

УПРАВЛЕНИЕ ФИЗИЧЕСКОЙ
КУЛЬТУРЫ И СПОРТА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ
УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО
ОБРАЗОВАНИЯ
ГОРОДА НАБЕРЕЖНЫЕ ЧЕЛНЫ
«СПОРТИВНАЯ ШКОЛА № 10»



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФИЗИК КУЛЬТУРА
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
№ 00860914628E8856B03B2A91CBF7ACE88A
Владелец: Зайнеева Оксана Валерьяновна
Действителен с 25.11.2025 до 18.02.2027
«№10 СПОРТ ШКОЛА»
ЕСТӘМӘ БЕЛЕМ БИРҮ
МУНИЦИПАЛЬ АВТОНОМ
УЧРЕЖДЕНИЕСЕ

МАУ ДО «СШ № 10», 423803, г. Набережные Челны, улица им. Комарова, дом 23
тел./факс: (8552) 49-36-23; ИНН 1650081908,
Отделение-НБ РТ банка России/УФК по РТ г. Казань, р/с 03234643927300001100
ЛАГ 30800125-ДЮСШ10 (бюджет) ЛАВ 30800126-ДЮСШ10 (вне бюджет) БИК(Казань) 019205400

ПРИКАЗ

от 17 июня 2026 г.

№ 123

Об утверждении ОРД в области использования СКЗИ

В целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации (далее — СКЗИ) в МАУ ДО «СШ №10», в соответствии с требованиями приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», приказа Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», приказа Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Составы 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 защищенности»,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с «17» июня 2026 г. следующие организационно-распорядительные документы в области использования средств криптографической защиты информации в МАУ ДО «СШ №10»:

- Приложение № 1 — Положение по использованию средств криптографической защиты информации в МАУ ДО «СШ №10»;
- Приложение № 2 — Порядок доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ в МАУ ДО «СШ №10»;
- Приложение № 3 — Инструкция пользователя средств криптографической защиты информации в МАУ ДО «СШ №10»;
- Приложение № 4 — Инструкция ответственного пользователя средств криптографической защиты информации в МАУ ДО «СШ №10».

2. Ответственным пользователем СКЗИ в МАУ ДО «СШ №10» является директор Зайнеева Оксана Валерьяновна. Ответственный пользователь СКЗИ обеспечивает:

ПОЛОЖЕНИЕ по использованию СКЗИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по использованию средств криптографической защиты информации (далее — Положение) определяет порядок организации и обеспечения безопасности хранения, обработки и передачи информации с использованием средств криптографической защиты информации (далее — СКЗИ, криптосредства) в МУНИЦИПАЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА НАБЕРЕЖНЫЕ ЧЕЛНЫ "СПОРТИВНАЯ ШКОЛА №10" (далее — Организация).

1.2. Положение разработано в соответствии с требованиями следующих нормативных правовых актов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ Р 56115-2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования»;
- Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказ 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 защищенности».

1.3. Положение распространяется на все структурные подразделения Организации, работников и иных лиц, допущенных к работе со СКЗИ.

1.4. В Организации обработка персональных данных следующих категорий субъектов: Действующие работники организации; Уволенные работники организации; Соискатели вакантных должностей; Родственники работников; Практиканты и стажёры; Законные представители клиентов; Члены организации; Заявители (авторы обращений); Участники

1.4. В Организации обработка персональных данных следующих категорий субъектов: 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 осуществляется в информационных системах персональных данных с применением СКЗИ класса КС2 в соответствии с установленным УЗ-3.

