Инструкция
по обеспечению безопасности эксплуатации СКЗИ

1. Термины и определения

1.1. В настоящей инструкции по обеспечению безопасности эксплуатации СКЗИ (далее – Инструкция) применяются следующие термины и определения:

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

Средство криптографической защиты информации (СКЗИ) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении;

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

Ключевой документ – электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

Персональный компьютер (АРМ) – вычислительная машина, предназначенная для эксплуатации пользователем ИС в рамках исполнения должностных обязанностей.

Ответственный за эксплуатацию СКЗИ – сотрудник, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами;

Пользователи СКЗИ – работники, непосредственно допущенные к работе с СКЗИ.

2. Общие положения

2.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ, входящих в состав средств криптографической защиты, а также порядок их изготовления, смены, уничтожения и действий сотрудников при компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

2.2. Под использованием СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов.

2.3. СКЗИ эксплуатируются, в соответствии с правилами пользования.

2.4.ИСПДн ДА использует сертифицированные Федеральной службой безопасности России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.5.Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях следующих нормативно-правовых актов:

- Федеральный закон от 27.07.2006 № 149 – ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 06.04.2011 № 63 – ФЗ «Об электронной подписи»;
- 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 СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

2.6.Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом назначается Ответственный за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ осуществляет:

- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;
- учет пользователей СКЗИ;
- контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;
- разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

2.7.Обучение пользователей правилам работы с СКЗИ осуществляет Ответственный за эксплуатацию СКЗИ.

2.8.Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается Ответственного за эксплуатацию СКЗИ.

2.9.Ответственный за эксплуатацию СКЗИ и Пользователи СКЗИ должны быть ознакомлены с настоящей Инструкцией под подпись.

3. Порядок допуска пользователей к работе с СКЗИ

3.1.Для работы с СКЗИ привлекаются должностные лица, допущенные к работе с СКЗИ в соответствии с приказом.

3.2.Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами, указанными в пункте 2.5 данной инструкции и проходит обучение правилам работы с СКЗИ, которое проводит Ответственный за эксплуатацию СКЗИ.

3.3.Пользователь считается допущенным к работе с СКЗИ после получения положительного «Заключения о подготовке и допуске к самостоятельной работе со СКЗИ».

4. Учет и хранение СКЗИ и криптографических ключей

4.1.СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

4.2.Поэкземплярный учет СКЗИ ведет Ответственный за эксплуатацию СКЗИ, в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) в ИСПДн ДА (далее – Журнал). При

этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если
аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

4.3.Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

4.4.Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под подпись в Журнале пользователям СКЗИ, несущим персональную ответственность за их сохранность.

4.5.При необходимости пользователю выдается документация по эксплуатации СКЗИ с последующим возвратом лицу, ответственному за эксплуатацию СКЗИ.

4.6.Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у ответственного за эксплуатацию СКЗИ. Криптографические ключи хранятся у пользователей СКЗИ. Хранение осуществляется в закрываемых на замок металлических хранилищах пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение и/или в опечатанном пенале (тубусе). Металлические шкафы должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками, и приспособлениями для опечатывания. Один экземпляр ключа от хранилища должен находиться у Ответственного за эксплуатацию СКЗИ. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе.

4.7.Пользователи СКЗИ могут осуществлять хранение рабочих и резервных криптографических ключей, предназначенных для применения в случае неработоспособности рабочих криптографических ключей. Резервные криптографические ключи могут также находиться на хранении у ответственного за эксплуатацию СКЗИ.

4.8.На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие надписи: на один ключевой носитель – «Рабочий»; на другой ключевой носитель – «Резервный».

4.9.Ключевой носитель с наклейкой «Резервный» помещается в конверт и опечатывается пользователем и ответственным за эксплуатацию СКЗИ.

4.10. Все полученные экземпляры криптографических ключей должны быть выданы под подпись в Журнале. Резервные криптографические ключи могут находиться на хранении у ответственного за эксплуатацию СКЗИ.

