Приложение 2
к Методическим рекомендациям

Приказ о назначении ответственного за эксплуатацию СКЗИ (типовая форма)

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

П Р И К А З

_____ № _____

О назначении ответственного за эксплуатацию
средств криптографической защиты информации в <наименование организации>

В связи с использованием средств криптографической защиты информации и иных шифровальных (криптографических) средств (далее – СКЗИ) в <наименование организации>, в целях обеспечения организации учета, хранения и эксплуатации СКЗИ, в соответствии с требованиями приказа ФСБ России от 010.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», «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», утвержденной приказом ФАПСИ от 13.06.2001 № 152, **п р и к а з ы в а ю:**

1. Назначить <Фамилия Имя Отчество>, <должность>, ответственным за эксплуатацию СКЗИ в организации. Во время временного отсутствия обязанности ответственного за эксплуатацию СКЗИ возлагать на <Фамилия Имя Отчество>, <должность>.

2. Ответственному за эксплуатацию СКЗИ при организации учета, хранения и эксплуатации СКЗИ руководствоваться действующими нормативными правовыми актами и методическими документами по эксплуатации СКЗИ, эксплуатационной и технической документацией на СКЗИ.

3. Контроль за исполнением данного приказа оставляю за собой.

<Должность руководителя> <И.О. Фамилия>

Приложение 3
к Методическим рекомендациям

Инструкция по обеспечению безопасности эксплуатации СКЗИ (типовая форма)

УТВЕРЖДАЮ
<Должность>
_____<И.О. Фамилия>
« ____ » _____ 20__ г.

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации
средств криптографической защиты информации
в <наименование организации>

1. Термины и определения

1.1. В настоящей инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации в <наименование организации> (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;

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 – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию;

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;

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

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

Ответственный за эксплуатацию СКЗИ – сотрудник, осуществляющий организацию учета, хранения и эксплуатации СКЗИ, в том числе обеспечения работ по техническому обслуживанию СКЗИ и управлению криптографическими ключами;

Пользователи СКЗИ – сотрудники <наименование организации>, непосредственно допущенные к работе с СКЗИ.

2. Общие положения

2.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок изготовления, смены, уничтожения и действий сотрудников <наименование организации> (далее – Организация) 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 и т.д.

2.3. Все действия с СКЗИ осуществляются в соответствии с эксплуатационной документацией на СКЗИ.

2.4. Организация использует сертифицированные ФСБ 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 нормативных правовых актов:

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказ ФАПСИ 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»;
- Приказ ФСБ от 010.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- иные нормативные правовые акты и методические документы по эксплуатации шифровальных (криптографических) средств.

2.6. Для организации и обеспечения работ по учету, хранению и эксплуатации СКЗИ, в том числе работ по техническому обслуживанию СКЗИ и управлению криптографическими ключами приказом Организации 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 на ответственного за эксплуатацию СКЗИ.

2.10. Ответственный за эксплуатацию СКЗИ и Пользователи должны быть ознакомлены с настоящей Инструкцией.

3. Порядок допуска пользователей к работе с СКЗИ

3.1. Перечень сотрудников, привлекаемых к работе с СКЗИ, утверждается приказом руководителя Организации.

3.2. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами (п.2.5), данной инструкцией и проходит обучение правилам работы с СКЗИ, которое проводит ответственный за эксплуатацию СКЗИ.

3.3. Пользователь считается допущенным к СКЗИ после оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе.

4. Учет СКЗИ, порядок ведения дел и журналов

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 (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. Ответственный за эксплуатацию СКЗИ ведет журналы:

4.4.1. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

4.4.2. Журнал учета лиц, допущенных к работе с СКЗИ;

4.4.3. Журнал учета ключей от помещений, в которых размещены СКЗИ;

4.4.4. Журнал учета печатей;

4.4.5. Журнал учета хранилищ СКЗИ;

4.4.6. Журнал учета журналов.

Каждый журнал имеет собственную нумерацию, нумерованные листы; журнал должен быть сброшюрован и прошит, прошивка скреплена печатью. Журнал ведется до полного окончания, после чего:

- заводится следующий том журнала, при этом записи в разных томах журнала имеют сквозную нумерацию;

- на титульном листе законченного журнала заполняются сведения о завершении его ведения, журнал хранится у ответственного эксплуатацию СКЗИ до передачи в архив в соответствии с номенклатурой дел Организации.

4.5. В Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов учитываются все используемые СКЗИ: установленные программные и программно-аппаратные СКЗИ, дистрибутивы СКЗИ, ключевые дистрибутивы СКЗИ и т.д. Для установленных программных и программно-

аппаратных СКЗИ отметки о подключении (установке) проставляет организация, имеющая лицензию ФСБ России на данный вид деятельности, либо вписываются реквизиты акта ввода в эксплуатацию СКЗИ.

4.6. В Журнале учета лиц, допущенных к работе с СКЗИ в организации, при заполнении вносится перечень СКЗИ, к работе с которыми допущен пользователь на основании заключений о допуске пользователя СКЗИ к самостоятельной работе.

4.7. В Журнале учета ключей от помещений, в которых размещены СКЗИ, отражается первичная выдача ключа от помещения, в котором используются СКЗИ, возможная повторная выдача ключа (в случае смены замка и других обстоятельствах) и сдача ключа при увольнении сотрудника или смене должностных обязанностей.

