Приложение № 1

Утверждена приказом
директора КОГОАУ «КЭПЛ»
от «03» 09_ 2021_г. № _83/6_

ИНСТРУКЦИЯ
по обращению с средствами криптографической защиты информации

Киров, 2021

Содержание

1. Общие положения

1.1. Назначение

Настоящая Инструкция содержит описание порядка организации и обеспечения функционирования сертифицированных Федеральной службой безопасности Российской Федерации средств криптографической защиты информации (далее СКЗИ), предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, обрабатываемой в информационных системах КОГОАУ «КЭПЛ» (далее - Организация).

СКЗИ эксплуатируются в соответствии с правилами пользования ими. Изменения условий эксплуатации СКЗИ, указанных в правилах пользования ими, допускаются исключительно по согласованию с ФСБ России.

1.2. Цель разработки Инструкции

Целью настоящего Порядка является:

обеспечение защиты персональных данных с использованием средств криптографической защиты информации;

обеспечение соответствия эксплуатации СКЗИ требованиям, установленным законодательством РФ и нормативными документами.

1.3. Область применения

Настоящий документ применяется:

к рабочим местам и сервисам, в которых применяются СКЗИ;

ко всем обособленным подразделениям Организации;

ко всем офисам и удаленным сотрудникам, независимо от их местоположения.

1.4. Аудитория

Инструкция предназначена для следующих категорий сотрудников Организации:

сотрудник, ответственный за СКЗИ;

администраторы СКЗИ;

сотрудники, выполняющие разработку программного обеспечения с использованием СКЗИ.

Под сотрудниками в настоящем положении понимаются лица, состоящие в трудовых отношениях с Организацией.

Все сотрудники, в обязанности которых входит работа с СКЗИ, кроме пользователей СКЗИ, должны быть ознакомлены с инструкцией, а также с документами, на которые она ссылается, в части их касающейся.

1.5. Нормативные ссылки

Настоящая Инструкция разработана в целях реализации следующих нормативных правовых актов:

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»;

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.

1.6. Срок действия и порядок внесения изменений в инструкцию

Инструкция действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим.

Документ подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, изменения оценки рисков информационной безопасности. Изменения в инструкцию вносятся путем издания новой версии и ознакомления с ней сотрудников.

Срок хранения после прекращения действия: постоянно.

1.7. Используемые сокращения

ИБ – информационная безопасность;

ОС – операционная система;

ПО – программное обеспечение;

ППО – прикладное программное обеспечение;

ПК – персональный компьютер;

СКЗИ - средства криптографической защиты информации;

ТС- технические средства;

ФСБ – Федеральная служба безопасности РФ

ЦОД – центр обработки данных.

2. Ответственные лица

Для эксплуатации сертифицированных СКЗИ в организации назначаются лица:

администратор СКЗИ;

пользователи СКЗИ.

Функции администратора СКЗИ могут быть возложены на одного из пользователей СКЗИ, либо на структурное подразделение или работника, ответственных за безопасность конфиденциальной информации (персональных данных) или за применение средств электронной подписи. При оказании услуг по обслуживанию СКЗИ сторонней организацией, она должна обладать лицензией ФСБ на соответствующий вид работ.

Ответственные лица:

назначаются приказом по организации и имеют функциональные обязанности в соответствии с настоящей Инструкцией;

Администраторы СКЗИ, лица, ответственные за контроль восстановления зашифрованной информации и контроль электронных подписей, допускаются к работе после ознакомления с настоящей Инструкцией под расписку в ней;

Пользователи СКЗИ допускаются на основании приказа по организации, ознакомления с Инструкцией пользователя средств криптографической защиты информации под расписку на листе ознакомления в ней и подписи Администратора СКЗИ о допуске;

должны иметь уровень компетентности, достаточный для корректной и безопасной эксплуатации СКЗИ.

