РАССМОТРЕНО
Общим собранием работников
Протокол № 03 от 17.06.2026 г

УТВЕРЖДЕНО
Приказом
МАУ ДО "СШ №10"
от «17» июня 2026 г. № 129
О.В.Зайнеева

ПОЛОЖЕНИЕ
о порядке организации и проведении работ по защите ПДн в ИСПДн

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке организации и проведении работ по защите персональных данных в информационных системах персональных данных (далее — Положение) МУНИЦИПАЛЬНОГО АВТОНОМНОЕГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА НАБЕРЕЖНЫЕ ЧЕЛНЫ "СПОРТИВНАЯ ШКОЛА №10" (далее — Организация) определяет порядок организации и проведения работ по обеспечению безопасности персональных данных (далее — ПДн) при их обработке в информационных системах персональных данных (далее — ИСПДн).

1.2. Положение разработано в соответствии с требованиями:

— Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

— ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

— ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

— иных нормативных правовых актов Российской Федерации в области обработки и защиты персональных данных.

1.3. Действие настоящего Положения распространяется на все структурные подразделения Организации, осуществляющие обработку ПДн в ИСПДн, и является

обязательным для исполнения всеми работниками Организации, допущенными к обработке ПДн.

1.4. Ответственность за организацию обработки ПДн в Организации возлагается на директора Организации.

1.5. Ответственность за обеспечение безопасности ПДн в ИСПДн возлагается на заместителя директора Организации.

1.6. Контроль за соблюдением требований настоящего Положения осуществляет директор .

Сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОРД	Организационно-распорядительная документация
ПДн	Персональные данные
ПО	Программное обеспечение
САВЗ	Средство антивирусной защиты
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
УЗ	Уровень защищённости
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ФСБ России	Федеральная служба безопасности Российской Федерации

2. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИИ

2.1. В Организации эксплуатируются информационные системы персональных данных, предназначенные для обработки ПДн Действующие работники организации; Уволенные работники организации; Соискатели вакантных должностей; Родственники работников; Практиканты и стажёры; Законные представители клиентов; Члены организации; Заявители (авторы обращений); Участники закупок (44-ФЗ, 223-ФЗ); Представители организаций-контрагентов; Посетители сайта; Зарегистрированные пользователи; Подписчики рассылок; Посетители помещений (пропускной режим); Обучающиеся; Индивидуальные предприниматели и самозанятые.

2.2. Для ИСПДн Организации установлены актуальные угрозы третьего типа.

2.3. По результатам определения уровня защищённости для ИСПДн Организации установлен УЗ-3 (3-й уровень защищённости персональных данных).

2.4. В ИСПДн Организации применяются средства криптографической защиты информации класса КС2.

2.5. Состав и структура ИСПДн определены в Перечне информационных систем персональных данных, утверждённом приказом Организации.

2.6. Перечень обрабатываемых персональных данных, категории субъектов, цели обработки определены в соответствующих перечнях, утверждённых приказами Организации.

3. ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Организация работ по обеспечению безопасности ПДн при их обработке в ИСПДн осуществляется заместителем директором Организации путём:

— издания организационно-распорядительных документов по вопросам обработки и защиты ПДн;

— назначения лиц, ответственных за организацию обработки и обеспечение безопасности ПДн;

— организации режима обеспечения безопасности помещений, в которых размещены ИСПДн;

— определения угроз безопасности ПДн при их обработке в ИСПДн;

— применения организационных и технических мер по обеспечению безопасности ПДн;

— оценки эффективности принимаемых мер по обеспечению безопасности ПДн;

— учёта машинных носителей ПДн;

— обнаружения фактов несанкционированного доступа к ПДн и принятия мер;

— восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

— установления правил доступа к ПДн, обрабатываемым в ИСПДн;

— контроля за принимаемыми мерами по обеспечению безопасности ПДн.

3.2. Директор обеспечивает:

— организацию и контроль работ по обработке ПДн в соответствии с требованиями законодательства;

— разработку и актуализацию локальных нормативных актов по вопросам обработки ПДн;

— взаимодействие с Роскомнадзором по вопросам обработки ПДн;

— рассмотрение обращений субъектов ПДн;

— организацию обучения работников по вопросам обработки и защиты ПДн.

3.3. Заместитель директора обеспечивает:

— планирование и организацию работ по защите ПДн в ИСПДн;

— разработку и актуализацию модели угроз безопасности ПДн;

— выбор и внедрение средств защиты информации;

— контроль функционирования системы защиты ПДн;

— организацию работ с криптографическими средствами защиты информации;

— проведение внутреннего контроля соответствия обработки ПДн установленным требованиям;

— расследование инцидентов информационной безопасности.

4. УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Управление системой защиты ПДн осуществляется на основе:

— результатов анализа актуальных угроз безопасности ПДн;

— класса ИСПДн и уровня защищённости ПДн;

— результатов оценки вреда субъектам ПДн;

— анализа эффективности реализованных мер защиты.