4.11. Ключевые носители с неработоспособными криптографическими ключами Ответственный за эксплуатацию СКЗИ принимает от пользователя под подпись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

4.12. При необходимости замены наклейки на ключевом носителе (стирание надписи реквизитов) пользователь передает его ответственному за эксплуатацию СКЗИ, который в присутствии пользователя снимает старую наклейку и приклеивает новую наклейку с такими же учетными реквизитами.

4.13. 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.

4.14. СКЗИ и криптографические ключи могут доставляться специальной (фельдъегерской) связью или курьером, имеющего доверенность на право получения СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во

время доставки.

4.15. Для пересылки СКЗИ и криптографические ключи помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптографические ключи пересылают в отдельном пакете с пометкой «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения целостности упаковок и оттисков печати.

4.16. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приема-передачи (Опись) документов, в котором указывается: что посылается и в каком количестве, учетные номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приема-передачи (Опись) документов вкладывается в упаковку.

4.17. Полученную упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приема-передачи (Описи) документов или сама упаковка и оттиск печати - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то должен быть составлен акт о происшедшем нарушении. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний от ответственного за эксплуатацию СКЗИ применять не разрешается.

4.18. При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует возвратить для установления причин происшедшего и их устранения в дальнейшем. В этом случае необходимо получить новые криптографические ключи.

4.19. Ключевые носители совместно с Журналом должны храниться у ответственного за эксплуатацию СКЗИ, в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.

4.20. На время отсутствия ответственного за эксплуатацию СКЗИ, должен быть назначен сотрудник его замещающий.

4.21. При необходимости криптографические ключи сдаются на временное хранение ответственному за эксплуатацию СКЗИ.

5. Использование СКЗИ и криптографических ключей

5.1. Криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

5.2. Криптографический ключ невозможно использовать, если истек срок действия.

5.3. Для обеспечения контроля доступа к СКЗИ системный блок автоматизированного рабочего места (далее – АРМ) опечатывается ответственным за эксплуатацию СКЗИ.

5.4. Пользователь должен периодически проверять сохранность оборудования и целостность печатей на АРМ. В случае обнаружения «посторонних» (не зарегистрированных) программ или выявления факта повреждения печати на системном блоке АРМ работа должна быть прекращена. По данному факту проводится служебное расследование, и осуществляются работы по анализу и ликвидации последствий данного нарушения.

5.5. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному за эксплуатацию СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей ответственный за эксплуатацию СКЗИ выполняет в присутствии пользователя.

5.6. В случае если рабочие криптографические ключи потеряли работоспособность, то по просьбе пользователя лицо, ответственное за эксплуатацию СКЗИ, вскрывает конверт (коробку) с резервными криптографическими ключами, делает копию ключевого носителя, используя

резервные криптографические ключи, помещает резервные криптографические ключи в конверт (коробку), а на новый ключевой носитель наклеивает наклейку с надписью: «Рабочий».

5.7.В экстренных случаях, не терпящих отлагательства, вскрытие конверта (коробки) с резервными криптографическими ключами может осуществляться комиссионно с последующим уведомлением ответственного за эксплуатацию СКЗИ, о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются ответственному за эксплуатацию СКЗИ.

5.8.Вскрытие системного блока АРМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного за эксплуатацию СКЗИ.

6. Обязанности пользователей СКЗИ

6.1.Пользователи СКЗИ обязаны:

- не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
- сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
- соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
- сообщать ответственному за эксплуатацию СКЗИ 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 при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять ответственного за эксплуатацию СКЗИ, 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.

6.2.Пользователь несет ответственность за то, чтобы на АРМ, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование СКЗИ. На АРМ, оборудованном СКЗИ, программное обеспечение должно быть лицензионным.

6.3.При обнаружении на АРМ, оборудованном СКЗИ, посторонних программ или вирусов, работа с СКЗИ на данном рабочем месте должна быть прекращена. Незамедлительно организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

6.4.Все полученные обладателем информации ограниченного доступа экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем Журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

6.5.Не допускается:

- разглашать информацию ограниченного доступа, к которой был допущен Пользователь СКЗИ;
- разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;
- выводить ключевую информацию на дисплей и(или) принтер;

- вставлять ключевой носитель в порт АРМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в порты других АРМ;
- записывать на ключевом носителе постороннюю информацию;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

6.6.О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать ответственному за эксплуатацию СКЗИ.