1.5. Основные термины и определения, используемые в настоящем Положении:

Термин	Определение
Персональные данные	Любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (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
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных
Информационная система персональных данных (ИСПДн)	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе
Средство криптографической защиты информации (СКЗИ)	Шифровальные (криптографические) средства, используемые для защиты информации конфиденциального характера
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенных для осуществления криптографической защиты информации в течение определённого срока
Компрометация криптоключей	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам
Пользователь СКЗИ	Физическое лицо, непосредственно допущенное к работе со СКЗИ
Спецпомещение	Помещение, где установлены СКЗИ или хранятся ключевые документы к ним
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств
Ключевой документ	Физический носитель определённой структуры, содержащий ключевую информацию

2. ПОРЯДОК ПРИМЕНЕНИЯ КРИПТОСРЕДСТВ

2.1. СКЗИ применяются в Организации для защиты персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями Приказа ФСБ России от 10.07.2014 № 378.

2.2. Класс применяемых СКЗИ (КС2) определён в соответствии с установленным для ИСПДн Организации УЗ-3 и требованиями к составу мер по обеспечению безопасности персональных данных.

2.3. СКЗИ используются для реализации следующих функций защиты информации:

- шифрование персональных данных при их передаче по открытым каналам связи;
- обеспечение целостности и подлинности передаваемой информации;
- защита от несанкционированного доступа к персональным данным при их хранении на машинных носителях информации;
- формирование и проверка электронной подписи электронных документов;
- обеспечение защищённого удалённого доступа к ИСПДн.

2.4. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее — спецпомещения), осуществляется в соответствии с требованиями Приказа ФАПСИ от 13.06.2001 № 152.

2.5. Перечень спецпомещений Организации определяется отдельным приказом руководителя.

2.6. Контроль за соблюдением требований настоящего Положения осуществляет Директор Организации.

2.7. Пользователи СКЗИ обязаны проходить инструктаж по правилам работы с криптосредствами перед началом самостоятельной работы.

2.8. Факт прохождения инструктажа фиксируется в журнале, форма которого приведена в Приложении № 1 к настоящему Положению.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

3.1. Ответственным пользователем криптосредств в Организации является Директор.

3.2. Ответственный пользователь криптосредств обязан:

- организовать учёт всех экземпляров СКЗИ, эксплуатируемых в Организации;
- организовать учёт всех носителей ключевой информации к СКЗИ;
- обеспечить соблюдение требований по размещению, специальному оборудованию, охране и организации режима в спецпомещениях;
- организовать и контролировать выполнение мероприятий по обеспечению безопасности хранения, обработки и передачи информации с использованием СКЗИ;
- проводить инструктаж пользователей СКЗИ по правилам безопасной работы с криптосредствами;
- контролировать соблюдение пользователями СКЗИ требований эксплуатационной и технической документации на СКЗИ;
- осуществлять плановую смену ключей в соответствии с требованиями эксплуатационной документации на СКЗИ;
- принимать меры по предотвращению компрометации ключевой информации;
- в случае компрометации или подозрения на компрометацию ключей немедленно прекратить их использование и организовать внеплановую смену скомпрометированных ключей.

3.3. Ответственный пользователь криптосредств имеет право:

- требовать от пользователей СКЗИ соблюдения требований настоящего Положения;
- вносить предложения по совершенствованию мер защиты информации с использованием СКЗИ;

- приостанавливать работу пользователей СКЗИ в случае нарушения ими требований по эксплуатации криптосредств.

4. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ КРИПТОСРЕДСТВ

4.1. Пользователи криптосредств обязаны:

- соблюдать требования настоящего Положения и эксплуатационной документации на СКЗИ;
- использовать СКЗИ только для выполнения своих должностных обязанностей;
- обеспечивать сохранность предоставленных им носителей ключевой информации;
- не допускать появления в программной среде СКЗИ компьютерных вирусов и программ, не относящихся к СКЗИ;
- не вносить изменения в программное обеспечение СКЗИ;
- не разглашать содержимое носителей ключевой информации или передавать сами носители лицам, не имеющим допуска к работе с ними;
- немедленно уведомлять ответственного пользователя криптосредств об утрате или недостатке носителей ключевой информации, ключей от хранилищ, личных печатей, а также о фактах, которые могут привести к компрометации ключевой информации;
- сдавать носители ключевой информации ответственному пользователю криптосредств при увольнении или отстранении от работ, связанных с использованием СКЗИ.