3. Компетенции ответственных лиц

Ответственность при эксплуатации СКЗИ в организации распределяются между ответственными лицами в пределах их служебных полномочий следующим образом:

Ответственное лицо	Сфера ответственности
Руководитель организации	Соответствие проводимых мероприятий по организации и обеспечению безопасности обработки конфиденциальной информации (персональных данных) с использованием СКЗИ лицензионным требованиям, эксплуатационной и технической документации на СКЗИ и настоящей Инструкции Соответствие квалификации сотрудников, допущенных к работе с СКЗИ, выполняемым обязанностям
Администратор СКЗИ	Установка и ввод в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к СКЗИ Проверка готовности СКЗИ к использованию с составлением заключений о возможности их эксплуатации Инструктаж пользователей СКЗИ по настоящей Инструкции и обучение пользователей СКЗИ правилам работы с ними Учет лиц, допущенных к работе с СКЗИ Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, носителей ключевой информации Контроль за соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией на них Контроль сроков использования ключевой информации. Режим доступа в помещения, где установлены и (или) хранятся СКЗИ, ключевые документы, эксплуатационная и техническая документация к ним Расследование и составление заключений по фактам нарушения условий хранения и использования СКЗИ, разработка и принятие мер по предотвращению нарушений и их последствий в будущем

Лицо, ответственное за восстановление зашифрованной информации	настройка и контроль механизмов восстановления; восстановление зашифрованной информации в нештатных ситуациях и недоступности ключей шифрования или пользователей СКЗИ.
Пользователь СКЗИ	Соблюдение конфиденциальности при обращении со сведениями, которые доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документов к ним. Выполнение требований к обеспечению безопасной и корректной эксплуатации СКЗИ Обеспечение надежного хранения СКЗИ, эксплуатационной и технической документации к ним, носителей ключевой информации Информирование Администратора СКЗИ о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ и ключевых документах к ним

4. Режимные помещения

Принципы организации режима в помещениях, где установлены и (или) хранятся СКЗИ, ключевые документы, эксплуатационная и техническая документация к ним (режимные помещения):

исключена возможность неконтролируемого проникновения в режимные помещения;

исключена возможность неконтролируемого пребывания посторонних лиц в режимных помещениях;

обеспечена сохранность конфиденциальной информации, СКЗИ, ключевых документов, эксплуатационной и технической документации к ним.

Требования к режимным помещениям, устанавливаются настоящей Инструкцией, а также эксплуатационной и технической документации на СКЗИ.

В отношении режимных помещений организацией проводятся следующие мероприятия:

назначается лицо, ответственное за помещение;

определяется перечень лиц, допущенных к работе в помещении и обслуживанию помещения;

устанавливается порядок доступа в помещение в рабочее и нерабочее время, в аварийных ситуациях (пожар, авария, стихийное бедствие и т.п.);

устанавливается порядок нахождения в помещении посторонних лиц (при необходимости их нахождения);

устанавливается порядок хранения и использования средств доступа (ключ, proximity-карта и т.п.) от помещения.

Решения по перечисленным мероприятиям закрепляются приказом по организации в отношении режимных помещений.

4.1. Требования к окнам режимных помещений

Окна помещений должны быть защищены от несанкционированного доступа посторонних лиц (в случае, если они на первом или последнем этаже, либо рядом с пожарными лестницами и другими местами, откуда возможно проникновение) металлическими решетками, ставнями или сигнализацией или другими средствами, препятствующими неконтролируемому проникновению в помещения.

Для предотвращения несанкционированного визуального просмотра режимных помещений извне окна должны быть защищены шторами или жалюзи.

4.2. Требования к дверям режимных помещений

Двери режимных помещений должны быть оборудованы надежными замками, гарантирующими их надежное закрытие в нерабочее время.

Средства доступа от входных дверей идентифицируются (нумеруются), учитываются и выдаются сотрудникам, имеющим право доступа в режимные помещения, под расписку в соответствующем журнале.

Дубликаты средств доступа в режимные помещения хранятся в сейфе руководителя организации, либо администратора СКЗИ, либо другом выделенном хранилище. Режим хранения дубликатов средств доступа в помещения должен исключать неконтролируемый и необнаруживаемый доступ к ним.

В обычных условиях двери режимных помещений могут быть открыты только сотрудниками, допущенными в них для санкционированного прохода в помещения.

Режим аварийного и нештатного доступа в режимные помещения устанавливается соответствующим приказом по организации.

Для исключения необнаруживаемого доступа в помещения, они должны защищаться одним из способов:

опечатываться;

оснащаться охранной сигнализацией или системой видеонаблюдения.

Мер должно быть достаточно, чтобы перед началом работы можно было определить, что проникновения в помещения не было.

4.3. Требования к техническим средствам охраны режимных помещений

Все технические средства охраны помещений должны проходить периодический контроль работоспособности.