7. Действия при компрометации криптографических ключей

7.1.К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, но не ограничивающим их, относятся следующие:

- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами;
- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к рабочим и/или резервным криптографическим ключам;
- возникновение подозрений относительно утечки информации или ее искажения;
- нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими ключами, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами;
- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

7.2.В случае возникновения обстоятельств, указанных в п. 7.1 настоящей Инструкции, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей, по телефону информировать ответственного за эксплуатацию СКЗИ о факте компрометации используемых закрытых криптографических ключей.

7.3.Решение о компрометации криптографических ключей принимается на основании письменного уведомления о компрометации, подписанного ответственным за эксплуатацию СКЗИ, с приложением, при необходимости, письменного объяснения пользователя по факту компрометации его криптографических ключей.

7.4.Уведомление должно содержать:

- идентификационные параметры скомпрометированного криптографического ключа;
- фамилию, имя, отчество пользователя СКЗИ, который владел скомпрометированным криптографическим ключом;
- сведения об обстоятельствах компрометации криптографического ключа;
- время и обстоятельства выявления факта компрометации криптографического ключа.

7.5.После принятия решения о компрометации ключа принимаются меры о его изъятии из обращения и замены его на новый. Ответственный за эксплуатацию СКЗИ, после получения информации о компрометации криптографического ключа, убеждается в достоверности полученной информации, выводит из действия ключ подписи, соответствующий скомпрометированному закрытому криптографическому ключу (прекращает обмен электронными

документами с использованием сертификата ключа подписи, соответствующего скомпрометированному закрытому криптографическому ключу). Проводит работу по отзыву сертификата ключа подписи пользователя. Отозванный сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу пользователя, помещается в список отозванных сертификатов.

7.6. Дата, начиная с которой сертификат ключа подписи считается недействительным, устанавливается равной дате формирования списка отозванных сертификатов, в который был включен отзываемый сертификат ключа подписи.

7.7. Сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу, должен храниться ответственным за эксплуатацию СКЗИ, в течение срока хранения электронных документов для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

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

8. Уничтожение криптографических ключей

8.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

8.2. Уничтожение криптографических ключей на ключевых носителях производится лицом, ответственным за эксплуатацию СКЗИ.

8.3. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

8.4. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

- установить наличие оригинала и количество копий криптографических ключей;
- проверить внешним осмотром целостность каждого ключевого носителя;
- установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в Журнале поэкземплярного учета;
- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

8.5. В Журнале поэкземплярного учета ответственным за эксплуатацию СКЗИ производится отметка об уничтожении криптографических ключей.

9. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи

9.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи (далее – режимные помещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.

9.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

9.3. Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в

режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

9.4.Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

9.5.Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает лицо, ответственное за эксплуатацию СКЗИ. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

9.6.Двери режимных помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в режимные помещения, под расписку. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

9.7.Для предотвращения просмотра извне помещений, где используются СКЗИ, окна должны быть защищены или экраны мониторов должны быть повернуты в противоположную сторону от окна.

9.8.Помещения, в которых используются при работе криптографические ключи, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Сотрудникам, ответственным за охрану здания необходимо проверять периодически исправность сигнализации с отметкой в соответствующих журналах.

9.9.В обычных условиях помещения, находятся опечатанные хранилища, могут быть вскрыты только пользователями или ответственного за эксплуатацию СКЗИ.

9.10. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ обязан оценить возможность компрометации хранящихся криптографических ключей, составить акт и принять при необходимости меры к локализации последствий компрометации криптографических ключей и к их замене.

9.11. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптографических ключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

9.12. На время отсутствия пользователей указанное оборудование, при наличии такой возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с лицом, ответственным за эксплуатацию СКЗИ, необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.