении в помещения и других нештатных ситуациях;
- инструкции по использованию средств криптографической защиты ифнормации;
- правилах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- положении об обработке и защите персональных данных Учреждения;
- должностных инструкциях работников Учреждения.

7. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ, ОБРАБАТЫВАЮЩИХ ПДн В ИСПДн

Директор Учреждения назначает ответственного за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных.

Ответственный получает указания непосредственно от директора Учреждения и подотчетен ему.

Ответственный обязан:

а) осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

б) доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальные акты по вопросам обработки персональных данных (приказы, руководства, инструкции), требования к защите персональных данных;

в) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Работники Учреждения ознакомлены с тем, что:

- моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации;
- возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков;
- лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Для решения вопросов по расследованию инцидентов информационной безопасности, возникших при обработке ПДн и другой конфиденциальной информации, уничтожения документов, содержащих персональные данные, в Учреждении создается комиссия.

Состав комиссии утверждается приказом директора Учреждения. В состав комиссии включается Ответственный.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных, изложена в:

а) Кодексе об административных правонарушениях Российской Федерации (КоАП РФ) – статьи **5.27, 5.39, 13.11-13.14, 19.4-19.7, 19.20, 20.25, 32.2**;

б) Уголовном кодексе Российской Федерации (УК РФ) – статьи **137, 140, 155, 183, 272, 273, 274, 292, 293**;

в) Трудовом кодексе Российской Федерации (ТК РФ) – статьи **81, 90, 195, 237, 391**.

8. РАЗМЕЩЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОФИЦИАЛЬНОМ САЙТЕ УЧРЕЖДЕНИЯ

Учреждение, в соответствии с законодательством Российской Федерации, имеет право размещать на официальном сайте Учреждения, находящимся по адресу: **https://www.gaudss.ru**, следующие персональные данные без письменного согласия субъекта персональных данных:

- сведения о директоре Учреждения, его заместителях;
- сведения о руководителях структурных подразделений (при их наличии);
- сведения о персональном составе работников (с указанием, с их согласия, уровня образования, квалификации и опыта работы);
- иную информацию, которая размещается, опубликовывается по решению Учреждения, и (или) размещение, опубликование которой является обязательным в соответствии с законодательством Российской Федерации.

Опубликование сведений о субъекте персональных данных (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) производится только после получения письменного согласия, за исключением информации, размещение и опубликование которой является обязательным в соответствии с законодательством Российской Федерации, от субъекта персональных данных или его законного представителя, с указанием в согласии перечня персональных данных, которые будут опубликованы на официальном сайте Учреждения.

Учреждение имеет право размещать изображения субъекта персональных данных на официальном сайте (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) без согласия субъекта в случаях, когда:

- использование изображения осуществляется в государственных, общественных или иных публичных интересах;
- изображение субъекта персональных данных получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;
- субъект персональных данных позировал за плату.

Публикация персональных данных субъекта персональных данных, для неограниченного круга лиц, производится Учреждением только после получения у субъекта персональных данных согласия, в котором субъект персональных данных однозначно определил категории своих персональных данных, предназначенных для распространения неограниченному кругу лиц.

За нарушение требований по размещению сведений о субъекте персональных данных в сетях общего доступа Учреждение несет ответственность в соответствии с нормативными правовыми актами Российской Федерации, перечисленными в разделе 7 настоящей Политики.