



**АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТЕМРЮКСКИЙ РАЙОН**

РАСПОРЯЖЕНИЕ

от 02.04.2011

№ 168-р

г. Темрюк

**Об утверждении организационно-распорядительной документации по
защите персональных данных в администрации муниципального
образования Темрюкский район**

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и в целях обеспечения безопасности персональных данных, обрабатываемых на объектах информатизации администрации муниципального образования Темрюкский район:

1. Утвердить:

1) инструкцию по порядку учета применяемых средств защиты информации, эксплуатационной и технической документации к ним (приложение № 1);

2) инструкцию по защите технических средств информационной системы персональных данных (приложение № 2);

3) положение по использованию средств криптографической защиты информации (приложение № 3);

4) инструкцию ответственного пользователя средств криптографической защиты информации (приложение № 4);

5) инструкцию пользователя средств криптографической защиты информации (приложение № 5).

2. Назначить ответственными пользователями криптосредств:

1) заведующего сектором информатизации отдела информатизации и взаимодействия со СМИ Стешенко Вячеслава Анатольевича;

2) главного специалиста сектора информатизации отдела информатизации и взаимодействия со СМИ Булахова Сергея Евгеньевича.

3. Отделу информатизации и взаимодействия со СМИ официально разместить настоящее распоряжение на официальном сайте муниципального образования Темрюкский район в информационно-телекоммуникационной сети «Интернет» в течение 10 дней со дня его подписания.

4. Контроль за выполнением распоряжения «Об утверждении организационно-распорядительной документации по защите персональных данных в администрации муниципального образования Темрюкский район» возложить на исполняющего обязанности заместителя главы муниципального образования Темрюкский район Л.Е. Черную.

5. Настоящее распоряжение вступает в силу со дня его подписания.

Глава муниципального образования
Темрюкский район



Ф.В. Бабенков

ПРИЛОЖЕНИЕ № 1

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Темрюкский район
от 02.04.2021 № 168-р

ИНСТРУКЦИЯ **по порядку учета применяемых средств защиты информации,** **эксплуатационной и технической документации к ним**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по порядку учета применяемых средств защиты информации, эксплуатационной и технической документации к ним (далее – Инструкция) устанавливает в администрации муниципального образования Темрюкский район (далее – администрация) порядок учета применяемых средств защиты информации, эксплуатационной и технической документации к ним.

1.2. Инструкция распространяется на всех должностных лиц и работников администрации (далее – Пользователь), являющихся пользователями информационных систем персональных данных администрации (далее – ИСПДн).

2. ПОРЯДОК УЧЕТА И ХРАНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Используемые или хранимые дистрибутивы сертифицированных по требованиям безопасности средств защиты информации (далее – СрЗИ), эксплуатационная и техническая документация к ним подлежат поэкземплярному учету в Журнале поэкземплярного учета сертифицированных средств защиты информации, эксплуатационной и технической документации к ним (далее – Журнал учета СрЗИ) (приложение № 1). При этом программные СрЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные средства защиты подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие средства защиты информации учитываются также совместно с соответствующими аппаратными средствами.

2.2. Учет и актуализация информации по СрЗИ проводится в технических паспортах, оформляемых на каждую ИСПДн.

2.3. Эксплуатационная и техническая документация, а также электронные носители с инсталляционными файлами СрЗИ должны содержаться в хранилищах (шкафах, ящиках, сейфах и др.), исключая бесконтрольный

доступ к ним, а также их непреднамеренное уничтожение.

2.4. СрЗИ изымаются из эксплуатации по решению администратора безопасности ИСПДн. При этом вносятся необходимые изменения в Журнал учета СрЗИ и технические паспорта на ИСПДн, в составе которых эксплуатировались изъятые из эксплуатации СрЗИ.

2.5. Изменения в составе СрЗИ ИСПДн фиксируются актом или заявкой на модификацию программно–аппаратной среды.

2.6. Администратор безопасности ИСПДн обязан не реже 1 раза в квартал проводить актуализацию используемых СрЗИ, а также сроков окончания или продления сертификации.

2.7. Особенности учета средств криптографической защиты информации описаны в Положении по использованию средств криптографической защиты информации.

3. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

3.1. Пользователь несет ответственность за достоверность сведений, указанных им в заявке, а также обязан обо всех изменениях этих сведений сообщать незамедлительно администратору безопасности ИСПДн.

3.2. Пользователь несет ответственность за сохранность и правильность эксплуатации носителя цифровой информации и хранящихся на нем данных.

3.3. Пользователь несет ответственность за использование устройств чтения/записи, предоставленных ему для работы.

3.4. Пользователь несет имущественную и административную ответственность за последствия и убытки, нанесенные администрации, в случае нарушения положений Инструкции.

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

Приложение № 1

к Инструкции по порядку учета
применяемых средств защиты
информации, эксплуатационной и
технической документации к ним

ЖУРНАЛ
поэкземплярного учета сертифицированных средств защиты информации,
эксплуатационной и технической документации к ним

Начат: « ___ » _____ 20__ г.

Окончен: « ___ » _____ 20__ г.

Ответственный за ведение
журнала:

/ _____ / _____ / _____
(должность) (фамилия, инициалы) (подпись)

№ п/ п	Наименование средства защиты, эксплуатацион ной и технической документации	Регистрацион ные номера средства защиты, эксплуатацион ной и технической документации	Отметка о выдаче		Отметка о подключении (установке) средства защиты				Отметка об изъятии средства защиты из аппаратных средств		
			Ф.И.О. пользовате ля средства защиты	Дата и подпись в получе нии	Ф.И.О. пользователя средства защиты, производив шего подключе ние (установку)	Дата подключе ния (установки) и подписи лиц, произвед ших подключе ние (установку)	Номера аппарат ных средств, в которые установле ны средства защиты	Дата изъя тия	Ф.И.О. пользова теля средства защиты, произво дившего изъятие	Под пись об изъя тии	
1	2	3	4	5	6	7	8	9	10	11	

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 2

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Темрюкский район
от 02.04.2022 № 168-р

ИНСТРУКЦИЯ по защите технических средств информационной системы персональных данных

1. ВВЕДЕНИЕ

1.1. Инструкция по защите технических средств информационной системы персональных данных (далее – Инструкция) предназначена для обеспечения защищенности персональных данных (далее – ПДн), обрабатываемых в информационных системах персональных данных (далее – ИСПДн) администрации муниципального образования Темрюкский район (далее – администрация).

1.2. Инструкция определяет порядок действий администратора безопасности и пользователей ИСПДн при защите технических средств ИСПДн, в том числе технических средств системы защиты информации.

2. ОПРЕДЕЛЕНИЕ ГРАНИЦ КОНТРОЛИРУЕМОЙ ЗОНЫ

2.1. Границами контролируемой зоны ИСПДн являются внешние границы стен помещений (включая окна и двери), в которых размещено оборудование ИСПДн и ее средства защиты информации (далее – СЗИ).

2.2. Границы контролируемой зоны ИСПДн определяются распоряжением администрации.

2.3. Помещения, предназначенные для размещения технических средств ИСПДн и СЗИ, определены в эксплуатационной документации на системы защиты информации каждой ИСПДн.

2.4. Перемещение стационарного оборудования ИСПДн и СЗИ за границу контролируемой зоны не допускается.

2.5. Несанкционированный вынос за границу контролируемой зоны учетных машинных носителей, мобильных технических средств запрещен.

2.6. Несанкционированный внос пользователями ИСПДн неучтенных машинных носителей, мобильных технических средств запрещен.

3. ДОСТУП В КОНТРОЛИРУЕМУЮ ЗОНУ

3.1. На период обработки защищаемых ПДн в помещениях, где размещено оборудование ИСПДн и СЗИ, могут находиться только пользователи,

допущенные к обработке персональных данных.

3.2. Нахождение в помещениях контролируемых зон других лиц возможно только в присутствии пользователя, допущенного к обработке персональных данных.

3.3. Организацию физического доступа в помещения контролируемых зон ИСПДн осуществляет администратор безопасности.

4. ПРАВИЛА РАЗМЕЩЕНИЯ УСТРОЙСТВ ВЫВОДА ИНФОРМАЦИИ

4.1. При размещении в помещениях контролируемых зон технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации.

4.2. Размещение средств отображения информации указано в эксплуатационной документации на ИСПДн и эксплуатационной документации на системы защиты информации.