Режимные помещения должны быть оборудованы охранной и пожарной сигнализацией, для которых организацией установлен порядок периодической проверки их исправности.

Параметры сети электроснабжения помещений должны соответствовать требованиям инструкций по эксплуатации технических средств и правилам техники безопасности.

4.4. Требования к мерам защиты оборудования в ЦОД

Оборудование в ЦОД, кабельные каналы, связывающее оборудование, должны находиться в телекоммуникационных шкафах, оснащенных мерами безопасности такими же, как предусмотренные для помещений в пп.4.1-4.3.

В случае размещения оборудования у стороннего оператора ЦОД по договору необходимо предусмотреть в соответствии с договором меры:

меры безопасности шкафов и кабельных систем, предусмотренных абзацем 1 настоящего пункта;

недопустимость вскрытия шкафов сотрудниками оператора ЦОД или другими лицами;

строгий пропускной режим в ЦОД;

регламентация проноса на территорию ЦОД и выноса оборудования лицами, перечень которых утвержден в Компании.

5. Хранение СКЗИ

За сохранность доверенных СКЗИ, ключевых носителей и документов, эксплуатационной и технической документации их владельцы несут персональную ответственность.

Для хранения СКЗИ, ключевых документов, ключевых носителей, эксплуатационной и технической документации к ним предусматривается:

для администратора СКЗИ - персональные металлических хранилища (сейфы, ящики, шкафы и т.п.), оборудованные надежными внутренними замками, в условиях, исключающих бесконтрольный доступ к ним, а также непреднамеренное уничтожение;

для пользователя - персональные хранилища (сейфы, ящики, шкафы и т.п.), оборудованных замками, в условиях, исключающих бесконтрольный доступ к ним, а также непреднамеренное уничтожение.

Организацией должен быть определен порядок доступа к хранилищам, хранения и использования средств доступа от них в рабочем режиме и аварийных и нештатных ситуациях (в том числе использование резервных средств доступа).

Средства доступа к хранилищам должны быть учтены в соответствующем журнале под расписку ответственных за их хранение лиц. Один экземпляр средства доступа передается лицу, ответственному за хранилище. Дубликат средства доступа хранится в сейфе руководителя организации, либо администратора СКЗИ, либо другом выделенном хранилище.

По окончании рабочего дня хранилища должны быть опечатаны. Печати, предназначенные для опечатывания хранилищ должны храниться у лиц, ответственных за эти хранилища.

При хранении ключевой информации СКЗИ в реестре Windows и на HDD персонального компьютера требования по хранению ключевых носителей распространяются на персональный компьютер. В случае невозможности отчуждения ключевого носителя с ключевой информацией от персонального компьютера организационно-техническими мероприятиями должен быть исключен

несанкционированный доступ к персональному компьютеру с ключами. При хранении ключей на HDD персонального компьютера необходимо использовать парольную защиту.

6. Замена средств доступа в режимные помещения, хранилища

При утрате средства доступа от хранилища или входной двери режимного помещения необходимо либо заменить или переделать секрет замка с изготовлением и учетом новых средств доступа к нему, либо заменить хранилище или замок (если невозможно выполнить первую меру).

До момента изменения секрета или замены замка режим работы с этим хранилищем устанавливает администратор СКЗИ, либо руководитель организации в рамках своих полномочий.

7. Передача, пересылка, обмен СКЗИ

Передача СКЗИ, инсталлирующих CD-дисков, эксплуатационной документации к СКЗИ, ключевых носителей допускается только между:

пользователями СКЗИ и администратором СКЗИ.

Любая передача СКЗИ осуществляется под расписку в соответствующем журнале учета.

Пересылка СКЗИ и ключевых документов возможна фельдъегерской (в том числе ведомственной) связью или со специально выделенным организацией сотрудником (-ами) при соблюдении мер, исключающими бесконтрольный доступ к СКЗИ во время доставки.

Правила пересылки:

СКЗИ должны быть упакованы в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия;

СКЗИ пересылаются отдельно от ключевых документов;

упаковка опечатывается, чтобы исключалась возможность извлечения содержимого без нарушения упаковок и оттисков печатей;

пересылка должна сопровождаться сопроводительным письмом, которое вкладывается в одну из упаковок и содержит информацию о том: что посылается, в каком количестве, учетные номера и документов.

