Муниципальное бюджетное учреждение дополнительного образования «Спортивная школа по киокусинкай»

140404, МО, Г.о. Коломна, ул. Девичье поле д.1, пом.1Б
8-496-618-32-36 Scool-Kyokushin@yandex.ru

ПРИКАЗ

№ 12 от 03.02.2025 г.

«Об утверждении локальных нормативных актов в области политики обработки персональных данных МБУ ДО «СШ по киокусинкай»

В целях приведения в соответствие обработку персональных данных в МБУ ДО «СШ по киокусинкай»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые локальные акты:

1.1. Положение об определении угроз безопасности персональных данных актуальных, при обработке персональных данных в информационных системах персональных данных в МБУ ДО «СШ по киокусинкай» (Приложение 1);

1.2. Политика информационной безопасности МБУ ДО «СШ по киокусинкай» (Приложение 2);

1.3. Инструкция о порядке физической охраны помещений, содержащих носители персональных данных в МБУ ДО «СШ по киокусинкай» (Приложение 3);

1.4. Положение о защите, хранении, обработке, и передаче персональных данных работников и обучающихся МБУ ДО «СШ по киокусинкай» (Приложение 4);

1.5. План мероприятий по внутреннему контролю за соблюдением безопасности персональных данных в МБУ ДО «СШ по киокусинкай» (Приложение 5);

1.6. Положение о комиссии по классификации информационных систем персональных данных в МБУ ДО «СШ по киокусинкай» (Приложение 6);

1.7. Положение о защите персональных данных работников муниципального бюджетного учреждения дополнительного образования «Спортивная школа по киокусинкай» (Приложение 7);

1.8. Перечень информационных систем персональных данных МБУ ДО «СШ по киокусинкай» (Приложение 8);

1.9. Положение об обработке и защите персональных данных обучающихся и их родителей (законных представителей) в МБУ ДО «СШ по киокусинкай» (Приложение 9);

1.10. Порядок уничтожения и обезличивания персональных данных в МБУ ДО «СШ по киокусинкай» (Приложение 10);

1.11. Журнал регистрации и учета обращений субъектов персональных данных (Приложение 11);

1.12. Журнал учета передачи персональных данных (Приложение 12);

1.13. Журнал учета съемных носителей персональных данных (Приложение 13);

1.14. Журнал учета машинных носителей персональных данных (Приложение 14);

1.15. Журнал уничтожения носителей персональных данных (Приложение 15);

1.16. Журнал антивирусных проверок (Приложение 16).

2. Контроль за исполнением приказа оставляю за собой.

И.о директора

МБУ ДО «СШ по киокусинкай » С.И. Масуфранов

Приложение №1
к приказу №12 от 03.02.25г.

Положение

об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в МБУ ДО «СШ по киокусинкай»

«

Настоящее положение об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных школы разработано в соответствии с Конституцией РФ, Федеральным законом от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации", частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Уставом школы.

1. Общие положения.

1.1. Угрозы безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в школе (далее - Актуальные угрозы безопасности ИСПДн), определены в соответствии с **частью 5 статьи 19** Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", **постановлением** Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", **приказом** Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", **приказом** ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", **приказом** Федеральной службы безопасности Российской Федерации (далее - ФСБ России) от 10.07.2014 N 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 уровнейзащищенности", **Методикой** определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008, **Методическими рекомендациями** по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждёнными руководством 8-го Центра ФСБ России от 31.03.2015 N 149/7/2/6-432, **Базовой моделью** угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008, и Банком данных угроз безопасности информации, размещенным на официальном сайте ФСТЭК России (**http://bdu.fstec.ru**).

1.2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) школы.

1.3.Актуальные угрозы безопасности ИСПДн подлежат адаптации в ходе разработки органами власти частных моделей угроз безопасности персональных данных для каждой информационной системы (далее - ИС).

1.4.При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик ИС, эксплуатируемой при осуществлении школой функций и полномочий, а
также применяемых в ней информационных технологий и особенностей ее функционирования, в том числе с использованием Банка данных угроз безопасности информации.

1.5.В частной модели угроз безопасности персональных данных указываются:
описание ИСПДн и ее структурно-функциональных характеристик; описание угроз безопасности персональных данных с учетом
совокупности предположений о способах, подготовке и проведении атак; описание возможных уязвимостей ИС, способов реализации угроз
безопасности информации и последствий нарушений безопасности информации.

1.6.Объектами информатизации в школе выступают ИС, имеющие сходную структуру и одноточечное подключение к сетям общего пользования и (или) информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") через выделенную инфраструктуру - межведомственную сеть передачи данных Московской области.

1.7.Базы данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение) персональных данных граждан Российской Федерации, находятся на территории Российской Федерации.

1.8.Ввод персональных данных в ИС и вывод данных из ИС осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и оптические диски. Доступ к
ИСПДн ограничен перечнем сотрудников школы, являющихся владельцем ИС.

1.9.Передача персональных данных в другие организации и в территориальные органы федеральных органов исполнительной власти по сетям общего пользования и (или) сети "Интернет" осуществляется с использованием сертифицированных шифровальных (криптографических) средств защиты информации (далее - СКЗИ).

1.10. Контролируемой зоной ИС являются административные здания колледжа. В пределах контролируемой зоны находятся рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИС. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям общего пользования и (или) сети "Интернет".

1.11. В зданиях спортивной школы:

должен быть организован пропускной режим;
должно быть исключено неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники;
помещения со средствами вычислительной техники должны быть оборудованы запирающимися дверями;
дополнительно может быть организовано видеонаблюдение в коридорах, вестибюлях и холлах.

1.12. Защита персональных данных в ИС школы и сетях общего пользования, подключаемых к сети "Интернет", обеспечивается средствами защиты информации (далее - СЗИ):
СЗИ от несанкционированного доступа, сертифицированными ФСТЭК России, не ниже 4 уровня контроля отсутствия недекларированных возможностей (далее - НДВ);

средствами антивирусной защиты, сертифицированными ФСТЭК России, не ниже 4 класса;
межсетевыми экранами, сертифицированными ФСТЭК России, не ниже 3 класса;
СКЗИ, формирующими виртуальные частные сети (VPN), сертифицированными ФСБ России по классу КС 1 и выше;
системами обнаружения вторжения не ниже 4 класса;
средством государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Характеристики безопасности информационных систем персональных данных.

2.1. Основными свойствами безопасности информации являются:
конфиденциальность - 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;
целостность - состояние защищенности информации, характеризуемое способностью ИС обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения;
доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.
2.2. 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 ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.
2.3. В зависимости от состава обрабатываемых персональных данных и типа актуальных угроз необходимый уровень защищенности персональных данных для каждой ИСПДн определяется индивидуально.
2.4. Для ИСПДн органов власти актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием НДВ в системном и прикладном программном обеспечении (далее - ПО), используемом в ИС.

3. Применение средств криптографической защиты информации в информационных системах персональных данных.

3.1. Актуальность применения в ИСПДн органов власти СКЗИ определяется необходимостью защиты персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сети "Интернет".
3.2. СКЗИ предназначены для защиты информации от действий со стороны лиц, не имеющих право доступа к этой информации.
3.3. Принятыми организационно-техническими мерами в колледже должна быть исключена возможность несанкционированного доступа потенциального нарушителя к ключевой информации СКЗИ.
3.4. При эксплуатации СКЗИ должны соблюдаться требования эксплуатационно-технической документации на СКЗИ и требования

действующих нормативных правовых актов в области реализации и эксплуатации СКЗИ.

3.5. Для обеспечения безопасности персональных данных при их обработке в ИСПДн используются СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

3.6. Объектами защиты в ИСПДн являются:

персональные данные;

средства криптографической защиты информации; среда функционирования СКЗИ (далее - СФ);

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную информацию и аутентифицирующую СКЗИ;

документы, дела, журналы, картотеки, издания, технические документы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

носители защищаемой информации, используемые в ИС в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

используемые информационной системой каналы (линии) связи, включая кабельные системы;

помещения, в которых находятся ресурсы ИС, имеющие отношение к криптографической защите персональных данных.

3.7. Реализация угроз безопасности персональных данных, обрабатываемых в ИСПДн, определяется возможностями источников атак. На основании исходных данных об объектах защиты и источниках атак в таблице 1 для школы определены обобщенные возможности источников атак.

Таблица 1

Обобщенные возможности источников атак	Да/Нет
1	2
1. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	Да
3. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и	Нет

среда их функционирования	
4. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

3.8.В соответствии с обобщенными возможностями источников атак (**таблица 1**) определены две актуальные уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы для ИС) (таблица 2).

Таблица 2

Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1	2	3
1. Проведение атаки при нахождении в пределах контролируемой зоны	Неактуально	Проводятся работы по подбору персонала; представители технических, обслуживающих других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах

		работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с надежными замками, обеспечено постоянное закрытие дверей помещений на замок, и их открытие осуществляется только для санкционированного прохода; утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также внештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные несанкционированного (далее - НСД); СЗИ от доступа используются сертифицированные средства антивирусной защиты Проводятся
2. Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:	Неактуально	работы по подбору персонала; документация на СКЗИ хранится у ответственного за СКЗИ в документацию на металлическом сейфе; помещения, в которых	

СФ; помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе средств вычислительной техники (далее - СВТ) и СФ		располагаются документация на СКЗИ, СКЗИ и компонент СФ, оснащены входными дверьми с надежными замкам обеспечено постоянное закрытие дверей помещений на замок, и их открытие осуществляется только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения
3. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Актуально	
4. Использование штатных ИСПДн, средств	Актуально	

ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
5. Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Неактуально	Проводятся работы по подбору персонала; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода
6. Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Неактуально	Проводятся работы по подбору персонала; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители обслуживающих технических, и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
7. Возможность обработка располагать сведениями, содержащимися в конструкторской документации на аппаратные и	Неактуально	Не осуществляется сведений, составляющих **государственную тайну**, а также иных сведений, которые могут представлять интерес для реализации возможности

программные компоненты СФ		
8. Возможность воздействовать на любые компоненты СКЗИ и СФ	Неактуально	Не осуществляется обработка сведений, составляющих **государственную тайну**, а также иных сведений, которые могут представлять интерес для реализации возможности

4. Определение актуальных угроз безопасности персональных данных в информационных системах персональных данных.