4.3. Выполнение требований к размещению устройств вывода информации в контролируемых зонах обеспечивает администратор безопасности.

5. ЗАЩИТА КАНАЛОВ СВЯЗИ

5.1. Технические средства для подключения ИСПДн к каналам связи, выходящими за пределы контролируемой зоны, должны быть размещены в пределах контролируемой зоны.

5.2. Расположение указанных технических средств и физический доступ к ним контролирует администратор безопасности.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Пользователи ИСПДн, должны быть предупреждены об ответственности за действия, нарушающие требования Инструкции.

6.2. Пользователи ИСПДн должны быть ознакомлены с Инструкцией до начала работы с ИСПДн, под подпись в листе ознакомлений. Обязанность ознакомления пользователей ИСПДн с Инструкцией лежит на ответственном за организацию обработки ПДн.

6.3. Сотрудники администрации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 3

УТВЕРЖДЕНО
распоряжением администрации
муниципального образования
Темрюкский район
от 22.04.2021 № 168-р

ПОЛОЖЕНИЕ по использованию средств криптографической защиты информации

1. ОПРЕДЕЛЕНИЯ

1.1. Ответственный пользователь криптосредств – пользователь, уполномоченный выполнять действия (имеющий полномочия) по администрированию (управлению) системы защиты информации информационной системы персональных данных в соответствии с установленной ролью.

1.2. Криптосредство - шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) – шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

1.3. Пользователь СКЗИ – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.4. Ответственный за организацию обработки персональных данных – должностное лицо организации, эксплуатирующей информационную систему персональных данных, отвечающее за организацию обработки персональных данных.

1.5. Криптоключ – секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Положение по использованию средств криптографической защиты информации (далее – Положение) по использованию средств криптографической защиты информации (далее – СКЗИ) в информационных системах персональных данных (далее – ИСПДн) администрации муниципального образования Темрюкский район (далее – администрация) разработано в соответствии со следующими нормативными правовыми актами и документацией на ИСПДн и ее системы защиты информации:

Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации,

информационных технологиях и защите информации»;

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 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 защищенности»;

Приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

Нормативно – техническим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) (утвержденным приказом Гостехкомиссии России от 30 августа 2002 года № 282);

ГОСТ Р 53114 – 2008 «Обеспечение информационной безопасности в организации. Основные термины и определения».

2.2. Положение предназначено для организации защиты персональных данных (далее – ПДн) с помощью СКЗИ.

2.3. Положение при использовании в ИСПДн СКЗИ используется в администрации совместно с организационно–распорядительными документами по управлению обработкой и защитой ПДн в ИСПДн.

2.4. Положение регламентирует порядок управления СКЗИ на стадии эксплуатации СКЗИ в составе системы защиты информации ИСПДн.

2.5. При использовании СКЗИ требования Положения имеют преимущество перед требованиями организационно-распорядительной документации по управлению обработкой и защитой ПДн в ИСПДн в отношении аналогичных объектов или процессов защиты.

2.6. Положение вступает в силу после его утверждения и действует бессрочно, до момента его замены новым.

Для обеспечения функционирования и безопасности СКЗИ глава муниципального образования Темрюкский район распоряжением назначает из числа сотрудников администрации ответственного пользователя криптосредств.

2.7. Обязанности ответственного пользователя криптосредств изложены в Инструкции пользователя средств криптографической защиты информации.

2.8. Все пользователи СКЗИ участвуют в защите ПДн, обрабатываемых в ИСПДн, и обязаны выполнять требования:

нормативных правовых документов по защите ПДн;
организационно – распорядительных документов по управлению системой защиты информации;
Положения в части их касающейся;
Инструкции пользователя средств криптографической защиты информации.

3. УПРАВЛЕНИЕ СКЗИ

3.1. Управление СКЗИ осуществляется администрацией с целью обеспечения безопасности обработки ПДн, с использованием криптосредств.

3.2. К управлению СКЗИ на этапе эксплуатации отнесены процедуры:
учет СКЗИ;

учет пользователей СКЗИ;

контроль соблюдения условий использования СКЗИ;

хранение, выдача, замена и уничтожение СКЗИ;

действия при утере и компрометации СКЗИ;

защита СКЗИ.

