

«28» августа 2025 г.

**ИНСТРУКЦИЯ
ПО ОБРАЩЕНИЮ С СЕРТИФИЦИРОВАННЫМИ ФСБ РОССИИ
СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – (СКЗИ)**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция регламентирует порядок обращения со средствами криптографической защиты информации (далее СКЗИ), сертифицированными ФСБ, в процессе получения, доставки, хранения, тестирования, передачи и установки (инсталляции).

1.2. СКЗИ, включая аппаратные средства, инсталляционные дискеты, ключевую документацию, описания и инструкции к СКЗИ, составляют служебную тайну <наименование учреждения>.

1.3. Сотрудники допускаются к работе с СКЗИ на основании приказа <должность руководителя> <наименование учреждения> после прохождения необходимой подготовки.

1.4. Приказом <должность руководителя> <наименование учреждения> назначаются лица, ответственные за обеспечение безопасности при обращении с СКЗИ.

1.5. Все сотрудники, допущенные к работе с СКЗИ, должны строго выполнять требования настоящей инструкции в части, их касающейся. Указанные сотрудники должны ознакомиться с данной инструкцией под роспись.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ СКЗИ

2.1. Пользователи СКЗИ обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать в ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- ведение технического (аппаратного) журнала;
- немедленно уведомлять ответственного пользователя криптосредств о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

3.1. Ответственный пользователь криптосредств обязан:

- контролировать соблюдение пользователями СКЗИ 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 СКЗИ и ключевых документах к ним;
- обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;
- своевременным выявлением попыток посторонних лиц получать сведения о защищаемой информации, об используемых криптосредствах или ключевых документах к ним;
- принимать меры по предупреждению разглашения защищаемой информации, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.
- контролировать соблюдение условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ;
- расследовать и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разрабатывать и принимать меры по предотвращению возможных опасных последствий подобных нарушений;
- вести журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- вести на каждого пользователя СКЗИ лицевой счет.

4. ТРЕБОВАНИЯ ПО РАЗМЕЩЕНИЮ, СПЕЦИАЛЬНОМУ ОБОРУДОВАНИЮ И ОХРАНЕ ПОМЕЩЕНИЙ, В КОТОРЫХ ПРОИЗВОДЯТСЯ РАБОТЫ С СКЗИ

4.1. Размещение, специальное оборудование, охрана и режим в помещениях, в которых производится работа с СКЗИ (далее - помещения), должны обеспечивать безопасность СКЗИ и исключать возможность неконтролируемого доступа к СКЗИ.

4.2. Доступ лиц в эти помещения должен быть ограничен и обеспечиваться в соответствии со служебной необходимостью и приказом *<должность руководителя>* *<наименование учреждения>*.

4.3. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, оборудованные надежными замками.

4.4. Входная дверь должна опечатываться металлической печатью, либо должна быть оборудована кодовым замком, код которого известен только сотрудникам, работающим в этом помещении.

4.5. По окончании рабочего дня ответственный сотрудник обязан закрыть помещение, опечатать помещение личной номерной печатью, сдать помещение под охрану с отметкой в журнале приема-сдачи помещений под охрану. При вскрытии помещений должны проверяться целостность печатей и замков. В случае нарушения целостности печатей или замков ответственный сотрудник обязан немедленно сообщить об этом лицу, ответственному пользователю криптосредств.

4.6. На дверях и оконных стеклах должны быть установлены датчики охранной сигнализации (при нахождении помещения вне крайних этажей допускается установка датчиков объемной сигнализации). В помещении должна быть установлена система пожарной сигнализации.

4.7. Для хранения СКЗИ, инсталляционных дискет, тестовых ключей, нормативной и эксплуатационной документации помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Сейфы должны быть оборудованы приспособлением для их опечатывания, либо специальным защитным замком для замочной скважины. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого *<должность руководителя> <наименование учреждения>*.

5. ПОРЯДОК ОБРАЩЕНИЯ С СКЗИ

5.1. СКЗИ, инсталляционные дискеты, тестовые ключи, нормативную и эксплуатационную документацию получает уполномоченный сотрудник *<наименование учреждения>* непосредственно у производителя СКЗИ. Безопасность в процессе доставки обеспечивается организационными мерами.