4.1.На основе проведенного анализа банка данных угроз безопасности информации (**www.bdu.fstec.ru**) с учётом структурно-функциональных характеристик типовых ИС, а также применяемых в них информационных технологий и особенностей функционирования, в ИС органов власти могут быть актуальны следующие угрозы безопасности ИСПДн:
УБИ.3 Угроза анализа криптографических алгоритмов и их реализации; УБИ.4 Угроза аппаратного сброса пароля BIOS;
УБИ.6 Угроза внедрения кода или данных;
УБИ.7 Угроза воздействия на программы с высокими привилегиями; УБИ.8 Угроза восстановления аутентификационной информации; УБИ.9 Угроза восстановления предыдущей уязвимой версии BIOS;
УБИ.12 Угроза деструктивного изменения конфигурации/среды окружения программ;
УБИ.13 Угроза деструктивного использования декларированного функционала BIOS;
УБИ.14 Угроза длительного удержания вычислительных ресурсов пользователями;
УБИ.15 Угроза доступа к защищаемым файлам с использованием обходного пути;
УБИ.16 Угроза доступа к локальным файлам сервера при помощи URL; УБИ.17 Угроза доступа/перехвата/изменения HTTP cookies;
УБИ.18 Угроза загрузки нештатной операционной системы; УБИ.19 Угроза заражения DNS-кеша;
УБИ.22 Угроза избыточного выделения оперативной памяти; УБИ.23 Угроза изменения компонентов системы;
УБИ.26 Угроза искажения XML-схемы;
УБИ.27 Угроза искажения вводимой и выводимой на периферийные устройства информации;
УБИ.28 Угроза использования альтернативных путей доступа к ресурсам; УБИ.30 Угроза использования информации идентификации/ аутентификации, заданной по умолчанию;

УБИ.31 Угроза использования механизмов авторизации для повышения привилегий;
УБИ.32 Угроза использования поддельных цифровых подписей BIOS; УБИ.33 Угроза использования слабостей кодирования входных данных; УБИ.34 Угроза использования слабостей протоколов сетевого/ локального обмена данными;
УБИ.36 Угроза исследования механизмов работы программы; УБИ.37 Угроза исследования приложения через отчёты об ошибках;
УБИ.39 Угроза исчерпания запаса ключей, необходимых для обновления BIOS;
УБИ.41 Угроза межсайтового скриптинга; УБИ.42 Угроза межсайтовой подделки запроса;
УБИ.45 Угроза нарушения изоляции среды исполнения BIOS; УБИ.49 Угроза нарушения целостности данных кеша;
УБИ.51 Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;
УБИ.53 Угроза невозможности управления правами пользователей BIOS; УБИ.59 Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;
УБИ.62 Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера;
УБИ.63 Угроза некорректного использования функционала программного обеспечения;
УБИ.67 Угроза неправомерного ознакомления с защищаемой информацией; УБИ.68 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
УБИ.69 Угроза неправомерных действий в каналах связи;
УБИ.71 Угроза несанкционированного восстановления уда лённой защищаемой информации;
УБИ.72 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;
УБИ.74 Угроза несанкционированного доступа к аутентификационной информации;
УБИ.86 Угроза несанкционированного изменения аутентификационной информации;
УБИ.87 Угроза несанкционированного использования привилегированных функций BIOS;
УБИ.88 Угроза несанкционированного копирования защищаемой информации;
УБИ.89 Угроза несанкционированного редактирования реестра;
УБИ.90 Угроза несанкционированного создания учётной записи пользователя;
УБИ.91 Угроза несанкционированного удаления защищаемой информации; УБИ.93 Угроза несанкционированного управления буфером;

УБИ.94 Угроза несанкционированного управления синхронизацией и состоянием;
УБИ.95 Угроза несанкционированного управления указателями;
УБИ.98 Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
УБИ.99 Угроза обнаружения хостов;
УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации;
УБИ.102 Угроза опосредованного управления группой программ через совместно используемые данные;
УБИ.103 Угроза определения типов объектов защиты; УБИ.104 Угроза определения топологии вычислительной сети; УБИ.107 Угроза отключения контрольных датчиков;
УБИ.109 Угроза перебора всех настроек и параметров приложения; УБИ.111 Угроза передачи данных по скрытым каналам;
УБИ.113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;
УБИ.114 Угроза переполнения целочисленных переменных;
УБИ.115 Угроза перехвата вводимой и выводимой на периферийные устройства информации;
УБИ.116 Угроза перехвата данных, передаваемых по вычислительной сети; УБИ.117 Угроза перехвата привилегированного потока;
УБИ.118 Угроза перехвата привилегированного процесса; УБИ.121 Угроза повреждения системного реестра; УБИ.122 Угроза повышения привилегий;
УБИ.123 Угроза подбора пароля BIOS;
УБИ.124 Угроза подделки записей журнала регистрации событий; УБИ.127 Угроза подмены действия пользователя путём обмана; УБИ.128 Угроза подмены доверенного пользователя;
УБИ.129 Угроза подмены резервной копии программного обеспечения BIOS; УБИ.130 Угроза подмены содержимого сетевых ресурсов;
УБИ.131 Угроза подмены субъекта сетевого доступа;
УБИ.132 Угроза получения предварительной информации об объекте защиты;
УБИ.139 Угроза преодоления физической защиты;
УБИ.140 Угроза приведения системы в состояние "отказ в обслуживании";
УБИ.143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ.144 Угроза программного сброса пароля BIOS;
УБИ.145 Угроза пропуска проверки целостности программного обеспечения; УБИ.149 Угроза сбоя обработки специальным образом изменённых файлов; УБИ.152 Угроза удаления аутентификационной информации;
УБИ.153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

УБИ.154 Угроза установки уязвимых версий обновления программного обеспечения BIOS; УБИ.155 Угроза утраты вычислительных ресурсов; УБИ.156 Угроза утраты носителей информации;
УБИ.157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ.158 Угроза форматирования носителей информации; УБИ.159 Угроза "форсированного веб-браузинга";
УБИ.160 Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ.162 Угроза эксплуатации цифровой подписи программного кода; УБИ.163 Угроза перехвата исключения/сигнала из привилегированного блока функций;
УБИ.167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;
УБИ.168 Угроза "кражи" учётной записи доступа к сетевым сервисам; УБИ.170 Угроза неправомерного шифрования информации;
УБИ.171 Угроза скрытного включения вычислительного устройства в состав бот-сети;
УБИ.172 Угроза распространения "почтовых червей"; УБИ.173 Угроза "спама" веб-сервера;
УБИ.174 Угроза "фарминга"; УБИ.175 Угроза "фишинга";
УБИ.176 Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;
УБИ.177 Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;
УБИ.178 Угроза несанкционированного использования системных и сетевых утилит;
УБИ.179 Угроза несанкционированной модификации защищаемой информации;
УБИ.180 Угроза отказа подсистемы обеспечения температурного режима;
УБИ.181 Угроза перехвата одноразовых паролей в режиме реального времени;
УБИ.182 Угроза физического устаревания аппаратных компонентов;
УБИ.183 Угроза перехвата управления автоматизированной системой управления технологическими процессами;
УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации;
УБИ.186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент;
УБИ.187 Угроза несанкционированного воздействия на средство защиты информации;
УБИ.189 Угроза маскирования действий вредоносного кода;

УБИ.190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;
УБИ.191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения;
УБИ.192 Угроза использования уязвимых версий программного обеспечения; УБИ.193 Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;
УБИ.197 Угроза хищения аутентификационной информации из временных файлов cookie;
УБИ.198 Угроза скрытной регистрации вредоносной программной учетных записей администраторов;
УБИ.201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;
УБИ.203 Угроза утечки информации с не подключенных к сети Интернет компьютеров;
УБИ.204 Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров;
УБИ.205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты.

4.2. Угрозами безопасности персональных данных при их обработке с использованием СКЗИ являются:

4.2.1. создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

4.2.2. создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ. К этапам жизненного цикла СКЗИ относятся: разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация;

4.2.3. проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона). Границей контролируемой зоны может быть: периметр охраняемой территории организации, ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения;

4.2.4. проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, в совокупности представляющие среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

4.2.5. проведение атак на этапе эксплуатации СКЗИ на: персональные данные;

ключевую, аутентифицирующую и парольную информацию СКЗИ; программные компоненты СКЗИ;

аппаратные компоненты СКЗИ;

программные компоненты СФ, включая программное обеспечение BIOS;

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

4.2.6. получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно- телекоммуникационную сеть "Интернет") информации об ИС, в которой используется СКЗИ. При этом может быть получена следующая информация:

общие сведения об ИС, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы ИС);

сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в ИС совместно с СКЗИ;

содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

4.2.7. применение находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

4.2.8. получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

сведений о физических мерах защиты объектов, в которых размещены ресурсы ИС;

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИС;

сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

4.2.9. использование штатных средств, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

Приложение №2
к приказу №12 от 03.02.25г.

ПОЛИТИКА
информационной безопасности МБУ ДО «СШ по киокусинкай»

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и
доступность персональных данных при их обработке в информационных системах персональных данных.

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

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функциональнораспределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту 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.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

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

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АВПО – антивирусной программное обеспечение
АРМ – автоматизированное рабочее место
ИСПДн – информационная система персональных данных
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
ТКУ И – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее Политика) МБУ ДО «СШ по киокусинкай» (далее Оператор) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями нормативных документов:

-Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями);

-Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденный Приказом ФСТЭК России от 18.02.2013г. № 21.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в МБУ ДО «СШ по киокусинкай».

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Оператора от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации УБПДн.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. Область действия

Требования настоящей Политики распространяются на всех сотрудников Оператора (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц.

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- перечня персональных данных;
- акта классификации информационных систем персональных данных;
- частной модели актуальных угроз и вероятного нарушителя;
- положения о разграничении прав доступа к персональным данным;
- нормативных документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Оператора. На основании анализа актуальных угроз безопасности ПДн описанного в Частной модели актуальных угроз и вероятного нарушителя, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по внутреннему контролю за соблюдением безопасности персональных данных.