3.3. Учет СКЗИ осуществляет ответственный пользователь криптосредств в журнале учета СКЗИ, эксплуатационной и технической документации к ним.

3.4. Учет пользователей СКЗИ осуществляет ответственный пользователь криптосредств созданием и ведением лицевых счетов пользователей СКЗИ.

3.5. Условия использования СКЗИ в ИСПДн должны периодически, не реже 1 раза в год, проверяться на соответствие требованиям эксплуатации СКЗИ.

3.6. Проверки осуществляются постоянно действующей комиссией по обеспечению безопасности персональных данных администрации муниципального образования Темрюкский район.

3.7. Результаты проверок оформляются Актом результатов проверки условий использования СКЗИ по форме приложения № 1 к Положению.

3.8. В Акте результатов проверки условий использования СКЗИ должны быть отражены результаты проверки по следующим пунктам:

состояние и актуальность журнала учета СКЗИ;

состояние и актуальность журнала учета пользователей СКЗИ;

соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИСПДн и систему защиты информации;

знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ;

знание и выполнение пользователями правил защиты СКЗИ.

3.9. Если произошла потеря или компрометация СКЗИ, то ответственный за организацию обработки персональных данных назначает внеплановую проверку условий использования СКЗИ.

3.10. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи ответственный пользователь криптосредств должен немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

3.11. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с ответственным за организацию обработки персональных данных, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.12. При обнаружении недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения ответственный пользователь криптосредств организует срочные меры к их розыску.

4. ПРАВИЛА УЧЕТА СКЗИ

4.1. СКЗИ, используемые для обеспечения безопасности ПДн при их обработке в ИСПДн, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

4.2. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в журнале учета СКЗИ по форме приложения № 2 к Положению. Заполнение, хранение и ведение журнала учета СКЗИ осуществляет ответственный пользователь криптосредств.

4.3. Программные криптосредства учитываются в журнале учета СКЗИ совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

4.4. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств ИСПДн, то такие криптосредства учитываются совместно с соответствующими аппаратными средствами, о чем вносится соответствующая запись в журнале учета СКЗИ.

5. ПРАВИЛА ХРАНЕНИЯ СКЗИ

5.1. Пользователи криптосредств должны хранить устанавливающие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.2. Пользователи криптосредств должны обеспечить отдельное

безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

5.3. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. Опечатывание (опломбирование) осуществляет ответственный пользователь криптосредств.

5.4. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища. Отключение и уборку криптосредств в опечатываемые хранилища производит пользователь этих криптосредств.

6. ПРАВИЛА ВЫДАЧИ СКЗИ

6.1. Все экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов ответственный пользователь криптосредств выдает пользователям криптосредств под расписку в журнале поэкземплярного учета.

6.2. Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет по форме приложения № 3 к Положению, в котором регистрирует числящиеся за ним криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

6.3. Передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов пользователю криптосредств может производить только ответственный пользователь криптосредств под расписку в журнале поэкземплярного учета. Передача криптосредств между пользователями криптосредств запрещена.

7. ПРАВИЛА УНИЧТОЖЕНИЯ СКЗИ

7.1. Уничтожение криптоключей (исходной ключевой информации) производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

7.2. Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями

организации, производившей запись криптоключей (исходной ключевой информации).

7.3. Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

7.4. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

7.5. Криптосредства уничтожаются (утилизируют) по приказу руководителя администрации.

7.6. Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятими из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств, и они полностью отсоединены от аппаратных средств.

7.7. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

7.8. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения в журнал поэкземплярного учета заносит ответственный пользователь криптосредств.

7.9. Ключевые документы уничтожаются ответственным пользователем криптосредств.

7.10. Уничтожение большого объема ключевых документов может быть оформлено актом по установленной форме. Уничтожение по акту (приложение № 4 к Положению) производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, устанавливающих криптосредства носителей, эксплуатационной и технической документации.

8. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ ДЛЯ УСТАНОВКИ И ХРАНЕНИЯ СКЗИ

8.1. Помещения должны быть оснащены входными дверьми с замками, обеспечивающими постоянное закрытие дверей на замок и их открытия только для санкционированного прохода, а также опечатывания их по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

8.2. Должны быть утверждены правила доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях

8.3. Должен быть утвержден перечень лиц, имеющих право доступа в помещение.