5.2. При транспортировке СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть обеспечены условия, исключающие возможность физических повреждений и внешнего воздействия на записанную информацию, а также копирование.

5.3. Все поступающие СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземпляруному учету.

5.4. Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

5.5. В соответствии с контрактом с производителем СКЗИ разрешается сделать одну копию программных СКЗИ (исключая ключевую информацию) для архива или обеспечения продажи, а также сделать одну дополнительную копию каждый раз, когда рабочая копия приходит в негодность и должна быть заменена. При этом ответственный сотрудник должен удостовериться, что каждая произведенная им копия отображает на дисплее авторские права производителя СКЗИ и другие указания в отношении собственности, которые записаны на оригинале.

5.6. Пользователи СКЗИ хранят 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.

5.7. Пользователи СКЗИ предусматривают также отдельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов. При вскрытии сейфа должна быть проверена целостность печатей и замков. В случае нарушения целостности печатей или замков ответственный сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

5.8. Хранение установочных дисков СКЗИ и тестовых ключей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами использования СКЗИ применение.

5.9. В случае отсутствия у сотрудника индивидуального хранилища установочные диски СКЗИ и тестовые ключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

5.10. В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

5.11. Ответственными сотрудниками периодически должен проводиться контроль сохранности СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

5.12. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно - программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

5.13. Ответственный сотрудник *<наименование учреждения>* заносит в Журнал учета СКЗИ дату приема-передачи СКЗИ, фамилию, имя, отчество сотрудника, которому передаются СКЗИ, серийный номера СКЗИ. Все операции по передаче СКЗИ производятся под роспись.

5.14. В каждый экземпляр передаваемого СКЗИ должна быть включена ссылка на авторские права производителя, его товарный знак и другие обозначения в форме, согласованной с производителем. Вся документация на СКЗИ и на продукты, включающие СКЗИ, а также отображаемая на экране при запуске информация о нем должна включать вышеуказанные обозначения.

5.15. Установка (инсталляция) СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

6. ВОССТАНОВЛЕНИЕ СВЯЗИ В СЛУЧАЕ КОМПРОМЕТАЦИИ ДЕЙСТВУЮЩИХ КЛЮЧЕЙ К СКЗИ

6.1. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

6.2. В случае возникновения обстоятельств, указанных в п.6.1 настоящей Инструкции, пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации ответственному пользователю криптосредств.

6.3. О факте компрометации ключевой информации Пользователями совместно с Ответственным пользователем производится информирование всех заинтересованных участников информационного обмена.

6.4. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

6.5. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в пункте 7 настоящей Инструкции.

7. УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

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

7.2. Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт - дисков (CD - ROM), eToken и т.п.). Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ.

7.3. Ключевые носители уничтожают 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 СКЗИ.

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

7.5. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали.

7.6. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. 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 оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная, и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация.

7.7. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

7.8. Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным пользователем СКЗИ под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом, форма акта представлена в Приложении №1 к данной инструкции. Ответственный пользователь СКЗИ обеспечивает хранение данных актов.

7.9. Пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом ответственного пользователя СКЗИ для списания уничтоженных документов с их лицевых счетов. Не реже одного раза в год пользователи СКЗИ должны направлять ответственному пользователю СКЗИ письменные отчеты об уничтоженных ключевых документах.

7.10. Ответственный пользователь СКЗИ делает соответствующие отметки об уничтожении в журнале поэкземплярного учета СКЗИ.

8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ИНСТРУКЦИИ

8.1. За нарушение требований настоящей Инструкции виновные в этом лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Разработал

Приложение №1 к Инструкции
по обращению с сертифицированными
ФСБ России средствами криптографической
защиты информации

АКТ № _____
об уничтожении криптографических ключей и ключевых документов

Комиссия в составе:

Председателя: _____,
членов комиссии: _____

произвела уничтожение криптографических ключей и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	Примечание

Всего уничтожено (_____) криптографических ключей на (_____) ключевых носителях. Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем их стирания в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Председатель комиссии: _____ / _____ /
Члены комиссии: _____ / _____ /
_____ / _____ /
_____ / _____ /
_____ / _____ /