Организационные мероприятия должны включать:

- правовое основание для сбора персональных данных;
- определение ответственных лиц за соблюдением мер безопасности;
- защиту персональных данных, обрабатываемых без средств автоматизации;
- защиту персональных данных, обрабатываемых с применением средств автоматизации;
- защиту объектов от хищения;
- защиту съемных накопителей, содержащих персональные данные;
- вопросы уничтожения персональных данных.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- защиты от несанкционированного доступа к персональным данным;
- антивирусной защиты для рабочих станций пользователей и серверов;
- межсетевого экранирования;
- криптографической защиты информации, при передаче защищаемой информации по каналам связи;
- средства защиты от утечки по ТКУИ.

4. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;

- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- контроля отсутствия недекларированных возможностей;
- криптографической защиты;
- защиты от утечки по ТКУИ.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн.

Подсистема управления доступом должна осуществлять:

- идентификацию и проверку подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

Подсистема регистрации и учета должна осуществлять:

- регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа.
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

Подсистема обеспечения целостности должна осуществлять:

- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- физическую охрану информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;
- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Межсетевое экранирование должно обеспечивать:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условнопостоянного действия;

- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- контроль целостности своей программной и информационной части;
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентированное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления; Защита от утечки видовой информации:
- размещение устройств вывода информации средств вычислительной техники информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).

5. Пользователи ИСПДн

В ИСПДн Оператора можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администраторы безопасности ИСПДн;
- пользователи ИСПДн;
- системные администраторы.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положении о разграничении прав доступа к персональным данным.

Администраторы безопасности ИСПДн:

Администратором безопасности является штатный сотрудник Оператора, ответственный за функционирование СЗПДн, назначается приказом директора.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;

- устанавливать доверительные отношения своей защищенной сети с другими защищенными сетями.

Пользователь ИСПДн

Пользователем ИСПДн является штатный сотрудник Оператора, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Системные администраторы:

Системным администратором может быть штатный сотрудник Оператора или лица сторонних организаций, осуществляющих свои функции на основании двухстороннего договора. Системный администратор не имеет полномочий для управления подсистемами обработки данных и безопасности.

Системный администратор обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Оператора, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Оператора, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Оператора, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Оператора обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Оператора должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7. Ответственность сотрудников

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администраторы безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Оператора – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приложение №3
к приказу №12 от 03.02.25г.

ИНСТРУКЦИЯ

о порядке физической охраны помещений, содержащих носители персональных данных в МБУ ДО «СШ по киокусинкай»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция о порядке физической охраны помещений, содержащих носители персональных данных (далее Инструкция) определяет обязанности должностных лиц (-далее Оператор) МБУ ДО «СШ по киокусинкай» по обеспечению безопасности носителей персональных данных.

1.2. Данная Инструкция разработана в соответствии с: Федеральным законом «О персональных данных»; Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

1.3. Обеспечение безопасности физической охраны помещений, содержащих носители персональных данных, является частью комплексной системы безопасности Оператора.

2.ПОРЯДОК ФИЗИЧЕСКОЙ ОХРАНЫ ПОМЕЩЕНИЙ, СОДЕРЖАЩИХ НОСИТЕЛИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Под носителями персональных данных (ПДн) в настоящей инструкции понимаются бумажные документы, содержащие ПДн, и элементы информационных систем персональных данных.

2.2. Помещения, содержащие носители персональных данных (далее Помещения), в нерабочее время должны быть закрыты на ключ и сданы на вахту.

2.3. В Помещения имеют допуск только лица, допущенные в установленном порядке к обработке ПДн. Возможность неконтролируемого проникновения или пребывания в этих Помещениях посторонних лиц должна быть исключена.

2.4. По окончании рабочего дня Помещение запирает и сдает на вахту работник, имеющий право доступа в Помещение.

2.5. В начале рабочего дня работник, имеющий право доступа в Помещение, перед вскрытием Помещения проверяет целостность и исправность дверных запоров. В случае обнаружения нарушений, указывающих на возможность проникновения в Помещение посторонних лиц, работник Помещение не вскрывает, а о случившемся незамедлительно сообщает администратору безопасности (АБ), который в свою очередь незамедлительно сообщает директору, составляет акт.

Приложение №4

к приказу №12 от 03.02.25г.

Положение о защите, хранении, обработке и передаче персональных данных работников и обучающихся МБУ ДО «СШ по киокусинкай»

1. Общие положения

1.1 Настоящее Положение определяет порядок защиты, хранение, обработки и передачи персональных данных работников и обучающихся, их родителей или законных представителей (далее - Субъекты персональных данных) МБУ ДО «СШ по киокусинкай» (далее - Оператор). Основанием для разработки данного локального нормативного акта являются: Конституция Российской Федерации; Гражданский кодекс Российской Федерации; Указ Президента Российской Федерации от 06 марта 1997 г. № 188 (ред. от 23 сентября 2005 г.) «Об утверждении перечня сведений конфиденциального характера»; Федеральный Закон от 04.12.2007 № 329-ФЗ «О физической культуре и спорте в Российской Федерации»; Федеральный закон Российской Федерации от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»; Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; и иные нормативно-правовые акты;

1.2 Целью настоящего Положения является определение порядка обработки персональных данных Субъектов персональных данных, обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным и защиту персональных данных.

1.3 Персональные данные Субъектов персональных данных относятся к категории конфиденциальной информации.

2. Основные понятия, используемые в настоящем Положении

Для целей настоящего Положения применяются следующие термины и определения:

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными, в данном случае – МБУ ДО «СШ по киокусинкай».

Субъект персональных данных - физические лица, родители (законные представители) обучающихся, работники, которые состоят в договорных и иных гражданско-правовых отношениях с Оператором по вопросам оказания услуг в сфере физической культуры и спорта, предусмотренных Уставом. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (Субъект персональных данных).

Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Документы, содержащие персональные данные – документы необходимые Оператору для обеспечения тренировочного процесса, трудовых и гражданско-правовых отношений и соблюдения законности в отношении конкретного субъекта 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 Субъектов персональных данных.

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

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

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

3. Общие принципы и условия обработки персональных данных

3.1 Обработка персональных данных Субъектов персональных данных осуществляется на основе принципов:

1) Законная и справедливая основа обработки персональных данных.

2) Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3) Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4) Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5) Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6) При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению

к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных.

7) Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных и требованиями законодательства о бухгалтерском и налоговом учете. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законодательством.

3.2 В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке персональных данных Субъектов обязаны соблюдать следующие общие требования:

1) Обработка персональных данных Субъектов персональных данных может осуществляться исключительно в целях реализации основных федеральных стандартов спортивной подготовки по виду спорта в соответствии с законодательством Российской Федерации в области персональных данных или выполнения трудовых, или гражданско-правовых договоров.

2) Все персональные данные следует получать непосредственно у Субъектов персональных данных, а если учащийся несовершеннолетний - у его родителей (представителей).

3) При определении объема и содержания обрабатываемых персональных Субъектов персональных данных, Оператор должен руководствоваться действующим законодательством.

4) Оператор не имеет права получать и обрабатывать персональные данные Субъектов персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

5) Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении Субъектов персональных данных или иным образом затрагивающих их права и законные интересы, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

6) Оператор обязан рассмотреть возражение в течение тридцати дней со дня его получения и уведомить Субъектов персональных данных о результатах рассмотрения такого возражения.

7) Защита персональных данных Субъектов персональных данных от неправомерного их использования или утраты должна быть обеспечена Оператором за счет своих средств, в порядке, установленном Федеральным законодательством и другими нормативными документами.

8) Обработку биометрических персональных данных производить в соответствии с требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

3.3 Оператор вправе поручить обработку персональных данных другому лицу с согласия Субъектов персональных данных, если иное не предусмотрено Федеральным законом.

3.4 Лицо, осуществляющее обработку персональных данных по поручению Оператора, не обязано получать согласие Субъектов персональных данных на обработку персональных данных Субъектов персональных данных.

3.5 В случае если Оператор поручает обработку персональных данных другому лицу, ответственность Субъектами персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.

4. Получение персональных данных Субъектов персональных данных

4.1. Получение персональных данных Субъектов персональных данных преимущественно осуществляется путем представления Субъектами персональных данных или их родителями (законными представителями) - в отношении несовершеннолетнего обучающегося, на основании их письменного согласия, за исключением случаев, прямо предусмотренных действующим законодательством РФ.

Согласие Субъекта персональных данных в письменной форме на обработку персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных (его представителя при наличии), номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

2) наименование и адрес Оператора, получающего согласие Субъекта персональных данных или его представителя;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие Субъекта персональных данных или его представителя;

5) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка будет поручена такому лицу;

6) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;

7) срок, втечение которого действует согласие Субъекта персональных данных или его представителя, а также способ его отзыва, если иное не установлено Федеральным законодательством;

8) подпись Субъекта персональных данных или его представителя.

4.2. В случае необходимости проверки персональных данных Субъекта персональных данных или его представителя Оператор заблаговременно должен сообщить об этом Субъекту персональных данных или его представителю, о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта персональных данных или его представителя дать письменное согласие на их получение.

5. Хранение и использование персональных данных Субъекта персональных данных или его представителя

5.1 Информация персонального характера Субъекта персональных данных или его представителя обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

5.2 Обработка персональных данных Субъекта персональных данных или его представителя МБУ ДО «СШ по киокусинкай» осуществляется смешанным путем:

-неавтоматизированным способом обработки персональных данных;

-автоматизированным способом обработки персональных данных (с помощью ПЭВМ и специальных программных продуктов).

5.3 Персональные данные Субъекта персональных данных или его представителя хранятся на бумажных носителях и в электронном виде.

5.4 Документы, содержащие персональные данные Субъекта персональных данных или его представителя МБУ ДО «СШ по киокусинкай», хранятся в административном здании.

Ответственные лица за хранение документов, содержащих персональные данные Субъекта персональных данных или его представителя, назначены Приказом директора Оператора.

5.5 Хранение оконченных производством документов, содержащих персональные данные Субъекта персональных данных или его представителя, осуществляется в помещении Оператора, предназначенном для хранения отработанной документации.

Ответственное лица за хранение оконченных производством документов, содержащих персональные данные, назначены Приказом директора Оператора.

5.6 Возможна передача персональных данных по внутренней сети Оператора с использованием технических и программных средств защиты информации, с доступом только для работников Оператора, допущенных к работе с персональными данными Приказом директора и только в объеме, необходимом данным работникам для выполнения своих должностных обязанностей.