Эксплуатационную, техническую документацию и дистрибутивы СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

8. Аппаратные средства, функционирующие вместе с СКЗИ

Аппаратные средства, которые функционируют в штатном режиме вместе с СКЗИ должны:

учитываться совместно с СКЗИ (п.10);

оборудоваться средствами контроля за вскрытием (опечатывание, пломбы).

При хранении ключевой информации СКЗИ в реестре Windows и на HDD персонального компьютера требования по хранению ключевых носителей распространяются на персональный компьютер. В случае невозможности отчуждения ключевого носителя с ключевой информацией от персонального компьютера организационно-техническими мероприятиями должен быть исключен

несанкционированный доступ к персональному компьютеру с ключами. При хранении ключей на HDD персонального компьютера необходимо использовать парольную защиту.

Важно! Ответственность за ПК, в составе которых установленны СКЗИ и ключевая информация, несут пользователи этих ПК с момента выдачи им ПК вместе с СКЗИ или момент установки СКЗИ и допуска к работе с ПК.

9. Учет СКЗИ

Администратор СКЗИ ведет учет поставки, установки и обслуживания в отношении следующих материалов:

средства криптографической защиты информации (***СКЗИ***);

эксплуатационная и техническая документация на СКЗИ (***Э***);

ключевые носители – USB-токены, диски, дискеты, реестр ОС (***А, КН***);

ключевые документы:

бумажные с ключевой информацией;

USB-токены, диски, дискеты, реестр Windows, в которые записана ключевая информация (для ширования и электронной подписи);

при необходимости ключевые документы содержат контрольную, служебную и технологическую информацию (***КД***);

эталонные CD диски (***Д***) – сертифицированные дистрибутивы.

Учет ведется в форме:

Журнале учета СКЗИ (Приложение №1) – учет действий с программными СКЗИ, носителями и ключами электронной подписи;

документы о передаче экземпляров СКЗИ от поставщика СКЗИ (акты передачи и т.п.);

акты о выполнении работ по установке, настройке, замене ключей, выводу из эксплуатации СКЗИ.

Журнал ведет администратор СКЗИ.

Журнал учета СКЗИ и документы по учету действий с СКЗИ должны храниться в систематизированном виде (в выделенных папках) в месте, исключающем возможность несанкционированного доступа к нему (сейф, личный шкаф с замком и т.п.). Данное хранилище или помещение, в котором оно находится должно быть опечатано.

Возможна организация учета СКЗИ с применением специального программного обеспечения, включающего возможность электронной подписи.

10. Вывод из эксплуатации

Вывод из эксплуатации производится следующим образом:

установленное на компьютере СКЗИ – удаление с компьютера;

ключевые документы – надежное удаление ключевой информации с носителя;

ключевые носители – надежная очистка носителя;

эксплуатационная и техническая документация к СКЗИ;

Вывод из эксплуатации осуществляется Администратором СКЗИ непосредственно в момент прекращения использования.

Удаление с компьютера СКЗИ, ключевой информации, а также других связанных с криптографией данных, должно производиться надежным образом.

После этого выполняется Администратором делается отметка в журнале учета и допускается применение компьютера в других целях.

Важно! Ключевая информация, как правило, действует в течение 1 года. Однако защищаемые с помощью её данные, чаще всего хранятся 5 и более лет, так как отражают хозяйственные, деловые или технические операции. В течение 1 года разрешается выполнять шифрование данных или их подпись. Однако еще на этапе создания ИС должны быть обеспечены условия для корректного расшифрования данных или проверки электронной подписи в будущем.

Поэтому не всю ключевую информацию следует удалять. В частности, необходимо сохранять сертификаты электронной подписи (являющиеся открытыми). Это обеспечивает Владелец информационной системы, а также Удостоверяющий центр. Также в этом заинтересован сам Пользователь.

Непосредственные действия по удалению криптоключей регламентируются эксплуатационной и технической документацией на соответствующие СКЗИ, а также организацией, производившей запись криптоключей.

11. Смена ключевой информации

При использовании СКЗИ необходимо соблюдать сроки действия ключей шифрования. Как правило он составляет для секретных ключей – 1 год.

Необходимо на уровне соответствующих СКЗИ, системных и прикладных средств предусмотреть адекватные механизмы периодической смены ключей шифрования и с выводом из эксплуатации и уничтожения старых ключей.

Порядок смены должен соответствовать правилам пользования СКЗИ.

Факт смены ключей должен учитываться.