4.2. Допуск пользователей к самостоятельной работе со СКЗИ оформляется заключением, форма которого приведена в Приложении № 2 к настоящему Положению.

4.3. При работе с СКЗИ пользователи обязаны соблюдать правила парольной защиты:

- длина пароля должна быть не менее 8 символов;
- пароль должен содержать буквы разных регистров, цифры и специальные символы;
- запрещается использовать в качестве пароля имена собственные, словарные слова, даты;
- пароль подлежит смене не реже одного раза в 90 дней.

5. ПОЛЬЗОВАТЕЛЯМ КРИПТОСРЕДСТВ ЗАПРЕЩАЕТСЯ

5.1. Пользователям криптосредств категорически запрещается:

- разглашать информацию о криптосредствах, в том числе ключевую информацию;
- записывать и хранить ключи в явном виде на носителях информации, в том числе на бумажных;
- использовать для шифрования ключи, не предназначенные для этих целей;
- передавать криптосредства и ключевые документы лицам, не допущенным к работе с ними;
- выносить криптосредства и ключевые документы из спецпомещений без разрешения ответственного пользователя криптосредств;
- оставлять без присмотра криптосредства, ключевые документы, а также компьютеры с установленными СКЗИ в режиме обработки информации;
- самостоятельно вскрывать, ремонтировать или вносить изменения в конструкцию СКЗИ;
- использовать СКЗИ при обнаружении их неисправностей;

- подключать СКЗИ к линиям связи, не предназначенным для работы с криптосредствами;
- изготавливать копии ключевых документов без письменного разрешения ответственного пользователя криптосредств.

6. ПОРЯДОК УЧЁТА КРИПТОСРЕДСТВ. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ

6.1. Все СКЗИ, эксплуатируемые в Организации, подлежат поэкземпляроному учёту. Учёт осуществляется в журнале, форма которого приведена в Приложении № 4 к настоящему Положению.

6.2. Каждому экземпляру СКЗИ присваивается учётный номер, который наносится на корпус изделия или вкладывается внутрь корпуса на бумажном носителе.

6.3. При получении СКЗИ проверяется комплектность поставки, целостность упаковки, наличие и целостность печатей (пломб).

6.4. Установка и ввод в эксплуатацию СКЗИ оформляется актом, форма которого приведена в Приложении № 3 к настоящему Положению.

6.5. Носители ключевой информации учитываются в лицевых счетах пользователей СКЗИ, форма которых приведена в Приложении № 5 к настоящему Положению.

6.6. Компрометацией ключей считаются следующие события:

- утрата носителей ключевой информации;
- утрата ключей от хранилищ, в которых хранятся носители ключевой информации;
- нарушение правил хранения и уничтожения носителей ключевой информации;
- возникновение подозрений в утечке информации о ключах или их несанкционированном копировании;
- нарушение печатей на аппаратных СКЗИ или иные попытки несанкционированного доступа к ключевой информации.

6.7. В случае компрометации ключей пользователь СКЗИ обязан:

- немедленно прекратить использование скомпрометированных ключей;
- немедленно доложить о факте компрометации ответственному пользователю криптосредств;
- действовать в соответствии с указаниями ответственного пользователя криптосредств.

6.8. При компрометации ключей ответственный пользователь криптосредств обязан:

- организовать немедленное прекращение использования скомпрометированных ключей всеми пользователями;
- провести служебное расследование обстоятельств компрометации;
- организовать внеплановую смену скомпрометированных ключей;
- доложить о факте компрометации Директору Организации.