5.7 Хранение персональных данных осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Хранение документов, содержащих персональные данные обучающихся и родителей (законных представителей) обучающихся, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению.

5.8 Оператор обеспечивает ограничение доступа к персональным данным Субъектов персональных данных лицам, не уполномоченным Федеральным законодательством, либо Оператором для получения соответствующих сведений.

Доступ к персональным данным Субъектов персональных данных или их представителей имеют работники Оператора, допущенные к работе с персональными данными Приказом директора.

Персональные данные Субъектов персональных данных или их представителей в полном объеме выдаются только директору, заместителям директора и лицам назначенным приказом директора.

Иным должностным лицам, допущенным к работе с персональными данными Субъектов персональных данных или их представителей, документы, содержащие персональные данные, выдаются, в объеме, необходимом для выполнения своих должностных обязанностей.

6. Защита персональных данных Субъектов персональных данных

6.1 Оператор при обработке персональных данных Субъектов персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2 Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

6.3 Обеспечение безопасности персональных данных Субъектов персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением 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) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.4 Выбор средств защиты информации для системы защиты персональных данных осуществляется Оператором в соответствии с нормативными правовыми актами.

6.5 Для обеспечения безопасности персональных данных Субъектов персональных данных при неавтоматизированной обработке предпринимаются следующие меры:

6.6.1. Определяются места хранения персональных данных (согласно настоящего Положения), которые оснащаются следующими средствами защиты:

- в кабинетах, где осуществляется хранение документов, содержащих персональные данные обучающихся и родителей (законных представителей) обучающихся, имеются сейфы, шкафы, стеллажи, тумбы.

- дополнительно кабинеты, где осуществляется хранение документов, содержащих персональные данные обучающихся и родителей (законных представителей) обучающихся, оборудованы замками и пожарной сигнализаций.

- оператор использует услуги охраны.

6.6.2. Все действия при неавтоматизированной обработке персональных данных Субъектов персональных данных осуществляются только должностными лицами Оператора, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.6.3. При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется(распространяется) только копия;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом,

исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление).

Персональные данные Субъектов персональных данных, содержащиеся на материальных носителях, уничтожаются по Акту об уничтожении персональных данных.

Эти правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

6.7. Для обеспечения безопасности персональных данных Субъектов персональных данных при автоматизированной обработке предпринимаются следующие меры:

6.7.1 Все действия при автоматизированной обработке персональных данных Субъектов персональных данных осуществляются только лицами, утвержденными Приказом директора, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.7.2 Персональные компьютеры, имеющие доступ к базам хранения персональных данных Субъектов персональных данных, защищены паролями доступа. Пароли устанавливаются Администратором информационной безопасности и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных обучающихся и родителей (законных представителей) обучающихся в на данном ПК.

6.7.3 Иные меры, предусмотренные Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

6.7.4 Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с Приказами по архивному делу, или продлевается на основании заключения экспертной комиссии Оператора, если иное не определено законодательством РФ.

Приложение №5

к приказу №12 от 03.02.25г.

ПЛАН МЕРОПРИЯТИЙ
по внутреннему контролю за соблюдением безопасности персональных данных в МБУ ДО «СШ по киокусинкай»

1. ОБЩИЕ ПОЛОЖЕНИЯ

План мероприятий по обеспечению защиты персональных данных (далее – План), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных.

План составлен на основании списка мер, методов и средств защиты, определенных в Политике информационной безопасности.

Выбор конкретных мероприятий осуществляется на основании анализа частной модели актуальных угроз и частной модели вероятного нарушителя.

В План включены следующие категории мероприятий:

- организационные (административные);
- технические (аппаратные и программные);
- физические;
- контролирующие.

В План включена следующая информация:

- Название мероприятия.
- Периодичность мероприятия.
- Исполнитель мероприятия/ответственный за исполнение.

2. ПЛАН МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

Мероприятие	Периодичность	Исполнитель/ Ответственный
Организационные мероприятия		
Осуществление внутреннего контроля за соблюдением сотрудниками учреждения законодательства РФ о персональных данных, в том числе требования к защите персональных данных.	Ежегодно	Масуфранов С. И.
Доведение до сведения положения законодательства РФ о персональных данных, разработанных внутренних локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.	По мере необходимости	Михеев О. А.
Организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление	По мере необходимости	Михеев О. А.

контроля за приемом и обработкой таких обращений и запросов		
Организация журнала учета обращений субъектов ПДн, журнала антивирусных проверок и т.д.	Разовое	Михеев О. А.
Определение уровней защищенности всех выявленных ИСПДн	Разовое/ ежегодно	Масуфранов С. И.
Организация информирования и обучения сотрудников о порядке обработки ПДн	По мере необходимости	Михеев О. А.
Собрание коллегиального органа по классификации ИСПДн	Разовое	Масуфранов С. И.

Физические мероприятия		
Организация пропускного режима для пропуска в контролируемую зону	постоянно	Михеев О. А.
Установка замков на дверях в помещениях с аппаратными средствами ИСПДн	Разовое	Михеев О. А.
Установка жалюзи на окнах	Разовое	Михеев О. А.
Установка системы пожаротушения в помещениях, где расположены элементы ИСПДн	Разовое	Михеев О. А.
Технические (аппаратные и программные) мероприятия		
Внедрение антивирусной защиты	Разовое	Светличная Е.В.
Осуществление обновления системы антивирусной защиты	Постоянно	Светличная Е.В.
Контролирующие мероприятия		
Контроль над соблюдением режима обработки ПДн	Еженедельно	Масуфранов С. И.
Контроль над выполнением антивирусной защиты	Еженедельно	Светличная Е.В.
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Светличная Е.В.
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	По мере необходимости	Бобрышова Е.А.
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	Светличная Е.В.
Контроль за обеспечением резервного копирования	Ежемесячно	Светличная Е.В.

Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Бобрышова Е.А.
Проведение мероприятий по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных	По мере необходимости	Масуфранов С. И.

Приложение №6

к приказу №12 от 03.02.25г.

ПОЛОЖЕНИЕ
о комиссии по классификации информационных систем персональных данных в МБУ ДО «СШ по киокусинкай»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Для проведения классификации информационных систем персональных данных создается Комиссия. Члены и председатель комиссии назначаются приказом директора. Комиссия в своей работе руководствуется Федеральным законом «О персональных данных» от 27.07.2006г. № 152-ФЗ (с изменениями и дополнениями), Постановлением Правительства Российской Федерации от 01.11.2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и иными нормативными актами, регулирующими отношения, связанные с обработкой персональных данных в информационных системах.

2. ФУНКЦИИ КОМИССИИ

2.1. Определение перечня информационных систем персональных данных, имеющихся в ОГБУ «Многопрофильный центр реабилитации» (далее ИСПДн).
2.2. Проведение анализа ИСПДн, имеющихся в наличии мер и средств защиты ИСПДн.
2.3. Проведение классификации ИСПДн в МБУ ДО «СШ по киокусинкай» в соответствии с характеристиками, заданными нормативными документами.
2.4. Определение и уточнение типовых моделей угроз и соответствующих им типовых требований к системам защиты ИСПДн.
2.5. Осуществление оценки необходимых мероприятий и затрат по приведению ИСПДн в соответствие с предъявляемыми требованиями

3. ПРАВА И ОБЯЗАННОСТИ КОМИССИИ

3.1. Комиссия имеет право:
3.1.1. Получать необходимые для своей работы сведения.
3.1.2. Присваивать класс информационным системам персональных данных на основании полученных сведений и нормативных документов.
3.2. Комиссия обязана:
3.2.1. Собирать необходимый объем информации.
3.2.2. Анализировать полученные данные.
3.2.3. Делать заключение о классе информационной системы персональных данных.
3.2.4. Подготавливать Акт классификации информационных систем персональных данных.

4. ПОРЯДОК РАБОТЫ КОМИССИИ

Состав комиссии, а также внесение изменений в него утверждается приказом директора МБУ ДО «СШ по киокусинкай»

Приложение №7
к приказу №12 от 03.02.25г.

Положение
о защите персональных данных работников муниципального бюджетного учреждения дополнительного образования «Спортивная школа по киокусинкай»

1. Общие положения

1.1 Настоящее Положение разработано в соответствии со статьей 24 Конституции Российской Федерации, Трудовым кодексом Российской Федерации, Федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями от 12 декабря 2023 года, от 27 июля 2006 года № 152-ФЗ «О персональных данных» с изменениями от 6 февраля 2023 года, Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 года № 179 «Об утверждении требований к подтверждению уничтожения персональных данных», Федеральным законом № 273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации» с изменениями от 25 декабря 2023 года, а также Уставом организации и другими нормативными правовыми актами Российской Федерации, регламентирующими деятельность организаций, осуществляющих образовательную деятельность.

1.2. Данное Положение разработано с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну работников организации от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Настоящее Положение регулирует отношения, связанные с обработкой персональных данных работников и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю, а также устанавливает ответственности должностных лиц, имеющих доступ к персональным данным работников спортшколы.

1.4. ***Персональные данные*** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.5. ***Оператор*** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.7. ***Автоматизированная обработка персональных данных*** — обработка персональных данных с помощью средств вычислительной техники.

1.8. ***Распространение персональных данных*** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.9. ***Предоставление персональных данных*** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
1.10. ***Блокирование персональных данных*** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
1.11. ***Уничтожение персональных данных*** — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
1.12. ***Обезличивание персональных данных*** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
1.13. ***Информационная система персональных данных*** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
1.14. ***Общедоступные данные*** — сведения общего характера и иная информация, доступ к которой не ограничен.
1.15. К персональным данным работника, получаемым и подлежащим хранению у работодателя в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах работников:

- паспортные данные работника;
- ИНН;
- копия страхового свидетельства государственного пенсионного страхования;
- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;
- копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе – автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- документы о возрасте малолетних детей;
- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);
- трудовой договор;
- заключение по данным психологического исследования (если такое имеется);
- копии приказов о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
- личная карточка по форме Т-2;
- заявления, объяснительные и служебные записки работника;
- документы о прохождении работником аттестации, повышения квалификации;
- иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых

правоотношений с работником (включая приговоры суда о запрете заниматься педагогической деятельностью или занимать руководящие должности).