Дубликаты ключей от помещений, в которых размещены СКЗИ, ответственный за эксплуатацию СКЗИ хранит в своем кабинете, в запираемом индивидуальном шкафу (ячейке, ящике). Дубликаты ключей должны быть помещены в конверты (пеналы), опечатанные сотрудниками, работающими в этих помещениях. Дубликат ключа от кабинета ответственного за эксплуатацию СКЗИ хранится у руководителя Организации.

4.8. Ответственный за эксплуатацию СКЗИ ведет дело с материалами по СКЗИ (далее – Дело), в которое приобщаются все документы по эксплуатации СКЗИ, кроме журналов:

- документы, подтверждающие право использования СКЗИ;
- акты ввода в эксплуатацию СКЗИ;
- заключения о допуске пользователя СКЗИ к самостоятельной работе;
- акты об уничтожении СКЗИ

и иные документы, связанные с эксплуатацией СКЗИ.

Приобщаемые в Дело материалы отражаются в описи, неотъемлемой части Дела, и нумеруются в хронологическом порядке поступления.

5. Хранение СКЗИ и криптографических ключей

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

5.2. При необходимости пользователю выдается документация по эксплуатации СКЗИ с последующим возвратом ответственному за эксплуатацию СКЗИ;

5.3. 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 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, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе.

5.4. 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.

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

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

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

5.8. Ключевые носители с неработоспособными криптографическими ключами ответственный за эксплуатацию СКЗИ принимает от пользователя под роспись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

5.10. 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.

5.10. 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.

На метке опечатывания проставляется номер, дата ее нанесения и подпись (или пломба с индивидуальными номерами) лица, проводившего опечатывание. Номер метки должен фигурировать в Акте ввода в эксплуатацию СКЗИ.

Опечатывание производит ответственный за эксплуатацию СКЗИ либо лицо, проводившее ввод в эксплуатацию СКЗИ:

- для СКЗИ, введенных в эксплуатацию до утверждения настоящей Инструкции, опечатывание может быть проведено ответственным за эксплуатацию СКЗИ;

- при вводе в эксплуатацию новых СКЗИ опечатывание производит лицо, которое проводит ввод в эксплуатацию СКЗИ.

5.11. СКЗИ и криптографические ключи могут доставляться специальной (фельдъегерской) связью или курьером, имеющим доверенность, подписанную руководителем Организации, на право получения СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

5.12. 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.

5.13. 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.

5.14. 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 руководителя Организации применять не разрешается.

5.15. 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.

5.16. Ключевые носители совместно с Журналом должны храниться ответственным 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.

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

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

6. Использование СКЗИ и криптографических ключей

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

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

6.3. Для обеспечения контроля доступа к СКЗИ системный блок ПЭВМ опечатывается ответственным за эксплуатацию СКЗИ.

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

6.5. 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.

6.6. В случае, если рабочие криптографические ключи потеряли работоспособность, то по просьбе пользователя ответственный 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».

6.7. 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.

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

7. Обязанности пользователей СКЗИ

7.1. 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 сотруднику, 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 сотрудника, 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.

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

7.3. При обнаружении на ПК, 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.

7.4. 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.

7.5. 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 ПК при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в порты других ПК;
- 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).

7.6. 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.

8. Действия при компрометации криптографических ключей

8.1. 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.

8.2. В случае возникновения обстоятельств, указанных в п. 7.1 настоящей Инструкции, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей/ключей электронной подписи, по телефону информировать о факте компрометации используемых закрытых криптографических ключей/ключей электронной подписи:

- ответственного за эксплуатацию СКЗИ;
- организацию, от которой получены СКЗИ.

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

8.4. 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.

8.5. 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 сертификат ключа проверки электронной подписи, соответствующий скомпрометированному закрытому криптографическому ключу/ключу электронной подписи (прекращает обмен электронными документами с использованием сертификата ключа проверки электронной подписи, соответствующего скомпрометированному закрытому криптографическому ключу/ключу электронной подписи). Проводит работу по отзыву сертификата ключа подписи пользователя. Отозванный сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу пользователя/ключу электронной подписи, помещается в список отозванных сертификатов.

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

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

8.8. Для симметричного закрытого криптографического ключа, используемого для шифрования/дешифрования информации вне инфраструктуры открытых ключей (не

имеющего сертификата) 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 такого закрытого криптографического ключа, убеждается в достоверности полученной информации и обеспечивает смену (увеличение) его варианта.

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

10. Уничтожение криптографических ключей

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

10.2. Уничтожение криптографических ключей на ключевых носителях производится ответственным за эксплуатацию СКЗИ.

10.3. 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.

10.4. 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.

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

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

10.1. 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.

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

10.3. 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.

10.4. 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.

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

10.6. 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 в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

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

10.8. 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.

10.10. В обычных условиях помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или ответственным за эксплуатацию СКЗИ или комиссионно сотрудниками с разрешения руководителя Организации.

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

10.11. 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.

10.12. 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 ответственным за эксплуатацию СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

С настоящей инструкцией ознакомлены:

Ответственный за эксплуатацию СКЗИ

_____	_____	_____
(дата)	(подпись)	(фамилия, инициалы)

Пользователи СКЗИ

_____	_____	_____
(дата)	(подпись)	(фамилия, инициалы)

_____	_____	_____

(дата)	(подпись)	(фамилия, инициалы)
_____	_____	_____
(дата)	(подпись)	(фамилия, инициалы)
_____	_____	_____
(дата)	(подпись)	(фамилия, инициалы)
_____	_____	_____
(дата)	(подпись)	(фамилия, инициалы)