7. ПОРЯДОК УНИЧТОЖЕНИЯ КРИПТОСРЕДСТВ

7.1. Уничтожение СКЗИ и носителей ключевой информации производится в следующих случаях:

- истечение срока действия ключевой информации;
- выход СКЗИ из строя (при невозможности ремонта);
- компрометация ключевой информации;

- прекращение использования конкретного экземпляра СКЗИ;
- непригодность носителей ключевой информации для дальнейшего использования.

7.2. Решение об уничтожении СКЗИ и носителей ключевой информации принимается комиссией, создаваемой приказом Директора.

7.3. В состав комиссии включаются не менее трёх человек, в том числе ответственный пользователь криптосредств.

7.4. Уничтожение производится способами, исключающими возможность восстановления информации:

- для магнитных носителей — размагничивание с последующим физическим разрушением;
- для оптических носителей — физическое разрушение;
- для флеш-накопителей — многократная перезапись случайными данными с последующим физическим разрушением;
- для бумажных носителей — сжигание или измельчение в шредере с размером фрагментов не более 2×15 мм.

7.5. По факту уничтожения составляется акт в двух экземплярах, который подписывается всеми членами комиссии.

7.6. В акте уничтожения указываются:

- дата и место уничтожения;
- основание для уничтожения;
- состав комиссии;
- перечень уничтожаемых СКЗИ и носителей ключевой информации с указанием их учётных номеров;
- способ уничтожения.

7.7. Первый экземпляр акта хранится у ответственного пользователя криптосредств, второй — в архиве Организации в течение 5 лет.

8. ОХРАНА И ОРГАНИЗАЦИЯ РЕЖИМА В СПЕЦПОМЕЩЕНИЯХ

8.1. Спецпомещения должны размещаться в пределах контролируемой зоны Организации.

8.2. Двери спецпомещений должны быть постоянно закрыты на замок и опечатаны личными печатями ответственных лиц.

8.3. Ключи от спецпомещений хранятся у ответственного пользователя криптосредств и его заместителя.

8.4. Хранилища ключевых документов (сейфы, металлические шкафы) должны быть оборудованы замками и опечатываться.

8.5. Учёт металлических хранилищ ведётся в журнале, форма которого приведена в Приложении № 6 к настоящему Положению.

8.6. В спецпомещениях запрещается:

- проводить работы, не связанные с использованием СКЗИ;
- хранить личные вещи и предметы, не имеющие отношения к работе;
- оставлять посторонних лиц без присмотра;
- курить, принимать пищу;
- использовать бытовые электроприборы.

8.7. При обнаружении нарушения целостности печатей, замков, дверей спецпомещений или хранилищ необходимо:

- немедленно доложить ответственному пользователю криптосредств;
- не входить в помещение и не трогать хранилище до прибытия ответственных лиц;
- обеспечить сохранность следов проникновения.

8.8. Плановая проверка соблюдения условий использования СКЗИ в спецпомещениях проводится не реже одного раза в квартал. Результаты проверки оформляются актом, форма которого приведена в Приложении № 7 к настоящему Положению.

9. ПОРЯДОК ДОСТУПА К ХРАНИЛИЩАМ КРИПТОСРЕДСТВ

9.1. Доступ к хранилищам криптосредств имеют только лица, включённые в список, утверждённый приказом Директора.

9.2. Хранилища должны открываться только в присутствии не менее двух лиц из числа допущенных.

9.3. При каждом вскрытии хранилища производится проверка наличия находящихся в нём СКЗИ и носителей ключевой информации.

9.4. Факт вскрытия хранилища фиксируется в техническом (аппаратном) журнале, форма которого приведена в Приложении № 8 к настоящему Положению.

9.5. В журнале указываются:

- дата и время вскрытия хранилища;
- фамилии лиц, присутствовавших при вскрытии;
- цель вскрытия;
- перечень изъятых или помещённых в хранилище предметов;
- результаты проверки наличия.

9.6. После закрытия хранилища опечатывается личными печатями присутствовавших лиц.