Помимо этого, в системах с шифрованием должен предусматриваться режим восстановления данных в случаях, когда невозможно получить отдельные ключи шифрования. Порядок восстановления зашифрованной информации или доступа к ней в нештатных ситуациях должен быть определен, в том числе должно быть назначено ответственное за восстановление информации лицо.

12. Уничтожение ключевых носителей и документов

Уничтожение производится в течение 10 суток после вывода из эксплуатации. Факт уничтожения фиксируется Журнале учета СКЗИ.

Уничтожение больших объемов ключевых документов и носителей может быть оформлено актом комиссией не менее двух человек из числа пользователей СКЗИ и Администратора СКЗИ. Акт утверждается руководителем организации.

Ключевые носители (диски, USB-токены) уничтожаются путем нанесения неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации на них. Непосредственные действия по уничтожению

ключевых носителей регламентируются эксплуатационной и технической документацией на соответствующие СКЗИ, а также организацией, производившей запись криптоключей.

Бумажные и прочие сгораемые носители, а также эксплуатационная и техническая документация на СКЗИ уничтожается путем сжигания или с помощью бумагорезательных машин.

13. Требования к программному обеспечению на персональном компьютере с СКЗИ

За установку, настройку общесистемного, прикладного программного обеспечения и дополнительных средств защиты на персональном компьютере с СКЗИ осуществляет администратор СКЗИ в соответствии с правилами установки и настройки СКЗИ и программного обеспечения, изложенными в эксплуатационной и технической документации на СКЗИ.

К установке и настройке СКЗИ и программному обеспечению предъявляются следующие общие требования:

устанавливаемое программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществить несанкционированный доступ к системным ресурсам;

устанавливаемое программное обеспечение должно быть лицензионным;

устанавливаемое программное обеспечение должно предусматривать организацию разрешительной системы доступа, при которой администратор СКЗИ и пользователи СКЗИ имеют свои атрибуты (учетную запись) для входа в систему и доступа к ресурсам;

устанавливаемое программное обеспечение и СКЗИ, а также диски для их инсталляции должны подвергаться периодическому контролю целостности в соответствии с эксплуатационной и технической документацией;

устанавливаемое программное обеспечение должно устанавливаться совместно с антивирусным программным обеспечением, базы которого должны своевременно и регулярно обновляться;

устанавливаемое программное обеспечение не должно содержать возможностей, позволяющих модифицировать системные ресурсы (области памяти, программный код), передавать управление несанкционированным подпрограммам, повышать предоставленные привилегии, использовать недокументированные разработчиками возможности операционной системы).

К операционной системе на персональном компьютере, в среде которой планируется использовать СКЗИ, предъявляются следующие общие требования:

на персональном компьютере должна быть установлена только одна лицензионная операционная система, удовлетворяющая системным требованиям СКЗИ (запрещается использовать нестандартные, измененные или отладочные версии операционной системы);

удаленное управление операционной системой должно быть запрещено или ограничено путем отключения всех служб, реализующих данные механизмы, или путем

настроек, запрещающих фильтров для протоколов и портов удаленного управления операционной системой для всех узлов, кроме специально выделенных для этих целей;

каждый пользователь должен иметь для входа в операционную систему свою учетную запись, длина пароля которой должна быть не менее 6 символов;

учетная запись для гостевого входа (Guest) должна быть отключена;

правом установки и настройки операционной системы и СКЗИ должен обладать только администратор СКЗИ;

все неиспользуемые ресурсы операционной системы должны быть отключены (протоколы, сервисы и т.п.);

режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

всем пользователям и группам, зарегистрированным в операционной системе, права доступа к ресурсам должны быть назначены в объеме, необходимом для выполнения ими своих обязанностей;

доступ должен быть максимально ограничен к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

системный реестр;

файлы и каталоги;

временные файлы;

журналы системы;

файлы подкачки;

кэшируемая информация (пароли и т.п.);

отладочная информация.

регулярно должны устанавливаться пакеты обновления безопасности операционной системы (Service Packs, Hot fix и т.п.), антивирусных баз;

периодически должны исследоваться информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на операционную систему;

должна быть исключена возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из сети Internet, без проведения соответствующих проверок на предмет содержания в них программных закладок и сетевых вирусов (при подключении к сети Internet);

на персональном компьютере с СКЗИ должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN сетей и т.п.) при подключению к сети Internet. При этом предпочтение должно отдаваться сертифицированным средствам защиты;

должна быть реализована система аудита событий безопасности операционной системы, проводиться регулярный анализ результатов аудита;

Администратор СКЗИ должен осуществлять периодический контроль выполнения указанных требований, а также требований, приведенных в эксплуатационной и технической документации на СКЗИ.

