



АДМИНИСТРАЦИЯ ЦИМЛЯНСКОГО РАЙОНА

РАСПОРЯЖЕНИЕ

19.03.2019

№ 58

г. Цимлянск

Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты (СКЗИ) в отделе ЗАГС Администрации Цимлянского района Ростовской области

В целях выполнения требований законодательства Российской Федерации в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты, 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 защищенности»:

1. Назначить ответственным пользователем криптосредств отдела ЗАГС Администрации Цимлянского района Ростовской области ведущего специалиста отдела ЗАГС Егорову Татьяну Васильевну.

2. Утвердить Инструкцию ответственного пользователя криптосредств отдела ЗАГС Администрации Цимлянского района Ростовской области, согласно приложению № 1.

3. Утвердить Перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных (пользователи криптосредств) отдела ЗАГС Администрации Цимлянского района Ростовской области, согласно приложению № 2.

4. Утвердить Инструкцию пользователя криптосредств отдела ЗАГС Администрации Цимлянского района Ростовской области, согласно приложению № 3.

5. Утвердить Перечень помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств,

приложению № 4.

6. Утвердить Перечень лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств, согласно приложению № 5.

7. Утвердить Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств, согласно приложению № 6.

8. Утвердить форму Журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов, согласно приложению № 7.

9. Утвердить форму Аппаратного журнала криптосредств, согласно приложению № 8.

10. Контроль за исполнением распоряжения возложить на заместителя главы Администрации района по социальной сфере Кузину С.Н.

Глава Администрации
Цимлянского района



В.В. Светличный

ИНСТРУКЦИЯ
ответственного пользователя криптосредств
отдела ЗАГС Администрации Цимлянского района Ростовской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция ответственного пользователя криптосредств отдела ЗАГС Администрации Цимлянского района Ростовской области (далее – Инструкция) определяет основные обязанности и права ответственного пользователя криптосредств.

1.2. Ответственный пользователь криптосредств назначается распоряжением Администрации Цимлянского района и отвечает за организацию, обеспечение функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.3. Ответственный пользователь криптосредств должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных, а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

1.4. В своей деятельности, связанной с обработкой персональных данных, ответственный пользователь криптосредств руководствуется настоящей Инструкцией.

**2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО
ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ**

Ответственный пользователь криптосредств обязан:

2.1. Соблюдать требования нормативных актов отдела ЗАГС, устанавливающих порядок работы с персональными данными.

2.2. Осуществлять контроль за организацией, обеспечением функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных:

– контролировать соблюдение условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

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

- вносить предложения по режиму охраны помещений, в которых установлены криптосредства или хранятся ключевые документы к ним;

- вести Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал);

- выдавать пользователям криптосредств экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов под расписку в соответствующем Журнале;

- вести на каждого пользователя криптосредств Лицевой счет, в котором регистрировать числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы;

- контролировать передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующем Журнале;

- пломбировать (опечатывать) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование криптосредств, а также аппаратных и аппаратно-программных криптосредствах;

- контролировать получение и доставку криптосредств, эксплуатационной и технической документации к ним;

- заблаговременно делать заказы на изготовление очередных ключевых документов и рассылку на места использования для своевременной замены действующих ключевых документов;

- контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку в соответствующем Журнале;

- выводить из действия носители ключевой информации (далее – НКИ), в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие НКИ;

- принимать решение в чрезвычайных случаях, когда отсутствуют НКИ для замены скомпрометированных, об использовании скомпрометированных НКИ;

- проводить инструктаж пользователей криптосредств по правилам работы с криптосредствами и ключевыми документами.

2.3. Требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ с криптосредствами или нарушения функционирования криптосредств.

2.4. Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей персональных данных, использования криптосредств,

которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.5. Контролировать исполнение пользователями криптосредств требований Инструкции пользователя криптосредствотдела ЗАГС Администрации Цимлянского района Ростовской области (далее – отдел ЗАГС) и прочих нормативных актов отдела ЗАГС в части обеспечения защиты персональных данных с помощью криптосредств.

2.6. Принимать все необходимые меры для обеспечения безопасности персональных данных, в случае получения от пользователей информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

- в каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводится служебное расследование; результатом расследования является квалификация или не квалификация данного события как компрометация;

- о факте компрометации ключевой информации пользователями криптосредств совместно с ответственным пользователем криптосредств производится информирование всех заинтересованных участников информационного обмена;

- выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в Журнале;

- для своевременного восстановления связи пользователю криптосредств выдается новый НКИ; для этого создаётся резервный запас НКИ, использование которых осуществляется в случаях крайней необходимости по решению ответственного пользователя криптосредств.

2.7. Подготавливать копии НКИ, которые подлежат основному учету и хранятся в сейфе ответственного пользователя криптосредств. Данные копии применяются с разрешения начальника отдела ЗАГС, если по результатам расследования не было установлено факта компрометации.

2.8. Хранить резервные НКИ отдельно от рабочих (актуальных) НКИ, с целью обеспечения невозможности их одновременной компрометации.