9.7. При обнаружении недостачи СКЗИ или носителей ключевой информации:

- составляется акт о недостаче;
- проводится служебное расследование;
- принимаются меры по розыску недостающих предметов;
- при необходимости информируются правоохранительные органы.

10. ОТВЕТСТВЕННОСТЬ

10.1. Ответственность за организацию работ по использованию СКЗИ в Организации возлагается на Директор.

10.2. Ответственность за соблюдение требований по эксплуатации СКЗИ, обеспечение сохранности криптосредств и носителей ключевой информации возлагается на Директора.

10.3. Пользователи СКЗИ несут персональную ответственность за:

- сохранность предоставленных им криптосредств и носителей ключевой информации;
- соблюдение требований настоящего Положения и эксплуатационной документации на СКЗИ;
- неразглашение ключевой информации.

10.4. Лица, виновные в нарушении требований настоящего Положения, привлекаются к ответственности в соответствии с законодательством Российской Федерации и локальными нормативными актами Организации.

10.5. За разглашение ключевой информации, утрату криптосредств или носителей ключевой информации виновные лица могут быть привлечены к дисциплинарной, административной, уголовной и гражданско-правовой ответственности в соответствии с законодательством Российской Федерации.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Настоящее Положение вступает в силу с момента его утверждения приказом Директора Организации.

11.2. Изменения и дополнения в настоящее Положение вносятся приказом Директора Организации.

11.3. Контроль за соблюдением требований настоящего Положения осуществляет Директор Организации.

11.4. Настоящее Положение подлежит пересмотру не реже одного раза в три года, а также при изменении законодательства Российской Федерации в области защиты персональных данных и использования СКЗИ.

11.5. Все работники Организации, допущенные к работе со СКЗИ, должны быть ознакомлены с настоящим Положением под подпись.

11.6. Оригинал настоящего Положения хранится у Директора, копии — в структурных подразделениях, использующих СКЗИ.

**Приложение № 1. Журнал инструктажа пользователей СКЗИ
и ознакомления с нормативными правовыми актами по использованию СКЗИ
к Положению по использованию средств криптографической защиты информации в МАУ ДО "СП №10"**

ЖУРНАЛ
инструктажа пользователей СКЗИ и ознакомления с нормативными правовыми актами по использованию СКЗИ

Журнал начат: «__» _____ 20__ г.

Журнал окончен: «__» _____ 20__ г.

На _____ листах

№ п/п	Дата	Фамилия, имя, отчество	Должность	Подразделение	Наименование СКЗИ	Вид инструктажа	Наименование НПА	Тема инструктажа	Кто проводил	Подпись проводившего	Подпись получившего	Примечание

**Приложение № 2. Заключение о возможности самостоятельной работы со
средствами криптографической защиты информации
к Положению по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10"**

ЗАКЛЮЧЕНИЕ

о возможности самостоятельной работы со средствами криптографической защиты
информации

Комиссия в составе:

Председатель: _____
(должность, фамилия, инициалы)

Члены комиссии: _____
(должность, фамилия, инициалы)

(должность, фамилия, инициалы)

провела проверку знаний _____
(должность, фамилия, имя, отчество)

Проверяемый изучил:

- руководящие документы по защите информации с использованием СКЗИ;
- эксплуатационную документацию на СКЗИ;
- Положение по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10";
- должностную инструкцию в части работы со СКЗИ.

По результатам проверки знаний комиссия приняла решение:

(допустить/не допустить к самостоятельной работе)

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /
_____ / _____ /

«__» _____ 20__ г.

**Приложение № 3. Акт установки и ввода в эксплуатацию средств
криптографической защиты информации
к Положению по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10"**

АКТ
установки и ввода в эксплуатацию средств криптографической защиты информации

г. _____ «___» _____ 20__ г.