1.16. Размещение на официальном сайте фотографий работников, видео с работниками сотрудники разрешают путем предоставления согласия на обработку персональных данных в организации.

1.17. Персональные данные работников спортшколы являются конфиденциальной информацией и не могут быть использованы сотрудниками организации, осуществляющей образовательную деятельность в личных целях.

2. Общие требования при обработке персональных данных работника и гарантии их защиты

2.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

2.1.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.1.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться 24 статьей Конституцией Российской Федерации, 65 статьей Трудового Кодекса и иными федеральными законами.

2.1.3. Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

2.1.4. Работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся (в соответствии со статьей 10 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных») к специальным категориям персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных: в частности

  1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

  2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

  3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

  4) цель обработки персональных данных;

  5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
9) подпись субъекта персональных данных.

- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных в п.2.2 данного Положения;
- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами,

муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

2.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом или иными федеральными законами.
2.1.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.
2.1.7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым Кодексом и иными федеральными законами.
2.1.8. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.
2.1.9. Работники не должны отказываться от своих прав на сохранение и защиту тайны.
2.1.10. Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.
2.2. Согласно ст.10.1 Федерального закона «О персональных данных», особенностями обработки персональных данных, разрешенных субъектом персональных данных для распространения являются:
2.2.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Работник образовательной организации (оператор) обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.
2.2.2. В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.
2.2.3. В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.
2.2.4. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.
2.2.5. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, предусмотренные п.2.2.9 настоящего Положения, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект

персональных данных устанавливает условия и запреты в соответствии с п.2.2.9 настоящего Положения, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

2.2.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

2.2.6.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, должно содержать следующую информацию:

1) фамилия, имя, отчество (при наличии) субъекта персональных данных;

2) контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);

3) сведения об операторе-организации - наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных); сведения об операторе - физическом лице - фамилия, имя, отчество (при наличии), место жительства или место пребывания; сведения об операторе-гражданине, являющемся индивидуальным предпринимателем, - фамилия, имя, отчество (при наличии), идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);

4) сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных;

5) цель (цели) обработки персональных данных;

6) категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к субъекту персональных данных);

специальные категории персональных данных (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни, сведения о судимости);

биометрические персональные данные;

7) категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов (заполняется по желанию субъекта персональных данных);

8) условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);

9) срок действия согласия.

2.2.7. Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определяются уполномоченным органом по защите прав субъектов персональных данных.

2.2.8. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.2.9. В согласии на обработку персональных данных, разрешенных субъектом

персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий не допускается.
2.2.10. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.
2.2.11. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.
2.2.12. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.
2.2.13. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования, указанного в п.2.2.12 настоящего Положения.
2.2.14. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения п.2.2 данного Положений или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.
2.2.15. Требования п.2.2 настоящего Положения не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.
2.3. МБУ ДО «СШ по киокусинкай» определяет объем, содержание обрабатываемых персональных данных работников, руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.
2.4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
2.5. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
2.6. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Хранение и использование персональных данных

3.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Персональные данные работников спортшколы хранятся на бумажных и электронных носителях (к доступу имеется определенный код), в специально предназначенных для этого помещениях.

3.3. В процессе хранения персональных данных работников должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;
- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;
- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.4. Доступ к персональным данным работников имеют:

- директор;
- заместители директора;
- специалист по кадрам;
- иные работники, определяемые приказом директора общеобразовательной организации в пределах своей компетенции.

3.5. Помимо лиц, указанных в п. 3.4. настоящего Положения, право доступа к персональным данным работников имеют лица, уполномоченные действующим законодательством.

3.6. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные работников лишь в целях, для которых они были предоставлены.

3.7. Ответственным за организацию и осуществление хранения персональных данных работников организации является заместитель директора, в соответствии с приказом директора спортивной школы.

3.8. Персональные данные работника отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в сейфе.

4. Передача персональных данных

4.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым Кодексом или иными федеральными законами.

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

4.1.3. Предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым Кодексом и иными федеральными законами.

4.1.4. Осуществлять передачу персональных данных работника в пределах общеобразовательной организации в соответствии с данным Положением, с которым работник должен быть ознакомлен под роспись.

4.1.5. Разрешать доступ к персональным данным работников только специально

уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.
4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.
4.1.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

5. Права работника в целях обеспечения защиты персональных данных, хранящихся у работодателя

5.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право:
5.1.1. Получать полную информацию о своих персональных данных и их обработке.
5.1.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении работника, – к заместителю директора, ответственному за организацию и осуществление хранения персональных данных работников.
5.1.3. На определение своих представителей для защиты своих персональных данных.
5.1.4. На доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору.
5.1.5. Требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением работника на имя директора школы. При отказе руководителя организации исключить или исправить персональные данные работника, работник имеет право заявить в письменном виде руководителю организации, осуществляющей образовательную деятельность, о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.
5.1.6. Требовать об извещении организацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.1.7. Обжаловать в суде любые неправомерные действия или бездействия организации при обработке и защите его персональных данных.

6. Обязанности субъекта персональных данных по обеспечению достоверности его персональных данных

6.1. В целях обеспечения достоверности персональных данных работники обязаны:
6.1.1. При приеме на работу в организацию, осуществляющую образовательную деятельность, представлять уполномоченным работникам достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.
6.1.2. В случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом в течение 5 рабочих дней с даты их изменений.

7. Уничтожение персональных данных

7.1. В соответствии с Приказом Роскомнадзора №179 от 28 октября 2022 года, определены требования к документальному оформлению факта уничтожения персональных данных работников общеобразовательной организации:

- в случае если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных;
- в случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

7.2. Акт об уничтожении персональных данных должен содержать:

- наименование общеобразовательной организации или фамилию, имя, отчество (при наличии) оператора персональных данных и его адрес;
- наименование общеобразовательной организации или фамилию, имя, отчество (при наличии) лица, осуществляющего обработку персональных данных субъекта персональных данных по поручению оператора (если обработка была поручена такому лицу;
- фамилию, имя, отчество (при наличии) субъекта или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;
- фамилию, имя, отчество (при наличии), должность лиц, уничтоживших персональные данные субъекта персональных данных, а также их подпись;
- перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;
- наименование уничтоженного материального носителя, содержащего персональные данные субъекта персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);
- способ уничтожения персональных данных;
- причину уничтожения персональных данных;
- дату уничтожения персональных данных субъекта (субъектов) персональных данных.

Форма акта об уничтожении персональных данных составляется в произвольной форме.

7.3. Акт об уничтожении персональных данных может быть оформлен как на бумаге, так и в электронной форме. В первом случае он заверяется личной подписью лиц, уничтоживших персональные данные, а во втором – их электронной подписью.

7.4. Выгрузка из журнала должна содержать:

- фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;
- перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;
- причину уничтожения персональных данных;
- дату уничтожения персональных данных субъекта (субъектов) персональных данных.

7.5. При невозможности указать в выгрузке из журнала какие-либо сведения, их следует отразить в акте об уничтожении персональных данных.

7.6. Если оператор обрабатывает персональные данные, используя и не используя средства автоматизации, при их уничтожении следует оформлять акт об уничтожении и выгрузку из журнала.

7.7. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

8.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско- правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

8.2. Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

8.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8.4. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

8.5. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

8.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ «О 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.

8.7. Организация вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию организации или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Во всех остальных случаях оператор (руководитель организации, осуществляющей образовательную деятельность, и (или) уполномоченные им лица) обязан направить в

уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

9. Заключительные положения

9.1. Настоящее Положение о защите персональных данных работников является локальным нормативным актом, принимается на Общем собрании работников спортивной школы и утверждается (либо вводится в действие) приказом директора организации, осуществляющей образовательную деятельность.

9.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

9.3. Положение о защите персональных данных работников организации дополнительного образования принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п.9.1. настоящего Положения.

9.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

Приложение №8

к приказу №12 от 03.02.25г.

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «СПОРТИВНАЯ ШКОЛА ПО КИОКУСИНКАЙ»

№ п/п	Наименование ИСДн	Категория ПДн (Хпд)	Объем ПДн (Хнпд)	Тип ИСДн	Уровень защищенности	Класс	Структура ИСПДн	Режим обработки Пдн	Наличие подключений к сети Интернет
1	ИПДн «Сотрудники»	2	3(<1000)	Специальная	4	К3	Локальная	Многопользовательский с разными правами	Одиоточетное
2	ИСПДн «Обучающиеся»	2	3(<1000)	Специальная	4	К3	Локальная	Многопользовательский с разными правами	Одиоточетноей

Приложение №9
к приказу №12 от 03.02.25г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ И ИХ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «СПОРТИВНАЯ ШКОЛА ПО КИОКУСИНКАЙ»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об обработке защите персональных данных обучающихся и их родителей (законных представителей) (далее – Положение) определяет порядок обработки и защиты персональных данных обучающихся и их родителей (законных представителей) (далее – субъекты персональных данных) и гарантии конфиденциальности сведений, предоставленных администрации Муниципального бюджетного учреждения дополнительного образования «Спортивная школа по киокусинкай» (далее – СШ, оператор), родителями (законными представителями) обучающихся, не достигших 14-летнего возраста и обучающимися, достигшими 14-летнего возраста самостоятельно, а также устанавливает ответственность должностных лиц СШ, имеющих доступ к персональным данным субъектов персональных данных.

1.2. Настоящее Положение разработано с целью обеспечения защиты прав и свобод обучающихся СШ и их родителей (законных представителей) при обработке (получении, обработки, использовании, хранении, уничтожении и т.д.) их персональных данных, в том числе защиты от несанкционированного доступа, неправомерного их использования или утраты.

1.3 Настоящее Положение разработано на основании статьи 24 Конституции Российской Федерации, Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями от 12 декабря 2023 года и Федерального закона Российской Федерации № 152-ФЗ от 27.07.2006 г. «О персональных данных» с изменениями от 6 февраля 2023 года), Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 года № 179 «Об утверждении требований к подтверждению уничтожения персональных данных», а также Уставом СШ и другими нормативными правовыми актами Российской Федерации, регламентирующими деятельность организаций, осуществляющих образовательную деятельность.

1.4. В целях настоящего Положения используются следующие основные понятия:

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

1.4.2. ***Персональные данные, разрешенные субъектом персональных данных для распространения***, – персональные данные, доступ неограниченного круга лиц к которым

предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом№ 152-ФЗ «О персональных данных».