2.9. Своевременно информировать ответственного за организацию обработки персональных данных отдела ЗАГС 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 защищаемых персональных данных.

3. ПРАВА ОТВЕТСТВЕННОГО ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

Ответственный пользователь криптосредств имеет право:

3.1. Знакомиться с нормативными актами отдела ЗАГС, регламентирующими процессы обработки персональных данных.

3.2. Требовать от пользователей ИСПДн соблюдения требований нормативных актов отдела ЗАГС в части обеспечения защиты информации с помощью криптосредств.

3.3. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных пользователей криптосредств, в случае выявления нарушений требований по работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных, или в связи с нарушением функционирования криптосредств.

Исполняющий обязанности
управляющего делами



А.В. Кулик

ПЕРЕЧЕНЬ

сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных (пользователи криптосредств) отдела ЗАГС Администрации Цимлянского района Ростовской области

№ п/п	ФИО сотрудника	Должность
1.	Сосова Татьяна Владимировна	Начальник отдела ЗАГС
2.	Егорова Татьяна Васильевна	Ведущий специалист отдела ЗАГС
3.	Смирнова Екатерина Александровна	Специалист 1 категории отдела ЗАГС
4.	Понкратова Татьяна Николаевна	Специалист 1 категории отдела ЗАГС

Исполняющий обязанности
управляющего делами



А.В. Кулик

ИНСТРУКЦИЯ
пользователя криптосредств отдела ЗАГС
Администрации Цимлянского района Ростовской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция пользователя криптосредствотдела ЗАГС Администрации Цимлянского района Ростовской области (далее – Инструкция) определяет права и обязанности пользователей криптосредств, порядок обращения с криптосредствами, а также определяет порядок восстановления связи в случае компрометации действующих ключей к криптосредствам.

1.2. Пользователем криптосредств является сотрудник отдела ЗАГС Администрации Цимлянского района Ростовской области (далее – отдел ЗАГС), включенный в перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных, утвержденный нормативным актом отдела ЗАГС.

1.3. Непосредственно к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных, пользователи допускаются только после соответствующего обучения. Обучение пользователей правилам работы с криптосредствами осуществляют сотрудники соответствующего органа криптографической защиты. Заключение о допуске или не допуске к работе с криптосредствами должно быть отмечено в Журнале обучения пользователей правилам работы с криптосредствами.

1.4. Пользователь криптосредствдолжен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных, а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

1.5. В своей деятельности, связанной с обработкой персональных данных, пользователь криптосредств руководствуется настоящей Инструкцией.

1.6. Пользователи криптосредств несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту криптосредств от несанкционированного использования.

2. ОБЯЗАННОСТИ И ПРАВА ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

2.1. Пользователь криптосредств обязан:

- соблюдать требования по обеспечению безопасности функционирования криптосредств;
- обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;
- сдать ответственному пользователю криптосредств отдела ЗАГС (далее – Ответственный) носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;
- сдать Ответственному НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;
- немедленно уведомлять руководителя структурного подразделения или Ответственного о компрометации НКИ, о фактах утраты или недостачи криптосредств;
- в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования криптосредств.

2.2. Пользователю криптосредств запрещается:

- осуществлять несанкционированное и безучётное копирование ключевых данных;
- хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;
- передавать НКИ каким бы то ни было лицам, кроме Ответственного;
- во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);
- хранить на НКИ какую-либо информацию, кроме ключевой;
- использовать в помещениях, где применяются криптосредства, личные технические средства, позволяющие осуществлять копирование ключевой информации;
- использовать НКИ, выведенные из действия.

2.3. Пользователь имеет право:

- вносить предложения руководству отдела ЗАГС по вопросам использования криптосредств;
- повышать уровень квалификации по использованию криптосредств.

3. ПОРЯДОК ОБРАЩЕНИЯ С КРИПТОСРЕДСТВАМИ

3.1. Монтаж и установка криптосредства осуществляются органом криптографической защиты.

3.2. Служебные помещения, в которых размещаются криптосредства, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения НКИ помещения обеспечиваются сейфами (металлическими шкафами), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, опечатываются личными печатями ответственных лиц (либо закрываются кодовым замком) и сдаются под охрану.

3.3. Для хранения НКИ пользователь криптосредств должен быть обеспечен личным сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня пользователь криптосредств обязан сдавать НКИ Ответственному под подпись в Журнале учета и выдачи носителей с ключевой информацией.

3.4. Дубликаты ключей от сейфов (а также значения кодов – при наличии кодовых замков) пользователей криптосредств должны храниться в сейфе руководителя структурного подразделения или Ответственного в упаковках, опечатанных личными печатями пользователей криптосредств. Несанкционированное изготовление дубликатов ключей запрещено. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

3.5. К эксплуатации криптосредств допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным криптосредством.

3.6. Все программное обеспечение ПЭВМ, предназначенное для установки криптосредств, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую криптосредства, не допускается.