Не допускается:

обрабатывать на персональных компьютерах, оснащенным СКЗИ, информацию, содержащую государственную тайну;

осуществлять несанкционированное изменение аппаратной и программной конфигурации персонального компьютера (в том числе несанкционированное вскрытие), СКЗИ, программного обеспечения.

14. Защита СКЗИ от несанкционированного доступа

Защита СКЗИ от несанкционированного доступа включают в себя выполнение следующих мероприятий:

на административном уровне (предпринимаемые руководством организации действия по обеспечению процессов информационной безопасности (в частности по вопросам применения СКЗИ) ресурсами, управлением и контролем со стороны руководства);

на организационном уровне (регламентация процессов охраны и режима допуска в отношении СКЗИ, технических средств с СКЗИ, помещений, процессов обеспечения информационной безопасности (в частности при эксплуатации СКЗИ) и контроля эффективности, процессов обеспечения и поддержания компетентности персонала при работе с СКЗИ, распределение обязанностей и ответственности);

на техническом уровне (обеспечение соблюдения правил эксплуатации и работоспособности СКЗИ).

Защита СКЗИ от несанкционируемого доступа должна удовлетворять следующим общим требованиям:

должна обеспечиваться на всех технологических этапах и во всех режимах функционирования СКЗИ, в том числе при проведении ремонтных и регламентных работ;

должна предусматривать контроль эффективности средств защиты от несанкционированного доступа. Этот контроль должен периодически выполняться администратором СКЗИ на основе требований документации на средства защиты от несанкционированного доступа;

должна исключать возможность несанкционированного не обнаруживаемого доступа к СКЗИ, технических средств с СКЗИ, инсталлирующих и ключевых носителей изменения аппаратной части технических средств с СКЗИ (путем опечатывания (опломбирования) системного блока и разъемов персонального компьютера, опечатывания сейфов, шкафов, ящиков для хранения).

Для регламентации входа в операционную систему, BIOS, при осуществлении шифрования на основе паролей, использовании токенов с пин-кодами Администратором СКЗИ разрабатывается и применяется политика назначения и смены паролей.

Пароли для однофакторной аутентификации должны формироваться в соответствии со следующими правилами:

длина пароля должна быть не менее 6 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

блокировка учетной записи пользователя на 30 минут после 5 неудачных попыток ввода пароля;

Пароли для двухфакторной аутентификации с использованием токенов должны формироваться в соответствии со следующими правилами:

длина пароля должна быть не менее 6 символов;

пароль может состоять из символов одной группы;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

блокировка токена после 10 неудачных попыток ввода пароля и возможность разблокировки только администратором СКЗИ.

Администратор СКЗИ, а также Пользователи СКЗИ несут персональную ответственность за обеспечение режима конфиденциальности в отношении паролей доступа. Запрещается записывать пароли на материальные носители и хранить их в легкодоступных местах, в том числе на мониторе, рабочем столе или ящиках стола.

Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год. Пароль должен быть изменен раньше плановой замены в случае его компрометации. Ответственность за своевременную смену пароля несет Администратор СКЗИ.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС, в которых применяется СКЗИ. Средствами BIOS должна быть исключена возможность работы на ПКс СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

15. Действия в случае компрометации ключей

К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, относятся следующие:

потеря ключевых носителей с криптографическими ключами;

потеря ключевых носителей с криптографическими ключами с последующим их обнаружением;

увольнение работников – пользователей СКЗИ, имевших доступ к криптографическим ключам;

возникновение подозрений относительно утечки информации или её искажения;

нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с криптографическими ключами, если используется процедура опечатывания сейфов;

утрата ключей от сейфов в момент нахождения в них ключевых носителей с криптографическими ключами.

Ключи шифрования, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению администратора СКЗИ, согласованного с руководителем организации, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации (персональных данных), пользователи СКЗИ обязаны сообщать администратору СКЗИ или руководителю организации.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации (персональных данных), пользователи СКЗИ обязаны сообщать администратору СКЗИ или руководителю организации.