1.4.3. ***Оператор***–государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а так обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.4.4. ***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.

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

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

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

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

1.4.9. ***Уничтожение персональных данных*** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.4.10. ***Обезличивание персональных данных*** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

же определяющие цели

1.4.11. ***Информационная система персональных данных***–совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5. Персональные данные относятся к категории конфиденциальной информации.

1.6. Все работники СШ, в соответствии со своими полномочиями владеющие информацией об обучающихся и их родителях (законных представителях), получающие и использующие ее, несут ответственность в соответствии законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

II. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ГАРАНТИИ ИХ ЗАЩИТЫ

2.1. СШ определяет объем, содержание обрабатываемых персональных данных обучающихся и их родителей (законных представителей), руководствуясь Конституцией Российской Федерации, иными нормативными актами Российской Федерации, а также настоящим Положением, Уставом и другими локальными нормативными актами СШ.

2.2. Обработка Оператором персональных данных осуществляется в следующих целях:

1. Цель обработки: обеспечение соблюдения законодательства в сфере образования			
Категории данных	Персональные данные	Специальные Персональные Данные	Биометрические персональные данные
Перечень данных	фамилия, имя, отчество; пол; гражданство; год рождения; месяц рождения; дата рождения; место рождения; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона; адрес электронной почты; СНИЛС; данные медицинского полиса, номер сертификата дополнительного образования, иные персональные данные, предоставляемые обучающимися необходимые для обеспечение соблюдения законодательства РФ в сфере образования и/или заключения и исполнения договоров	сведения о Состоянии Здоровья	данные изображения лица, полученные с помощью фото-видео устройств, позволяющие установить личность субъекта персональных данных
Категории субъектов	**Обучающиеся (занимающиеся)**		
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет		
Сроки обработки	В течение срока обучения и периода после его завершения, необходимого для выполнения всех обязательств сторон		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные		
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в СШ в зависимости от способа обработки персональных данных и типа носителя персональных данных		

2. Цель обработки: обеспечение соблюдения законодательства РФ в сфере образования	
Категории данных	Персональные данные
Перечень данных	фамилия, имя, отчество; пол; год рождения; месяц рождения; дата рождения; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона; адрес электронной почты;

	иные персональные данные, предоставляемые Законными представителями учащихся необходимые для обеспечение соблюдения законодательства РФ в сфере образования и/или заключения и исполнения договоров
Категории субъектов	**Родители (законные представители)**
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет
Сроки обработки	В течение срока обучения обучающихся (воспитанников) и периода после его завершения, необходимого для выполнения всех обязательств сторон
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в СШ в зависимости от способа обработки персональных данных и типа носителя персональных данных
3. Цель обработки: обеспечение пропускного режима на территорию Оператора	
Категории данных	Персональные данные
Перечень данных	фамилия, имя, отчество; данные документа, удостоверяющего личность
Категории субъектов	Обучающиеся (спортсмены), Родители (законные представители)
Способы обработки	Неавтоматизированная, внесение персональных данных в журнал учета Посетителей
Сроки обработки	В течение срока, необходимого для ведения журнала учета посетителей
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в СШ в зависимости от способа обработки персональных данных и типа носителя персональных данных

2.3. В целях обеспечения прав и свобод обучающихся и их родителей (законных представителей) сотрудники СШ при обработке персональных данных субъекта персональных данных обязаны соблюдать следующие общие требования:

2.3.1. Обработка персональных данных обучающихся и их родителей (законных представителей) может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

2.3.2. При определении объема и содержания обрабатываемых персональных данных субъекта персональных данных руководитель СШ должен руководствоваться Конституцией Российской Федерации, Федеральным законом № 152-ФЗ «О персональных данных», иными нормативными актами Российской Федерации, также настоящим Положением, Уставом и другими локальными нормативными актами СШ.

2.3.3. Все персональные данные обучающегося, достигшего 14-летнего возраста, следует получать у него самого. Персональные данные обучающегося, не достигшего 14-летнего возраста, следует получать у родителей (законных представителей).

2.3.4. Обработка персональных данных осуществляется только с согласия субъекта персональных данных. Согласие субъекта персональных данных оформляется в письменной форме. Письменное согласие субъекта персональных данных, на обработку своих персональных данных должно соответствовать требованиям ч. 4 ст. 9 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и включать в**,** в частности:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

Образец согласия утвержден приложением № 1 к настоящему положению.

Представители СШ должны сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, также о характере подлежащих получению персональных данных и разъяснить юридические последствия отказа предоставить СШ персональные данные и (или) дать письменное согласие на их получение.

2.3.5. Администрация и педагогические работники СШ не имеют права получать и обрабатывать персональные данные обучающихся и их родителей (законных представителей), относящиеся (в соответствии со ст. 10 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных») к специальным категориям персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

- обработка персональных данных осуществляется в соответствии с Федеральным законом от 25.01.2002 г.№ 8-ФЗ «О Всероссийской переписи населения»;

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни,

здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

- обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

– обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи осуществлением правосудия;

- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

- обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи осуществлением ими прокурорского надзора;

- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

2.3.6. При принятии решений, затрагивающих интересы обучающегося и/или его родителей (законных представителей), директор СШ и представители СШ не имеют права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

2.3.7. Защита персональных данных обучающегося и/или его родителей (законных представителей) от неправомерного их использования или утраты должна быть обеспечена директором СШ в порядке, установленном действующим законодательством.

2.3.8. Субъект персональных данных вправе отозвать согласие на обработку его данных, а оператор в таком случае — обязан прекратить их обработку в течение 10 рабочих дней, и в случае, если сохранение данных более не требуется для целей обработки, уничтожить их в срок, не превышающий 30 дней с даты поступления отзыва.

Если у оператора отсутствует возможность уничтожения персональных данных в течение установленного срока, оператор обязан заблокировать данные и обеспечить их уничтожение в срок не более чем 6 месяцев. Факт уничтожения оператором персональных

данных в указанных случаях осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных — на основании Приказа Роскомнадзора от 28.10.2022 № 179. Акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных подлежат хранению в течение 3 лет с момента уничтожения данных.

2.3.9. Обучающиеся СШ, достигшие 14-летнего возраста, и родители или законные представители обучающихся (воспитанников), не достигших 14-летнего возраста, должны быть ознакомлены под подпись с документами, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

2.4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

2.5. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Обработка персональных данных, разрешенных для распространения, из числа специальных категорий персональных данных, указанных в части 1 статьи 10 Федерального закона от 27.07.2006 г. № 152-ФЗ, допускается, если соблюдаются запреты и условия, предусмотренные статьи 10.1 указанного Закона.

2.6. Письменное согласие субъекта на обработку персональных данных, разрешенных для распространения, оформляется отдельно от других согласий на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.7. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

-непосредственно;

-с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

2.8. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, должно содержать следующую информацию:

1) фамилия, имя, отчество (при наличии) субъекта персональных данных;

2) контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);

3) сведения об операторе-организации - наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);

4) сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных;

5) цель (цели) обработки персональных данных;

6) категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, другая информация, относящаяся к субъекту персональных

данных); специальные категории персональных данных (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, сведения о судимости); биометрические персональные данные;
7) категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов (заполняется по желанию субъекта персональных данных);
8) условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);
9) срок действия согласия.

Образец согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утвержден приложением № 2 к настоящему положению.

2.9. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.10. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий не допускается.

2.11. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

2.12. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

2.13. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных.

2.14. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

III. ПРАВА И ОБЯЗАННОСТИ ОБУЧАЮЩИХСЯ (ЗАНИМАЮЩИХСЯ), ДОСТИГШИХ 14-ЛЕТНЕГО ВОЗРАСТА И РОДИТЕЛЕЙ ИЛИ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ ОБУЧАЮЩИХСЯ (ВОСПИТАННИКОВ), НЕ ДОСТИГШИХ 14-ЛЕТНЕГО ВОЗРАСТА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обучающиеся СШ, достигшие 14-летнего возраста, и родители или законные представители обучающихся, не достигших 14-летнего возраста, имеют право на:

3.1.1. Полную информацию о своих персональных данных и обработке этих данных.

3.1.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные обучающегося, за исключением случаев, предусмотренных федеральными законами.

Получение указанной информации о своих персональных данных возможно при личном обращении обучающегося (его родителя или представителя) к лицу, ответственному за организацию обработки персональных данных в СШ.

3.1.3. Обжалование в суде любых неправомерных действия при обработке и по защите персональных данных.

3.2. Обучающиеся СШ, достигшие 14-летнего возраста, и родители или законные представители обучающихся, не достигших 14-летнего возраста, обязаны:

3.2.1. Передавать директору СШ, его заместителям, тренерам-преподавателям, медицинским работникам и другим уполномоченным представителям СШ достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

3.2.2. В случае изменения персональных данных: фамилия, имя, отчество, адрес места жительства, паспортные данные, состоянии здоровья сообщать тренеру-преподавателю об этом в течение 5 рабочих дней с даты их изменений.

IV. СБОР, ОБРАБОТКА, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Получение, обработка, хранение и любое другое использование персональных данных обучающихся может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

4.2. Личные дела обучающихся хранятся в бумажном виде в папках, находятся в специальном шкафу, обеспечивающим защиту от несанкционированного доступа.

4.3. Персональные данные обучающихся и/или их родителей (законных представителей) могут также храниться в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные, защищается системой паролей и ограничивается для пользователей, не являющихся оператором информационной системы.

4.4. Хранение персональных данных обучающихся и/или их родителей (законных представителей) должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом.

4.5. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.6. Уничтожение персональных данных осуществляется в соответствии с Регламентом уничтожения персональных данных комиссией, созданной приказом директора СШ.

4.7. Способы уничтожения персональных данных устанавливаются в Регламенте уничтожения персональных данных.

