**УТВЕРЖДАЮ**
Директор
ГБУ КО «СШ по силовым видам спорта»
_____ М.Ю. Смоляков
«05» марта 2022 г.

# ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
## государственного бюджетного учреждения Калининградской области «Спортивная школа по силовым видам спорта»

Настоящая Политика информационной безопасности (далее – Политика) **государственного бюджетного учреждения Калининградской области «Спортивная школа по силовым видам спорта»** (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»;
- Гражданского кодекса Российской Федерации;
- Устава государственного бюджетного учреждения Калининградской области «Спортивная школа по силовым видам спорта»;
- Изменения в устав государственного бюджетного учреждения Калининградской области «Спортивная школа по силовым видам спорта» от 13 декабря 2021 г.

В Политике определены требования к работникам Учреждения, допущенным для работы с материальными носителями содержащие персональные данные (далее – материальные носители), степень ответственности таких работников, структура и необходимый уровень защищенности мест хранения материальных носителей в Учреждении, статус и обязанности работников, ответственных за обеспечение безопасности материальных носителей в Учреждении.

## 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 работников Учреждения допущенных для выполнения своих должностных обязанностей с материальными носителями (далее – работники).

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 Учреждении 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. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Защита персональных данных (далее – ЗПДн) Учреждения строится на основании:

- перечня персональных данных, подлежащих защите;
- локальных актов (приказов, распоряжений) Учреждения;
- организационно-распорядительной документации, относящейся к защите информации и ПДн в Учреждении;
- руководящих и нормативных документов Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязи России);
- руководящих и нормативных документов Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Управление Роскомнадзора Российской Федерации);
- руководящих документов ФСТЭК и ФСБ России.

На основании анализа актуальных угроз безопасности ПДн, делается заключение о необходимости проведения организационных мероприятий для обеспечения безопасности ПДн в Учреждении.

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

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

## 3. ТРЕБОВАНИЯ К РАБОТНИКАМ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

Все работники Учреждения, осуществляющие работу с материальными носителями, 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 такого работника с необходимыми документами, регламентирующими требования по защите ПДн, а также, обучает его правилам работы с ПДн.

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

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

Работники Учреждения проинструктированы о необходимости следовать установленным процедурам поддержания режима безопасности ПДн.

Работники Учреждения ознакомлены с правилами обеспечения надлежащей защиты материальных носителей, оставляемых без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Работники Учреждения ознакомлены с требованиями обеспечения отсутствия возможности просмотра материальных носителей третьими лицами при работе 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 обязаны без промедления сообщать директору Учреждения, Ответственному обо всех попытках несанкционированного доступа, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам Учреждения **ЗАПРЕЩАЕТСЯ:**

а) производить несанкционированное копирование носителей ПДн;

б) производить модификацию и уничтожение ПДн без разрешения Ответственного;

в) разглашать защищаемую информацию, которая стала им известна при работе с материальными носителями в Учреждении, третьим лицам.

## 4. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ РАБОТНИКОВ

Должностные обязанности работников Учреждения описаны в следующих организационно-распорядительных документах:

- руководстве ответственного за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных;
- руководстве пользователя;
- инструкции по организации режима доступа в помещения, о порядке действий при несанкционированном проникновении в помещения и других нештатных ситуациях;
- 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.

## 5. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ, ОБРАБАТЫВАЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

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, локальных актов по вопросам обработки персональных данных (распоряжений, инструкций); 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 должен включаться 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**.