Комиссия в составе:

Председатель: _____

Члены комиссии: _____

составила настоящий акт о том, что произведена установка и ввод в эксплуатацию
следующих средств криптографической защиты информации:

№ п/п	Наименование СКЗИ	Заводской номер	Место установки

Приложение № 4. Журнал поэкземплярного учёта средств криптографической защиты информации, криптографических ключей и эксплуатационной документации к ним
к Положению по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10"

ЖУРНАЛ
поэкземплярного учёта средств криптографической защиты информации,
криптографических ключей и эксплуатационной документации к ним

Журнал начат: «__» _____ 20__ г.
Журнал окончен: «__» _____ 20__ г.
На _____ листах

Поэкземплярный учёт эксплуатационной и технической документации к СКЗИ,
криптографических ключей

№ п/п	Дата поступления	Откуда поступили	Наименование СКЗИ	Серийные номера	Количество	№ сопроводительного документа	Расписка в получении

**Приложение № 5. Лицевой счёт пользователя средств криптографической
защиты информации
к Положению по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10"**

ЛИЦЕВОЙ СЧЁТ
пользователя средств криптографической защиты информации

Фамилия, имя, отчество: _____
Должность: _____
Подразделение: _____
Номер и дата приказа о допуске к работе со СКЗИ: _____

Дата выдачи	Наименование СКЗИ или носителя ключевой информации	Серийный или учётный номер	От кого получен	Расписка в получении	Расписка в возврате

Приложение № 6. Журнал учёта хранилищ (металлических шкафов, сейфов и т.п.) и печатей к ним
к Положению по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10"

ЖУРНАЛ
учёта хранилищ (металлических шкафов, сейфов и т.п.) и печатей к ним

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО
ОБРАЗОВАНИЯ ГОРОДА НАБЕРЕЖНЫЕ ЧЕЛНЫ "СПОРТИВНАЯ ШКОЛА №10"

Журнал начат: «___» _____ 20__ г.
Журнал окончен: «___» _____ 20__ г.
На _____ листах

№ п/п	Дата поступления	Наименование хранилища	Инвентарный номер	Место установки	Номер и оттиск печати	Расписка в получении	Примечание

Приложение № 7. Акт периодической проверки наличия и состояния средств криптографической защиты информации и соблюдения условий их использования
к Положению по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10"

АКТ
периодической проверки наличия и состояния средств криптографической защиты
информации и соблюдения условий их использования

г. _____ «___» _____ 20__ г.

Комиссия в составе:

Председатель: _____

Члены комиссии: _____

провела проверку наличия и состояния средств криптографической защиты информации, а также соблюдения условий их использования.

В ходе проверки установлено:

1. Проверка наличия СКЗИ:

- по данным учёта числится: _____ экземпляров;
- фактически в наличии: _____ экземпляров;
- результат проверки: _____

2. Проверка наличия криптографических ключей:

- по данным учёта числится: _____ комплектов;
- фактически в наличии: _____ комплектов;
- результат проверки: _____

3. Проверка условий хранения СКЗИ и криптографических ключей:

- состояние хранилищ: _____
- состояние печатей: _____
- соблюдение режима в спецпомещениях: _____

4. Проверка соблюдения требований эксплуатационной документации:

5. Выводы и рекомендации:

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /
_____ / _____ /

Приложение № 8. Технический (аппаратный) журнал
к Положению по использованию средств криптографической защиты информации в
МАУ ДО "СШ №10"

1

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО
ОБРАЗОВАНИЯ ГОРОДА НАБЕРЕЖНЫЕ ЧЕЛНЫ "СПОРТИВНАЯ ШКОЛА №10"

Журнал начат: «__» _____ 20__ г.

Журнал окончен: «__» _____ 20__ г.