8.4. Для предотвращения просмотра извне помещений, в которых установлены или хранятся СКЗИ, их окна должны быть защищены.

9. ТРЕБОВАНИЯ К РАЗМЕЩЕНИЮ И УСТАНОВКИ СКЗИ

9.1. Размещение и установка СКЗИ, а также другого оборудования, функционирующего с криптосредствами, в соответствующих помещениях должны сводить к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

9.2. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

10. ОТВЕТСТВЕННОСТЬ

10.1. Все пользователи криптосредств должны быть предупреждены об ответственности за действия с СКЗИ, нарушающие требования Положения и других организационных и правовых документов, определяющих меры по защите ПДн с помощью криптосредств.

10.2. Пользователи криптосредств, в том числе ответственный пользователь криптосредств должны быть ознакомлены в части их касающейся, с Положением до начала работы с криптосредствами под подпись. Обязанность ознакомления пользователей с Положением лежит на ответственном за организацию обработки персональных данных.

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 1
к Положению по использованию
средств криптографической
защиты информации

Акт № _____
проверки соблюдения условий использования
средств криптографической защиты информации

Дата составления: _____

Место проведение проверки: _____

Комиссия в составе:

Председатель

Члены комиссии

В соответствии с требованиями Положения по использованию средств криптографической защиты информации проведена проверка соблюдения условий использования средств криптографической защиты информации в информационной системе персональных данных ИСПДн.

В ходе проведения проверки определялись:

состояние и актуальность журнала учета СКЗИ;

состояние и актуальность журнала учета пользователей СКЗИ;

соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИС и систему защиты информации;

знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ;

знание и выполнение пользователями правил защиты СКЗИ;

случаи компрометации СКЗИ и действия по устранению причин и последствий компрометации СКЗИ;

состояние помещений с установленными или хранящимися в них СКЗИ и состояние режима доступа в эти помещения;

наличие и состояние хранилищ СКЗИ и режим доступа к ним.

Выявленные нарушения: _____

ЗАКЛЮЧЕНИЕ комиссии:

Соблюдений условий использования средств криптографической защиты информации **СООТВЕТСТВУЕТ** (НЕ СООТВЕТСТВУЕТ) требованиям к условиям использования СКЗИ в администрации муниципального образования

Темрюкский район.

Председатель комиссии:

Члены комиссии:

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 2
к Положению по использованию
средств криптографической
защиты информации

ЖУРНАЛ
учета средств криптографической защиты информации

Учетный № _____
2 _____ год. Листов (_____)

№ п/п	Наименование СКЗИ	Регистрационные номера СКЗИ	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ		Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов				
Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, производивших подключение (установку)	Номера аппаратных средств, в которых установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	Примечание
9	10	11	12	13	14	15

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 3

к Положению по использованию
средств криптографической
защиты информации

ЛИЦЕВАЯ КАРТОЧКА ПОЛЬЗОВАТЕЛЯ СКЗИ

Пользователь _____

№ п/п	Наименование СКЗИ	Регистрационные номера СКЗИ	Номера экземпляров ключевых документов	Дата получения	Примечание

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 4
к Положению по использованию
средств криптографической
защиты информации

АКТ № _____
уничтожения криптографических средств защиты информации

Проведен отбор СКЗИ, применяемых ранее в информационной системе персональных данных «_____», и установлено, что в соответствии с действующими требованиями отобранные СКЗИ подлежат уничтожению:

№	Дата	Наименование СКЗИ	Регистрационный номер СКЗИ	Номер экземпляра ключевых документов	Примечание

Всего экземпляров СКЗИ _____
(цифрами и прописью количество)

На указанных экземплярах СКЗИ информация уничтожена путем _____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные экземпляры СКЗИ уничтожены путем _____
(механического уничтожения, сжигания и т.п.)

Пользователь СКЗИ: _____ / _____ /
(подпись) (расшифровка)

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 4

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Темрюкский район
от 02.04.2021 № 168-р

ИНСТРУКЦИЯ ответственного пользователя средств криптографической защиты информации

1. ВВЕДЕНИЕ

1.1. Инструкция ответственного пользователя средств криптографической защиты информации (далее – Инструкция) регламентирует обязанности и действия ответственного пользователя средств криптографической защиты информации (далее – СКЗИ) при их использовании для защиты персональных данных (далее – ПДн), обрабатываемых в информационных системах персональных данных (далее – ИСПДн) администрации муниципального образования Темрюкский район (далее – администрация).