4. ВОССТАНОВЛЕНИЕ СВЯЗИ В СЛУЧАЕ КОМПРОМЕТАЦИИ ДЕЙСТВУЮЩИХ КЛЮЧЕЙ К КРИПТОСРЕДСТВАМ

4.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца НКИ и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- утрата (хищение) НКИ, в том числе – с последующим их обнаружением;
- увольнение (переназначение) сотрудников, имевших доступ к НКИ;
- передача секретных ключей по линии связи в открытом виде;
- нарушение правил хранения НКИ;
- вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);
- ошибки при совершении криптографических операций;
- несанкционированное или безучётное копирование ключевой информации;
- все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда НКИ вышел из строя и доказательно не опровергнута

вероятность того, что данный факт произошел в результате злоумышленных действий).

4.2. При наступлении любого из перечисленных выше событий пользователь криптосредств или владелец НКИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь криптосредств или владелец НКИ обязан убедиться, что его сообщение получено и прочтено.

4.3. При подтверждении факта компрометации действующих ключей пользователь криптосредств обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу Ответственному в течение 3 рабочих дней.

4.4. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь криптосредств получает у Ответственного новые ключи.

Исполняющий обязанности
управляющего делами



А.В. Кулик

Лист ознакомления

[illegible]

Приложение № 4
к распоряжению
Администрации
Цимлянского района
от 19.03.2019 № 58

ПЕРЕЧЕНЬ

помещений, где размещены используемые криптосредства, хранятся криптосредства
и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств

№ п/п	Адрес места расположения	Наименование структурного подразделения	Наименование помещения
1.	347320, Ростовская область, г.Цимлянск, ул. Ленина,15	Отдел ЗАГС Администрации Цимлянского района	Архив

Исполняющий обязанности
управляющего делами



А.В. Кулик

ПЕРЕЧЕНЬ

лиц, имеющих доступ в помещения, где размещены используемые
криптосредства, хранятся криптосредства и (или) носители ключевой,
аутентифицирующей и парольной информации криптосредств

№ п/п	ФИО Сотрудника	Должность
1.	Сосова Татьяна Владимировна	Начальник отдела ЗАГС
2.	Егорова Татьяна Васильевна	Ведущий специалист отдела ЗАГС
3.	Смирнова Екатерина Александровна	Специалист 1 категории отдела ЗАГС
4.	Понкратова Татьяна Николаевна	Специалист 1 категории отдела ЗАГС

Исполняющий обязанности
управляющего делами



А.В. Кулик

ПОРЯДОК
доступа в помещения, где размещены используемые
криптосредства, хранятся криптосредства и (или) носители ключевой,
аутентифицирующей и парольной информации криптосредств

1. Настоящий Порядок регламентирует условия и порядок осуществления доступа в помещения отдела ЗАГС Администрации Цимлянского района Ростовской области (далее – отдел ЗАГС), где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств (далее – Помещения) в целях организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

2. Настоящий Порядок разработан в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10 июля 2014 г. № 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», приказа ФАПСИ от 13 июня 2001 г. № 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».

3. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

4. Помещения, где размещены используемые криптосредства, хранятся криптосредства, должны быть оснащены входными дверьми с замками, должно обеспечиваться постоянное закрытие дверей таких Помещений на замок и их открытие только для санкционированного прохода. Данные Помещения должны опечатываться по окончании рабочего дня/оборудоваться соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии.

5. Доступ в Помещения в рабочее (служебное) время имеют сотрудники, включенные в Перечень лиц, имеющих доступ в Помещения, утвержденный нормативным актом отдела ЗАГС.

6. В нерабочее (неслужебное) время пребывание вышеуказанных сотрудников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных начальником отдела ЗАГС.

7. Нахождение в Помещениях посторонних лиц в рабочее (служебное) и нерабочее (неслужебное) время запрещается.

8. Уборка и техническое обслуживание Помещений допускаются только в присутствии Сотрудников отдела ЗАГС.

9. Руководитель и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.

10. О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать начальнику отдела ЗАГС.

11. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать начальнику отдела ЗАГС.

12. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении сотрудников, имеющих доступ в Помещения.

Исполняющий обязанности
управляющего делами



А.В. Кулик

Лист ознакомления

[illegible]

Приложение № 7
к распоряжению Администрации Цимлянского района
от 19.03.2019 № 58

ЖУРНАЛ

поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование криптосредства, эксплуатационной и технической документации и к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации и к ним, номера серийных ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств			Примечание	
				От кого получены	Дата и № сопроводит. докум.	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. работников произведших установку	Дата установки	Инв. № аппаратных средств, к которым подключены СКЗИ	Дата изъятия	Ф.И.О. работников произведших изъятие	№ акта (расписка) об уничтожении	Сфера применения	№ комнаты
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Исполняющий обязанности
управляющего делами



А.В. Кулик

А.В. Кулик

Аппаратный журнал СКЗИ

№ п/ п	Дата	Тип и серийные номера используе мых СКЗИ	Записи по обслужива нию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключево го докумен та	Серийный, криптографически й номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ в которую введены крипто ключи	Дата	Подпись пользовате ля СКЗИ	

Исполняющий обязанности
управляющего делами



А.В. Кулик

А.В. Кулик