На _____ листах

№ п/п	Дата и время	Помещение	Хранилище	Цель вскрытия	ФИО присутствующих	Изъято	Помещено	Результат проверки	Подписи

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				

ИНСТРУКЦИЯ **ответственного пользователя СКЗИ**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция ответственного пользователя средств криптографической защиты информации (далее — СКЗИ) в МАУ ДО "СШ №10" (далее — Инструкция) определяет обязанности, права и порядок действий лица, назначенного ответственным пользователем СКЗИ, при эксплуатации криптографических средств, применяемых для защиты персональных данных в информационных системах персональных данных (далее — ИСПДн).

1.2. Инструкция разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состав 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»;
- Приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- иными нормативными правовыми актами Российской Федерации в области защиты персональных данных и криптографической защиты информации.

1.3. Действие настоящей Инструкции распространяется на лицо, назначенное ответственным пользователем СКЗИ в МАУ ДО "СШ №10", а также на всех работников, допущенных к работе с СКЗИ в пределах их компетенции.

1.4. Ответственным пользователем СКЗИ в МАУ ДО "СШ №10" является Директор (далее — ответственный пользователь СКЗИ).

1.5. Ответственный пользователь СКЗИ в своей деятельности руководствуется действующим законодательством Российской Федерации, настоящей Инструкцией, Положением по работе с СКЗИ МАУ ДО "СШ №10", а также эксплуатационной документацией на применяемые СКЗИ.

1.6. Ответственный пользователь СКЗИ подчиняется непосредственно Директору.

ИНСТРУКЦИЯ пользователя СКЗИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации (далее — Инструкция, СКЗИ) разработана в соответствии с требованиями следующих нормативных правовых актов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состав 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»;
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утверждена Приказом ФАПСИ от 13.06.2001 № 152).

1.2. Настоящая Инструкция определяет порядок работы пользователей со средствами криптографической защиты информации, применяемыми для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее — ИСПДн) МАУ ДО "СШ №10" (далее — Организация).

1.3. Для ИСПДн Организации установлен УЗ-3. Класс применяемых СКЗИ: КС2.

1.4. Действие настоящей Инструкции распространяется на всех работников Организации, допущенных к работе с СКЗИ в соответствии с приказом о допуске к СКЗИ.

1.5. Пользователь СКЗИ (далее — Пользователь), — работник Организации, непосредственно осуществляющий работу с СКЗИ (ключевыми носителями, криптографическими ключами, электронной подписью) в ходе выполнения своих должностных обязанностей.

1.6. Ответственным за организацию работ по криптографической защите информации является директор Организации (далее — Ответственный за СКЗИ).

ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ СКЗИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок доступа в помещения, в которых размещены средства криптографической защиты информации (далее — СКЗИ, помещения СКЗИ), разработан в МАУ ДО "СШ №10" (далее — Организация) в соответствии с требованиями следующих нормативных правовых актов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состав 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»;
- Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (далее — Инструкция ФАПСИ № 152).

1.2. Настоящий Порядок определяет правила допуска работников Организации и иных лиц в помещения, в которых размещены СКЗИ, ключевые документы к ним, а также серверное и коммуникационное оборудование информационных систем персональных данных (далее — ИСПДн), обрабатывающих персональные данные с использованием СКЗИ.

1.3. Требования настоящего Порядка являются обязательными для всех работников Организации, а также для сторонних лиц, которым предоставляется доступ в помещения СКЗИ.

1.4. Ответственным за организацию режима доступа в помещения СКЗИ является Директор (далее — ответственный за обеспечение безопасности персональных данных).

1.5. Ответственным за организацию обработки персональных данных в Организации является Директор.

1.6. Общее руководство обеспечением безопасности персональных данных осуществляется Директором.

1.7. Для ИСПДн Организации установлен УЗ-3. Класс применяемых СКЗИ: КС2.

Лист согласования			Тип согласования: последовательное	
N°	ФИО	Срок согласования	Результат согласования	Замечания
1	Зайнеева О.В.		 Подписано 06.07.2026 - 13:09	-