16. Ограничения и запреты

осуществлять несанкционированное копирование ключевых носителей;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным

вывод ключевых документов на дисплей (монитор) персональный компьютер или принтер;

вставлять ключевой носитель в считывающее устройство в режимах, не предусмотренных штатным режимом использования ключевого носителя;

оставлять без контроля технические средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации;

записывать на ключевой носитель постороннюю информацию;

использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

17. Контроль соблюдения условий эксплуатации и работоспособности СКЗИ

Контроль за соблюдением условий эксплуатации может осуществляться:

самой Организацией, как обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением

СКЗИ, а также как собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;

Лицензиатом ФСБ России, имеющим право на оказание услуг в области шифрования;

ФСБ России.

Требования, проверяемые в ходе контроля, устанавливаются эксплуатационной и технической документацией к СКЗИ, настоящей Инструкцией, а также иными нормативно-методическими документами по эксплуатации и документами, принятыми в организации.

Лицензиат также осуществляет контроль выполнения Организацией данных ей указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

От Организации контроль выполняется Администратором СКЗИ.

Контроль может быть плановым и внеплановым.

Плановый контроль осуществляется с установленной периодичностью, но не реже 1 раза в год.

Внеплановый контроль осуществляется в случае установления фактов нарушения Организацией условий эксплуатации или работоспособности СКЗИ.

В ходе контроля оцениваются:

организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;

достигнутый уровень криптографической защиты конфиденциальной информации;

условия использования СКЗИ.

Сведения о контроле заносятся проверяющим в Журнал контроля соблюдения условий эксплуатации и работоспособности СКЗИ (Приложение № 2). При необходимости по результатам контроля проверяющим оформляется протокол проверки.

Протокол проверки предоставляется Ответственному за информационную безопасность персональных данных в Организации и руководителю Организации.

Если при контроле обнаружены недостатки, то указываются также замечания по результатам контроля. На каждое замечание назначается лицо, ответственное за его устранение, а также срок устранения. По результатам работы над замечанием в Журнале контроля делается запись о статусе устранения замечания, которая заверяется подписью Администратора СКЗИ.

Организация обязана принять меры по устранению вскрытых недостатков, а также выполнению рекомендаций Лицензиата (если он привлекался), изложенных в Журнале контроля.

Если в ходе контроля выявлены серьезные нарушения в эксплуатации СКЗИ, из-за чего становится реальной утечка конфиденциальной информации, Лицензиат вправе дать указание о прекращении использования СКЗИ до устранения причин выявленных нарушений.

Приложение №1 – Форма журнала учета СЗИ/СКЗИ

№ п. п.	Наименование СЗИ/СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СЗИ/СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СЗИ/СКЗИ			Отметка об удалении СЗИ/СКЗИ из компьютера, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводи-тельного письма	Ф.И.О. пользователя СЗИ/СКЗИ	Дата и расписка в получении	Ф.И.О. пользователя СЗИ/СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к кото-рым подключены СЗИ/СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СЗИ/СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение №2 – Форма журнала контроля соблюдения условий эксплуатации и работоспособности СКЗИ

№ п/п	Вид контроля (плановый/ внеплановый)	Дата	ФИО контролирующего	Замечания по результатам контроля, подпись контролирующего	Дата устранения замечания, подпись Администратора СКЗИ
1	*2*	*3*	*4*	*5*	*6*
1.	*Плановый*	*01.09.20*	*Иванов И.И.*	*Контроль пройден*	*администратор СКЗИ*
				без замечаний	
				Иванов И.И.	*Петров П.П.*
2.	*Плановый*	*01.09.21*	*Иванов И.И.*	*По результатам контроля*	
				выявлены замечания:	
				1. Не опечатывается	*05.09.21 устранено*
				сейф для хранения СКЗИ	*Петров П.П.*
				2. Возврат ключа	*13.09.21 устранено*
				Корольковой И.А. на	*Петров П.П.*
				время отпуска не учтен	
				в журнале ключей	
				3. Приказ о допущенных	*15.09.21 устранено*
				пользователях не	*Петров П.П.*
				актуален	
				Иванов И.И.	

Лист ознакомления с настоящей Инструкцией

Я изучил(а) и понял(а) содержание настоящей Инструкции и обязуюсь ее выполнять.

№ п/п	Фамилия Имя Отчество	Дата	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			