ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0296759800C0B293A84B02717194FF8892
Владелец: СОКОЛЕНКО ЮЛИЯ АЛЕКСАНДРОВНА
Действителен: с 15.04.2025 до 15.07.2026

ПРИЛОЖЕНИЕ №4
УТВЕРЖДЕНО
Приказом
МКУ ДО «ЦППМ и СП»
от 05.08.2025 № 139
«Об утверждении организационно-распорядительных документов в области использования средств криптографической защиты информации в МКУ ДО «ЦППМ и СП»
Директор
Соколенко Юлия Александровна

_____
(подпись, печать)

«___» _____ 2025 г.

ИНСТРУКЦИЯ

ответственного пользователя средств криптографической защиты информации в МКУ ДО «ЦППМ и СП»

1. Общие положения.

1.1. Настоящая Инструкция ответственного пользователя средств криптографической защиты информации (далее - Инструкция) определяет в МКУ ДО «ЦППМ и СП» права и обязанности ответственного за организацию эксплуатации средств криптографический защиты информации (далее – ответственный пользователь криптосредств), используемых для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
СКЗИ, криптосредство	Средство криптографической защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Информация	Сведения (сообщения, данные) независимо от формы их представления	ГОСТ Р 50922-2006
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенных для осуществления криптографической защиты информации в течение определенного срока	Приказ ФАПСИ от 13.06.2001 № 152
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию	Приказ ФАПСИ от 13.06.2001 № 152
Компрометация криптоключей	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам	Приказ ФАПСИ от 13.06.2001 № 152
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе	Приказ ФАПСИ от 13.06.2001 № 152
Пользователь СКЗИ	Физическое лицо, непосредственное допущенное к работе с СКЗИ	Приказ ФАПСИ от 13.06.2001 № 152
Спецпомещение	Помещение, где установлены СКЗИ или хранятся ключевые документы к ним	Приказ ФАПСИ от 13.06.2001 № 152
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера	Приказ ФАПСИ от 13.06.2001 №

Термин	Определение	Источник
	К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	152

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

приказ 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»,

приказ 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)»,

приказ Федеральной службы безопасности Российской Федерации 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 требованиям к защите персональных данных для каждого из уровней защищенности».

1.4. Ответственный пользователь криптосредств назначается приказом руководителя МКУ ДО «ЦППМ и СП». При смене Ответственного

пользователя криптосредств должны быть внесены соответствующие изменения в приказ «О назначении ответственного пользователя криптосредств в МКУ ДО «ЦППМ и СП».

1.5. Ответственный пользователь криптосредств должен быть ознакомлен с настоящей Инструкцией под подпись.

2. Обязанности ответственного пользователя криптосредств.

2.1. Ответственный пользователь криптосредств при эксплуатации СКЗИ должен выполнять требования нормативных и правовых актов Российской Федерации, Положения по использованию средств криптографической защиты информации, настоящей Инструкции, эксплуатационной, технической, и организационно-распорядительной документации для информационной системы персональных данных, в том числе для СКЗИ.

2.2. Ответственный пользователь криптосредств обязан:

проводить обучение пользователей криптосредств правилам работы с криптосредствами с оформлением Заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации и отметкой в Журнале ознакомления работников с нормативными правовыми актами Российской Федерации и локальными актами МКУ ДО «ЦППМ и СП» по обеспечению безопасности персональных данных с использованием криптосредств;

вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов с документальным оформлением в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

контролировать заполнение Акта установки и ввода в эксплуатацию средств криптографической защиты информации (Приложение №3 к Положению по использованию средств криптографической защиты информации в МКУ ДО «ЦППМ и СП»), делать отметку Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

хранить Акты установки и ввода в эксплуатацию средств криптографической защиты информации;

организовать надежное хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации, ключей от металлических хранилищ (сейфов);

вести учет лиц, допущенных к работе с СКЗИ. Формировать и актуализировать приказом МКУ ДО «ЦППМ и СП» Перечень лиц, допущенных к работе со средствами криптографической защиты информации в МКУ ДО «ЦППМ и СП»;

заводить и вести лицевые счета на каждого пользователя СКЗИ, в котором регистрировать числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;

выдавать СКЗИ, эксплуатационную и техническую документацию, ключевые документы пользователям криптосредств с документальным

оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

принимать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы от пользователя криптосредств при их увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

контролировать результаты уничтожения ключевых документов пользователями СКЗИ после окончания срока действия, не позднее 10 дней после вывода их из действия, если иной срок уничтожения не предусмотрен эксплуатационной и технической документацией к СКЗИ (Факт уничтожения оформляется под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

вести учет металлических хранилищ (сейфов), предназначенных для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов с документальным оформлением в Журнале учета металлический хранилищ (сейфов);

хранить в опечатанной упаковке дубликаты ключей от металлических хранилищ (сейфов);

передать дубликаты ключа от металлического хранилища (сейфа) ответственного пользователя криптосредств руководителю МКУ ДО «ЦППМ и СП» с документальным оформлением (под расписку в Журнале учета металлических хранилищ (сейфов);

хранить в опечатанной упаковке дубликаты ключей от входных дверей спецпомещений в металлическом хранилище (сейфе);

выдавать ключ от металлического хранилища (сейфа) пользователю криптосредства с документальным оформлением (под расписку в Журнале учета металлический хранилищ (сейфов);

принимать ключ от металлического хранилища (сейфа) при увольнении или отстранении от исполнения обязанностей работника, связанных с использованием СКЗИ, с документальным оформлением в Журнале учета металлический хранилищ (сейфов);

проводить не реже одного раза в год проверку создаваемой приказом МКУ ДО «ЦППМ и СП» комиссии (в состав комиссии включается Ответственный за организацию обработки персональных данных, Ответственный пользователя криптосредств), соблюдения условий использования криптосредств с оформлением акта проверки соблюдения использования средств криптографической защиты информации;

осуществлять контроль за соблюдением условий использования СКЗИ, предусмотренной эксплуатационной и технической документации к ним, обеспечением функционирования и безопасности СКЗИ и ключевых документов в пределах своих полномочий;

осуществлять контроль за выполнением пользователями СКЗИ требований к обеспечению безопасности персональных данных,

обрабатываемых в информационной системе персональных данных с использованием СКЗИ;

осуществлять контроль за ведением пользователем криптосредства технического (аппаратного) журнала в случае, если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ;

осуществлять контроль за установлением режима охраны спецпомещений пользователей СКЗИ, в том числе правила допуска работников и посетителей в рабочее и нерабочее время;

проводить периодический контроль за состоянием технических средств охраны (при их наличии) совместно с представителем службы охраны или дежурным по организации с отметкой в Журнале контроля состояния охранной сигнализации;

осуществлять контроль за проведением работ по размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ в спецпомещениях пользователей СКЗИ;

контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ пользователей криптосредств;

контролировать наличие и актуальность Перечня помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом руководителя МКУ ДО «ЦППМ и СП»;

контролировать наличие и актуальность Перечня лиц, имеющих право доступа в Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом руководителя МКУ ДО «ЦППМ и СП»;

соблюдать режим конфиденциальности информации, которая стала известной в процессе выполнения должностных (трудовых) обязанностей, в том числе сведений о криптоключах, паролях и применяемых СКЗИ, организации хранения, обработки и передачи связи информации с использованием СКЗИ;

выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных с использованием СКЗИ;

немедленно уведомлять руководителя МКУ ДО «ЦППМ и СП» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

своевременно выявлять попытки посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;

организовывать мероприятия по розыску и локализации последствий компрометации персональных данных в информационной системе персональных данных, передаваемых (хранящихся) с использованием СКЗИ.

3. Права ответственного пользователя криптосредств.

3.1. Ответственный пользователь СКЗИ имеет право:

требовать от пользователей СКЗИ соблюдения положений Положения по использованию средств криптографической защиты информации и Инструкции пользователя средств криптографической защиты информации;

обращаться к руководителю МКУ ДО «ЦППМ и СП» с предложением прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

инициировать проведение служебных проверок по фактам нарушения порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ персональных данных информационной системы персональных данных.

4. Ответственность.

4.1. Ответственный пользователь криптосредств несет ответственность за несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности СКЗИ, предназначенных для защиты персональных данных при их обработке в информационной системе персональных данных, в соответствии с действующим законодательством Российской Федерации.