4.8. Подтверждение уничтожения персональных данных осуществляется в соответствии с требованиями, установленными приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

4.9. В процессе хранения персональных данных обучающихся и/или их родителей (законных представителей) должны обеспечиваться:

-требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

-сохранность имеющихся данных, ограничение доступа к ним, в соответствии законодательством Российской Федерации и настоящим Положением;

-контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4.10. Доступ к персональным данным обучающихся и/или их родителей (законных представителей) имеют:

-директор СШ;

-заместители директора;

-инструкторы-методисты- только к тем данным, которые необходимы для выполнения конкретных функций;

- медицинская сестра – в объеме данных в сфере своей компетенции;

-тренеры-преподаватели - только к тем данным, которые необходимы для выполнения конкретных функций,

-лица, работающие с информационными системами,

- иные представители СШ, определяемые дополнительно приказом директора СШ в пределах своей компетенции.

4.11. Сведения об обучающемся (воспитаннике) могут быть предоставлены (на основании официального запроса на бланке организации):

-Управлению образования;

- Управлению по физической культуре, спорту и молодежной политике;

-Администрации;

-Военному комиссариату;

-Надзорным (контрольным) органам, которые имеют доступ к информации только в сфере своей компетенции;

-Центральной районной больнице и т.д.

4.12. Персональные данные обучающегося могут быть предоставлены родственникам с письменного разрешения родителей или законных представителей обучающихся, не достигших 14-летнего возраста или письменного разрешения обучающегося, достигшего 14-летнего возраста.

4.13. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные обучающихся и/или их родителей (законных представителей) лишь в целях, для которых они были предоставлены.

4.14. Ответственным за организацию обработки персональных данных обучающихся СШ и/или их родителей (законных представителей) является заместитель руководителя, в соответствии с приказом директора СШ.

V. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При передаче персональных данных обучающегося директор СШ, его заместители, тренеры-преподаватели, лица, работающие с информационной системы и другие уполномоченные представители СШ должны соблюдать следующие требования:

5.1.1. Не сообщать персональные данные обучающегося третьей стороне без письменного согласия обучающегося при достижении им 14-летия или родителей (законных представителей), за исключением случаев, когда это необходимо целях предупреждения угрозы жизни и здоровью обучающегося, а также других случаях, предусмотренных федеральными законами.

5.1.2. Не сообщать третьим лицам персональные данные обучающегося в коммерческих целях.

5.1.3. Предупредить лиц, получающих персональные данные обучающегося, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получающие персональные данные обучающегося, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными обучающегося в порядке, установленном федеральными законами.

5.1.4. Осуществлять передачу персональных данных обучающихся в пределах СШ в соответствии с настоящим Положением.

Родителей (законных представителей) обучающихся, не достигших 14-летнего возраста и обучающихся, достигших 14-летнего возраст, необходимо ознакомить с настоящим Положением.

5.1.5. Разрешать доступ к персональным данным обучающихся только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные детей, которые необходимы для выполнения конкретных функций.

5.1.6. Не запрашивать информацию о состоянии здоровья обучающегося, за исключением тех сведений, которые определены законодательством Российской Федерации.

VI. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩЕГОСЯ И/ИЛИ ЕГО РОДИТЕЛЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

6.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных обучающегося и/или его родителей (законных представителей), привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

6.2. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

6.3. Работники СШ, в соответствии со своими полномочиями владеющие информацией об обучающихся и/или их родителях (законных представителях), получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

6.4. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб СШ, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

6.5. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

6.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных

настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ «О 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.

VII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящее Положение является локальным нормативным актом и утверждается (либо вводится в действие) приказом директора СШ.

7.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

7.3. Положение о защите персональных данных обучающихся и их родителей (законных представителей) принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п.7.1. настоящего Положения.

7.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

Приложение № 1
Положению о защите персональных данных обучающихся
и их родителей (законных представителей)
в МБУ ДО «СШ по киокусинкай»

Согласие на обработку персональных данных
обучающихся, достигших 14-летнего возраста

Я,_____
(фамилия, имя, отчество)

Гражданин(ка)_____паспорт серия _____№_____, выдан _____
_____,
зарегистрированный(ая) по адресу:_____
_____,
далее Субъект, в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" **даю** Муниципальному образовательному учреждению дополнительного образования «Спортивная школа по киокусинкай» (далее – МБУ ДО «СШ по киокусинкай»), зарегистрированному по адресу: Московская область, г.о. Коломна, ул. Девичье поле, д.1, пом 1Б, ОГРН 1205000116991, ИНН 5022061895, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, необходимых в связи с поступлением в МБУ ДО «СШ по киокусинкай» и в целях содействия в осуществлении учебной деятельности, обеспечения личной безопасности, учета результатов исполнения договорных обязательств, а также наиболее полного исполнения МБУ ДО «СШ по киокусинкай» обязательств и компетенций в соответствии с законодательством РФ следующих моих персональных данных:

- фамилия, имя, отчество;
- дата и место рождения, пол;
- сведения о гражданстве (подданстве);
- паспортные данные;
- адрес регистрации, адрес фактического проживания;
- контактная информация (мобильный, домашний телефон, e-mail);
- реквизиты страхового медицинского полиса обязательного медицинского страхования граждан
- реквизиты страхового свидетельства обязательного пенсионного страхования
- номер сертификата дополнительного образования.
- группа здоровья
- физкультурная группа

Настоящее согласие на обработку персональных данных действует с момента представления данных на период моего обучения в МБУ ДО «СШ по киокусинкай» и срок хранения моих документов в соответствии с законодательством об архивном деле в Российской Федерации. Согласие может быть отозвано мной в любое время путем подачи заявления в письменной форме в соответствии с требованиями законодательства Российской Федерации.

Права и обязанности в области защиты персональных данных, а также возможные последствия в случае моего отказа от согласия на обработку персональных данных мне разъяснены.

Обязуюсь сообщать в МБУ ДО «СШ по киокусинкай» об изменении моих персональных данных. Об ответственности за достоверность представленных персональных сведений предупрежден(а).

«___»_____20___г. _____(подпись) _____(Ф.И.О.)

Согласие на обработку персональных данных
родителей (законных представителей) обучающихся, не достигших 14-летнего возраста)

Настоящим Я, _____,
номер телефона: _____, электронная почта: _____, в соответствии со статьёй 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», своей волей и в своих интересах и в интересах моего ребенка даю согласие Муниципальному образовательному учреждению дополнительного образования «Спортивная школа по киокусинкай» (далее – МБУ ДО «СШ по киокусинкай»), зарегистрированному по адресу: Московская область, г.о. Коломна, ул. Девичье поле, д.1, пом 1Б, ОГРН 1205000116991, ИНН 5022061895, на автоматизированную, а также без использования средств автоматизации обработку персональных данных включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных моего ребенка

_____,почтовый адрес_____

необходимых в связи с обучением в МБУ ДО «СШ по киокусинкай» и в целях содействия в осуществлении учебной деятельности, обеспечения личной безопасности, учета результатов исполнения договорных обязательств, а также наиболее полного исполнения МБУ ДО «СШ по киокусинкай» обязательств и компетенций в соответствии с законодательством РФ в объеме:

- фамилия, имя, отчество;
- дата и место рождения, пол;
- сведения о гражданстве (подданстве);
- паспортные данные;
- адрес регистрации, адрес фактического проживания;
- контактная информация (мобильный, домашний телефон, e-mail);
- реквизиты страхового медицинского полиса обязательного медицинского страхования граждан
- реквизиты страхового свидетельства обязательного пенсионного страхования

Настоящее согласие на обработку персональных данных действует с момента представления данных на период обучения в МБУ ДО «СШ по киокусинкай» и срок хранения моих документов в соответствии с законодательством об архивном деле в Российской Федерации. Согласие может быть отозвано мной в любое время путем подачи заявления в письменной форме в соответствии с требованиями законодательства Российской Федерации.

Права и обязанности в области защиты персональных данных, а также возможные последствия в случае моего отказа от согласия на обработку персональных данных мне разъяснены.

Обязуюсь сообщать в МБУ ДО «СШ по киокусинкай» об изменении персональных данных ребенка. Об ответственности за достоверность представленных персональных сведений предупрежден(а).

«___»_____20___г. _____(подпись) _____(Ф.И.О.)

Приложение № 2
Положению о защите персональных данных обучающихся
и их родителей (законных представителей)
в МБУ ДО «СШ по киокусинкай»

СОГЛАСИЕ

на обработку персональных данных, разрешенных для распространения родителей (законных представителей) обучающихся, не достигших 14-летнего возраста

Я, _____,

номер телефона: _____, электронная почта: _____, в

соответствии со статьями 6 и 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О

персональных данных», приказом Роскомнадзора от 24.02.2021 № 18, своей волей и в своих интересах и в интересах моего ребенка даю согласие Муниципальному образовательному учреждению дополнительного образования «Спортивная школа по киокусинкай» (далее – МБУ ДО «СШ по киокусинкай»), зарегистрированному по адресу: Московская область, г.о. Коломна, ул. Девичье поле, д.1, пом 1Б, ОГРН 1205000116991, ИНН 5022061895, на обработку персональных данных моего ребенка,

почтовый адрес: _____,

в объеме:

_____

_____

_____

с целью размещения _____

_____

ребенка на сайте МБУ ДО «СШ по киокусинкай» по адресу: https://kyokushin-kolomna.ru/

Подтверждаю, что ознакомлена с документами МБУ ДО «СШ по киокусинкай», устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями. Предупреждена, что согласие на обработку персональных данных может быть отозвано мною путем направления МБУ ДО «СШ по киокусинкай» письменного отзыва.

Настоящее согласие действует со дня его подписания на период обучения моего ребенка

_____

в МБУ ДО «СШ по киокусинкай»

СОГЛАСИЕ

на обработку персональных данных, разрешенных для распространения обучающихся, достигших 14-летнего возраста

Я, _____, номер телефона_____, электронная почта: _____, в соответствии со статьями 6 и 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказом Роскомнадзора от 24.02.2021 № 18, своей волей и в своих интересах даю согласие Муниципальному образовательному учреждению дополнительного образования «Спортивная школа по киокусинкай» (далее – МБУ ДО «СШ по киокусинкай»), зарегистрированному по адресу: Московская область, г.о. Коломна, ул. Девичье поле, д.1, пом 1Б, ОГРН 1205000116991, ИНН 5022061895 на обработку моих персональных данных:

_____
_____
_____

_____и других сведений, определенных в подпункте «г» пункта 3.6 Требований, утвержденных приказом Рособрнадзора от 14.08.2020 № 831,
с целью размещения их на официальном сайте МБУ ДО «СШ по киокусинкай» по адресу: https://kyokushin-kolomna.ru/

Подтверждаю, что ознакомлен с документами МБУ ДО «СШ по киокусинкай», устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями. Предупрежден, что согласие на обработку персональных данных может быть отозвано мною путем направления МБУ ДО «СШ по киокусинкай» письменного отзыва.