4.2. Определение состава и выбор средств защиты информации для ИСПДн осуществляется в соответствии с УЗ-3 на основе:

— модели угроз безопасности ПДн;

— требований приказа ФСТЭК России от 18.02.2013 № 21;

— требований приказа ФСБ России от 10.07.2014 № 378 для средств криптографической защиты информации;

— результатов анализа применимости мер защиты.

4.3. Пересмотр и актуализация модели угроз и системы защиты ПДн проводится:

— не реже одного раза в 3 года в плановом порядке;

— при изменении характеристик ИСПДн;

— при изменении законодательства в области защиты ПДн;

— при выявлении новых актуальных угроз безопасности ПДн.

4.4. Ввод в эксплуатацию ИСПДн осуществляется после:

— установки и настройки средств защиты информации;

— проведения предварительных испытаний;

— опытной эксплуатации;

— анализа уязвимостей ИСПДн;

— приёмочных испытаний.

4.5. Документирование процессов управления системой защиты ПДн включает:

— ведение журналов учёта СЗИ и машинных носителей ПДн;

— протоколирование событий безопасности;

— документирование изменений в составе и конфигурации ИСПДн;

— актирование результатов проверок и испытаний.

5. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Для обеспечения УЗ-3 в ИСПДн реализуются следующие меры защиты:

— идентификация и аутентификация субъектов доступа и объектов доступа;

— управление доступом субъектов доступа к объектам доступа;

— ограничение программной среды;

— защита машинных носителей ПДн;

— регистрация событий безопасности;

— антивирусная защита;

— обнаружение (предотвращение) вторжений;

— контроль (анализ) защищённости ПДн;

— обеспечение целостности ИСПДн и ПДн;

— обеспечение доступности ПДн;

— защита среды виртуализации (при использовании);

— защита технических средств;

— защита ИСПДн, её средств, систем связи и передачи данных;

— выявление инцидентов и реагирование на них;

— управление конфигурацией ИСПДн и системы защиты ПДн.

5.2. Криптографическая защита ПДн обеспечивается применением сертифицированных СКЗИ класса КС2 в соответствии с:

— приказом ФСБ России от 10.07.2014 № 378;

— эксплуатационной документацией на СКЗИ;
— инструкциями по работе со СКЗИ, утверждёнными в Организации.
5.3. Организационные меры защиты ПДн включают:
— организацию режима обеспечения безопасности помещений, препятствующего возможности неконтролируемого проникновения;
— обеспечение сохранности носителей ПДн;
— утверждение перечня лиц, доступ которых к ПДн необходим для выполнения служебных обязанностей;
— организацию учёта и хранения материальных носителей ПДн;
— использование средств защиты информации, прошедших процедуру оценки соответствия;
— назначение должностного лица, ответственного за обеспечение безопасности ПДн в ИСПДн;
— ограничение доступа к ПДн путём установления персональной ответственности.

6. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

6.1. Обработка ПДн в ИСПДн осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации.
6.2. Доступ к обработке ПДн в ИСПДн предоставляется работникам Организации в соответствии с перечнем должностей, утверждённым приказом Организации.
6.3. Допуск работников к обработке ПДн в ИСПДн осуществляется после:
— ознакомления с положениями законодательства о персональных данных;
— ознакомления с локальными нормативными актами по вопросам обработки ПДн;
— принятия обязательства о неразглашении ПДн;
— прохождения инструктажа по работе в ИСПДн.
6.4. Работники, допущенные к обработке ПДн, при работе в ИСПДн обязаны:
— знать и выполнять требования нормативных документов по обработке и защите ПДн;
— выполнять требования парольной политики при работе в ИСПДн;
— использовать только разрешённое программное обеспечение;
— немедленно сообщать о попытках несанкционированного доступа к ПДн;
— соблюдать правила работы со средствами защиты информации;
— не разглашать ПДн, ставшие известными в связи с исполнением должностных обязанностей.
6.5. При обработке ПДн в ИСПДн запрещается:
— обрабатывать ПДн в присутствии лиц, не допущенных к их обработке;
— передавать ПДн по открытым каналам связи без применения средств защиты;
— записывать и хранить ПДн на неучтённых носителях;
— оставлять без присмотра незаблокированное АРМ;
— самостоятельно устанавливать программное обеспечение;
— отключать средства защиты информации.

7. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

7.1. Защита ПДн от несанкционированного доступа обеспечивается:
— использованием средств защиты от несанкционированного доступа;
— разграничением прав доступа пользователей ИСПДн;

— регистрацией и учётом всех действий с ПДн в ИСПДн;
— контролем соблюдения парольной политики;
— применением средств антивирусной защиты;
— использованием средств межсетевого экранирования;
— контролем целостности программного обеспечения.
7.2. Разграничение доступа к ПДн в ИСПДн осуществляется на основе:
— перечня должностей работников, допущенных к обработке ПДн;
— матрицы доступа к информационным ресурсам;
— принципа минимальных привилегий;
— служебной необходимости.
7.3. Парольная защита в ИСПДн обеспечивается требованиями:
— длина пароля — не менее 6 символов для УЗ-3;
— использование букв в разных регистрах, цифр и специальных символов;
— срок действия пароля — не более 90 дней;
— запрет на использование ранее применявшихся паролей;
— блокировка учётной записи после 5 неудачных попыток входа.
7.4. Контроль физического доступа к техническим средствам ИСПДн включает:
— размещение технических средств в помещениях с контролируемым доступом;
— использование запираемых шкафов и сейфов для хранения носителей ПДн;
— опечатывание системных блоков АРМ;
— ведение журнала доступа в помещения ИСПДн.

8. ВЫЯВЛЕНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. К инцидентам информационной безопасности при обработке ПДн относятся:
— несанкционированный доступ к ПДн;
— нарушение конфиденциальности, целостности или доступности ПДн;
— утрата (хищение) носителей ПДн;
— нарушение правил обработки ПДн;
— сбои в работе средств защиты информации;
— заражение вредоносным программным обеспечением.
8.2. При выявлении инцидента информационной безопасности работник обязан:
— прекратить работу в ИСПДн;
— немедленно сообщить директору;
— зафиксировать обстоятельства инцидента;
— сохранить состояние рабочего места до прибытия ответственных лиц.
8.3. Директор при получении сообщения об инциденте:
— организует расследование инцидента;
— определяет масштаб и последствия инцидента;
— принимает меры по локализации инцидента;
— организует восстановление работоспособности ИСПДн;
— информирует ответственных лиц о результатах расследования.
8.4. В случае выявления факта неправомерной или случайной передачи ПДн, повлекшей нарушение прав субъектов ПДн, Организация обязана:
— в течение 24 часов уведомить Роскомнадзор о произошедшем инциденте;

— в течение 72 часов предоставить информацию о результатах внутреннего расследования;
— принять меры по устранению последствий инцидента.
8.5. По результатам расследования инцидента оформляется акт, содержащий:
— дату и время выявления инцидента;
— описание инцидента и его последствий;
— перечень затронутых ПДн и количество субъектов;
— принятые меры по устранению последствий;
— рекомендации по предотвращению подобных инцидентов.

9. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ УРОВНЯ ЗАЩИЩЁННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Контроль за обеспечением уровня защищённости ПДн включает:
— внутренний контроль соответствия обработки ПДн требованиям законодательства;
— контроль выполнения организационных и технических мер защиты;
— анализ эффективности системы защиты ПДн;
— аудит событий безопасности в ИСПДн.
9.2. Внутренний контроль проводится:
— в плановом порядке — не реже 1 раза в год;
— во внеплановом порядке — по решению Директора;
— при изменении законодательства о персональных данных;
— при модернизации ИСПДн.
9.3. При проведении внутреннего контроля проверяется:
— соблюдение условий обработки ПДн;
— актуальность организационно-распорядительных документов;
— выполнение мер по обеспечению безопасности ПДн;
— функционирование средств защиты информации;
— соблюдение порядка доступа в помещения ИСПДн;
— порядок резервного копирования и восстановления ПДн;
— своевременность реагирования на обращения субъектов ПДн.
9.4. Результаты контроля оформляются актом, который должен содержать:
— дату проведения контроля;
— основание проведения контроля;
— перечень проверенных мероприятий;
— выявленные нарушения и недостатки;
— рекомендации по устранению выявленных нарушений;
— сроки устранения нарушений.
9.5. Акты проверок хранятся в течение 5 лет.

10. ОТВЕТСТВЕННОСТЬ

10.1. Работники Организации, виновные в нарушении требований законодательства Российской Федерации в области персональных данных, несут ответственность в соответствии с законодательством Российской Федерации.

10.2. За нарушение требований настоящего Положения работники несут дисциплинарную ответственность в соответствии с Трудовым кодексом Российской Федерации.

10.3. Директор несёт ответственность за:

— организацию обработки ПДн в соответствии с требованиями законодательства;

— своевременное реагирование на обращения субъектов ПДн;

— взаимодействие с Роскомнадзором.

10.4. Заместитель директора несёт ответственность за:

— обеспечение безопасности ПДн при их обработке в ИСПДн;

— функционирование системы защиты ПДн;

— своевременное выявление и устранение уязвимостей в ИСПДн.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Настоящее Положение вступает в силу с даты его утверждения приказом директора.

11.2. Все работники Организации должны быть ознакомлены с настоящим Положением под подпись.

11.3. Изменения и дополнения в настоящее Положение вносятся приказом директора МАУ ДО "СШ №10".

11.4. Ответственность за поддержание настоящего Положения в актуальном состоянии возлагается на директора Организации.

Приложение
к Положению о порядке организации и
проведении работ по защите ПДн
в ИСПДн
МАУ ДО "СШ №10"

ЛИСТ ОЗНАКОМЛЕНИЯ

С настоящим документом ознакомлен(а) и обязуюсь выполнять его требования:

№	Фамилия, имя, отчество	Должность	Дата	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Лист согласования к документу № 402 от 06.07.2026
Инициатор согласования: Зайнеева О.В. Директор
Согласование инициировано: 06.07.2026 13:13

Лист согласования Тип согласования: **последовательное**

N°	ФИО	Срок согласования	Результат согласования	Замечания
1	Зайнеева О.В.		Подписано 06.07.2026 - 13:13	-