1.2. Инструкция дополняет комплект организационно-распорядительной документации (далее – ОРД) для ИСПДн, эксплуатируемой администрацией.

2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ПОЛЬЗОВАТЕЛЯ

2.1. Ответственный пользователь криптосредств назначается распоряжением администрации.

2.2. В ходе своей деятельности ответственный пользователь криптосредств обязан выполнять требования технической и эксплуатационной документации на использование СКЗИ, ОРД для ИСПДн.

2.3. Ответственный пользователь криптосредств обязан:
обучать пользователей криптосредств и контролировать соблюдение ими конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

организовать точное выполнение пользователями криптосредств требований к обеспечению безопасности ПДн, обрабатываемых в ИСПДн;

организовать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

организовать своевременное выявление попыток посторонних лиц получить сведения о защищаемой информации, об используемых крипто средствах или ключевых документах к ним;

немедленно принимать меры по предупреждению разглашения защищаемой информации, а также возможной ее утечки при выявлении фактов утраты или недостачи крипто средств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.;

контролировать организацию и обеспечение функционирования крипто средств в пределах своих служебных полномочий;

вести поэкземплярный учет СКЗИ и учет пользователей крипто средств;

проводить уничтожение и контролировать результаты уничтожения СКЗИ;

проводить мероприятия по розыску и локализации последствий компрометации ключевых документов.

3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

3.1. Ответственный пользователь крипто средств несет ответственность за действия с СКЗИ, нарушающие требования настоящего руководства и других организационных и правовых документов, определяющих меры по защите информации, в том числе персональных данных, с помощью крипто средств.

3.2. Ответственный пользователь крипто средств обязан ознакомиться с требованиями Инструкции.

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная

ПРИЛОЖЕНИЕ № 5

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Темрюкский район
от 12.04.2024 № 169-р

ИНСТРУКЦИЯ пользователя средств криптографической защиты информации

1. ВВЕДЕНИЕ

1.1. Инструкция пользователя средств криптографической защиты информации (далее – Инструкция) регламентирует обязанности и действия пользователя средств криптографической защиты информации (далее – СКЗИ) при их использовании для защиты персональных данных (далее – ПДн), обрабатываемых в информационных системах персональных данных (далее – ИСПДн) администрации муниципального образования Темрюкский район (далее – администрация).

1.2. Инструкция дополняет комплект организационно-распорядительной документации (далее – ОРД) для ИСПДн, эксплуатируемой администрацией.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Пользователи криптосредств допускаются к работе с ними по решению ответственного пользователя криптосредств.

2.2. При наличии двух и более пользователей криптосредств обязанности между ними распределяются с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.3. В ходе своей деятельности пользователи криптосредств обязаны выполнять требования технической и эксплуатационной документации на использование СКЗИ, ОРД по защите ПДн, обрабатываемых в ИСПДн. При выполнении своих обязанностей по криптографической защите информации пользователи криптосредств выполняют все требования и указания ответственного пользователя криптосредств.

2.4. Пользователи криптосредств обязаны:
проходить обучение пользованию криптосредствами;
не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

не допускать снятие копий с ключевых документов;

не допускать вывод ключевых документов на дисплей (монитор) автоматизированного рабочего места (далее – АРМ) или принтер;

не допускать записи на ключевой носитель посторонней информации;

соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

не допускать установки ключевых документов в непредназначенные для этого АРМ;

сообщать ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

немедленно уведомлять ответственного пользователя криптосредств о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации (в том числе персональных данных).

3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

3.1. Все пользователи криптосредств несут ответственность за действия с СКЗИ, нарушающие требования настоящего руководства и других организационных и правовых документов, определяющих меры по защите ПДн, с помощью криптосредств.

3.2. Пользователи криптосредств обязаны ознакомиться с требованиями Инструкции.

Исполняющий обязанности
заместителя главы
муниципального образования
Темрюкский район



Л.Е. Черная