Настоящее согласие действует со дня его подписания и на период обучения в МБУ ДО «СШ по киокусинкай».

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение №10

к приказу №12 от 03.02.25г.

ПОРЯДОК УНИЧТОЖЕНИЯ И ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «СПОРТИВНАЯ ШКОЛА ПО КИОКУСИНКАЙ»

1. Общие положения

1.1. Порядок уничтожения персональных данных в МБУ ДО «СШ ПО КИОКУСИНКАЙ»(далее – Порядок) устанавливает способы уничтожения и обезличивания носителей, содержащих персональные данные субъектов персональных данных, а также лиц, уполномоченных проводить эти процедуры.

1.2. Настоящий Порядок разработан на основе Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

2. Правила уничтожения персональных данных

2.1. Уничтожение персональных данных и носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть конфиденциальным, исключая возможность последующего восстановления;
- оформляться юридически, в частности, актом о выделении к уничтожению носителей, содержащих персональные данные субъектов персональных данных (приложение № 1), и актом об уничтожении персональных данных (приложение № 2, приложение № 3), а также выгрузкой из журнала регистрации событий в информационной системе персональных данных (приложение № 4);
- должно проводиться комиссией по уничтожению персональных данных;
- уничтожение должно касаться только тех персональных данных, которые подлежат уничтожению в связи с истечением срока хранения, достижением цели обработки указанных персональных данных либо утратой необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

3. Порядок уничтожения носителей, содержащих персональные данные

3.1. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении, а также в иных случаях, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3.2. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются комиссией по уничтожению персональных данных, утвержденной приказом директора МБУ ДО «СШ по киокусинкай» (далее – Комиссия).

3.3. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются Комиссией в сроки, установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3.4. Комиссия производит отбор носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

3.5. На все отобранные к уничтожению материалы составляется акт по форме, приведенной в приложении № 1 к Порядку. В акте исправления не допускаются. Комиссия проверяет наличие всех материалов, включенных в акт.

3.6. По окончании сверки акт подписывается всеми членами Комиссии и утверждается ответственным за организацию обработки персональных данных.

3.7. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.
3.8. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.
3.9. Уничтожение носителей, содержащих персональные данные, осуществляется в следующем порядке:

- уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем измельчения на мелкие части, исключающие возможность последующего восстановления информации. Измельчение осуществляется с использованием шредера (уничтожителя документов);
- хранящихся на ПЭВМ и (или) на перезаписываемых съемных машинных носителях информации, используемых для хранения информации вне ПЭВМ (флеш-накопителях, внешних жестких дисках, CD-дисках и иных устройствах), производится с использованием штатных средств информационных и операционных систем;
- уничтожение персональных данных, содержащихся на машиночитаемых носителях, которые невозможно уничтожить с помощью штатных средств информационных и операционных систем, производится путем нанесения носителям неустранимого физического повреждения, исключающего возможность их использования, а также восстановления данных, в том числе путем деформирования, нарушения единой целостности носителя.

4. Порядок оформления документов об уничтожении персональных данных
4.1. Об уничтожении носителей, содержащих персональные данные, обрабатываемых без средств автоматизации, Комиссия составляет и подписывает акт об уничтожении персональных данных по форме, приведенной в приложении № 2 к Порядку.
4.2. Об уничтожении персональных данных, обрабатываемых с использованием средств автоматизации, Комиссия составляет и подписывает акт об уничтожении персональных данных по форме, приведенной в приложении № 3 к Порядку, а также Комиссия оформляет выгрузку из журнала регистрации событий в информационной системе персональных данных по правилам приказа Роскомнадзора от 28.10.2022 № 179.
4.3. Если обработка персональных данных осуществляется одновременно с использованием средств автоматизации и без использования средств автоматизации, Комиссия по итогам уничтожения таких данных составляет акт об уничтожении персональных данных, соответствующий пунктам 3 и 4 Требований к подтверждению уничтожения персональных данных, и выгрузку из журнала, соответствующую пункту 5 настоящих Требований к подтверждению уничтожения персональных данных, утвержденных приказом Роскомнадзора от 28.10.2022 № 179.
4.4. Акты об уничтожении персональных данных подписываются членами Комиссии, уничтожившими данные, и утверждаются директором МБУ ДО «СШ по киокусинкай».
4.5. Акты о выделении документов, содержащих персональные данные субъектов
персональных данных, к уничтожению хранятся у ответственного за организацию обработки персональных данных в течение срока хранения, предусмотренного номенклатурой дел, затем акты передаются в архив МБУ ДО «СШ по киокусинкай».
4.6. Акты об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных хранятся у ответственного за организацию обработки персональных данных в течение трех лет с момента уничтожения персональных данных.

5. Порядок обезличивания персональных данных
5.1. В случае невозможности уничтожения персональных данных они подлежат обезличиванию, в том числе для статистических и иных исследовательских целей.

5.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- замена части данных идентификаторами;
- обобщение, изменение или удаление части данных;
- деление данных на части и обработка в разных информационных системах;
- перемешивание данных.

5.3. Ответственным за обезличивание персональных данных является работник, ответственный за организацию обработки персональных данных.

5.4. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный за организацию обработки персональных данных.

5.5. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

5.6. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

5.7. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

5.8. В процессе обработки обезличенных данных в случаях, установленных законодательством Российской Федерации, может производиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

Приложение № 1

к Порядку уничтожения
и обезличивания персональных данных

УТВЕРЖДАЮ
Ответственный за организацию обработки персональных данных
МБУ ДО «СШ по киокусинкай»
_____

А К Т

_____ № _____ г. о. Коломна

о выделении к уничтожению носителей, содержащих персональные данные

На основании требований законодательства Российской Федерации о персональных данных и локальных нормативных актов МБУ ДО «СШ по киокусинкай» комиссия по уничтожению персональных данных отобрала к уничтожению носители, содержащие персональные данные:

№ п/п	Заголовок дела (групповой заголовок документов)	Носитель	Номер описи	Номер ед. хр. по описи	Количество ед. хр.	Сроки хранения и номера статей по перечню	Примечание
1	2	3	4	5	6	7	8
<…>	<…>	<…>	<…>	<…>	<…>	<…>	<…>
7	График отпусков за 20__ год	Бумага	05/2015	05-15	1	3 года, статья 453	—
8	Табель учета рабочего времени за 20__ год	Бумага	05/2011	05-11	12	5 лет, статья 402	—
<…>	<…>	<…>	<…>	<…>	<…>	<…>	<…>

Итого: 10 (десять) единиц.

Комиссия в составе:

Ответственного за организацию обработки персональных данных	_____	ФИО
Заместителя директора	_____	ФИО
Секретаря	_____	ФИО

Приложение № 2

к Порядку уничтожения
и обезличивания персональных данных

УТВЕРЖДАЮ
Ответственный за организацию обработки персональных данных
МБУ ДО «СШ по киокусинкай»
_____

А К Т

_____ № _____ г. о. Коломна
об уничтожении персональных данных,
обрабатываемых без использования средств автоматизации

Комиссия по уничтожению персональных данных, созданная на основании приказа директора МБУ ДО «СШ ПО КИОКУСИНКАЙ» от _____.202__ № ____, составила акт о том, что _____.202__г. уничтожила нижеперечисленные носители, содержащие персональные данные, а именно:

Наименование материального носителя, кол-во листов	**Категории уничтоженных пересданных**	**Информация о лицах, чьи данные уничтожили**	**Способ уничтожения**	**Причина уничтожения**
Журналы учета занятий за 20__ – 20___ гг., 540	**Ф.И.О. Медицинская группа здоровья**	**Обучающиеся _____ групп**	**Измельчение в шредере**	**Дубль оригинала в электронном виде**
График отпусков за 20____ год, 10	**Ф.И.О. Должность**	**Работники МБУ ДО СШ**	**Измельчение в шредере**	**Истек срок хранения**
Табель учета рабочего времени за 20___ год, 30	**Ф.И.О. Должность Сведения о работе**	**Работники МБУ ДО СШ**	**Измельчение в шредере**	**Истек срок хранения**
…	**…**	**…**	**…**	**…**

Настоящий акт составили:

Ответственный за организацию обработки персональных данных _____ ФИО

Заместитель директора _____ ФИО

Секретарь _____ ФИО

Приложение № 3

к Порядку уничтожения
и обезличивания персональных данных

УТВЕРЖДАЮ
Ответственный за организацию обработки персональных данных
МБУ ДО «СШ по киокусинкай»
_____

А К Т

_____ № _____ г. о. Коломна
об уничтожении персональных данных, обрабатываемых с использованием средств автоматизации

Комиссия по уничтожению персональных данных, созданная на основании приказа директора МБУ ДО «СШ ПО КИОКУСИНКАЙ» от _____.202__ № ____, составила акт о том, что _____.202_г. уничтожила персональные данные, а именно:

Наименование ИСПДн	**Наименование документа**	**Категории Уничтоженных персданных**	**Информация о лицах, чьи данные уничтожили**	**Способ уничтожения**	**Причина уничтожения**
1С: Делопроизводство	График отпусков за 2019 год	Ф.И.О. Должность	Работники	Удаление	Истечение сроков хранения
1С: Делопроизводство	Табель учета рабочего времени за 2017 год	Ф.И.О. Должность Сведения о работе	Работники	Удаление	Истечение сроков хранения
…		…	…	…	…

Настоящий акт составили:

Ответственный за организацию обработки персональных данных _____ ФИО

Заместитель директора _____ ФИО

Секретарь _____ ФИО

Приложение № 4

к Порядку уничтожения
и обезличивания персональных данных

Форма выгрузки из журнала регистрации событий в информационной системе персональных данных

Наименование ИСПДн				
Дата	**Событие (уничтожение персданных)**	**Категории уничтоженных персданных**	**Информация о лицах, чьи данные уничтожили**	**Причина уничтожения***

* Если ИСПДн не позволяет отобразить причину уничтожения, ответственный за уничтожение указывает ее вручную