ДЕПАРТАМЕНТ ОХРАНЫ ЗДОРОВЬЯ НАСЕЛЕНИЯ КЕМЕРОВСКОЙ ОБЛАСТИ

ПРИКАЗ
от 19 июня 2015 г. N 882

ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ И КЛЮЧЕВЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ДЕПАРТАМЕНТЕ ОХРАНЫ ЗДОРОВЬЯ НАСЕЛЕНИЯ КЕМЕРОВСКОЙ ОБЛАСТИ

Руководствуясь федеральными законами от 27.06.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27.07.2006 N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах передачи данных", от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами", а также иных нормативных документов по защите информации, приказываю:

1. Утвердить инструкцию по обеспечению безопасности эксплуатации средств защиты информации, средств криптографической защиты информации, электронно-цифровой подписи и ключевых носителей информации в департаменте охраны здоровья населения Кемеровской области, приложением к настоящему приказу.
2. Контроль за исполнением приказа оставляю за собой.

Начальник департамента
В.М.ШАН-СИН

Утверждена
приказом департамента
охраны здоровья населения
Кемеровской области
от 19 июня 2015 г. N 882

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ И КЛЮЧЕВЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ДЕПАРТАМЕНТЕ ОХРАНЫ ЗДОРОВЬЯ НАСЕЛЕНИЯ КЕМЕРОВСКОЙ ОБЛАСТИ

1. Термины и определения

1.1. В настоящей инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации (далее - Инструкция) в департаменте охраны здоровья населения Кемеровской области (далее - учреждение) применяются следующие термины и определения:

Администратор безопасности - должностное лицо, обеспечивающее эксплуатацию средств криптографической защиты информации (далее - СКЗИ) и управление криптографическими ключами.

Безопасность эксплуатации СЗИ, СКЗИ, ЭЦП и ключевых носителей -совокупность мер управления и контроля, защищающая СЗИ, СКЗИ, ЭЦП и ключевые носители от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования.

Ответственный за эксплуатацию СЗИ, СКЗИ, ЭЦП и ключевых носителей - сотрудник, осуществляющий организацию и обеспечение работ по техническому обслуживанию СЗИ, СКЗИ и управление криптографическими ключами, ЭЦП и ключевых носителей информации.

Пользователь - сотрудник, который использует СЗИ, СКЗИ, ЭЦП и ключевые носители.

ПЭВМ - персональная электронно-вычислительная машина (персональный компьютер).

Средства защиты информации - средства защиты информации, средства криптографической защиты информации, электронно-цифровая подпись и ключевые носители.

Электронный документ (ЭД) - документ, в котором информация представлена в электронно-цифровой форме.

Остальные термины и определения, используемые в настоящей Инструкции, должны пониматься в соответствии с законодательством Российской Федерации.

2. Общие положения

2.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств защиты информации, а также порядок их изготовления, уничтожения и действий сотрудников учреждения при компрометации, или поломки, в целях обеспечения безопасности эксплуатации средств защиты информации.

2.2. Все действия работы с средствами защиты информации осуществляются в соответствии с эксплуатационной документацией.

2.3. Учреждение использует сертифицированные ФСБ России средства защиты информации, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.4. Для организации и обеспечения работ по техническому обслуживанию средств защиты информации, приказом учреждения назначается ответственный за эксплуатацию.

Ответственный за эксплуатацию средств защиты информации осуществляет:

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

2.5. Пользователи средств защиты информации назначаются приказом учреждения.

Пользователь средств защиты информации обязан:

- не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;

- соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании средств защиты информации;

- сдать средства защиты информации, эксплуатационную и техническую документацию к ним, криптографические ключи в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования средств защиты информации;

- незамедлительно уведомлять ответственного за эксплуатацию средств защиты информации о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, ключевых носителей 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.

2.6. Обучение пользователей правилам работы с средствами защиты информации осуществляет ответственный за эксплуатацию. Ответственный за эксплуатацию средствами защиты информации должен иметь соответствующий документ о квалификации в области эксплуатации. Непосредственно к работе с средствами защиты информации пользователи допускаются после обучения.

2.7. Текущий контроль, обеспечение функционирования и безопасности средств защиты информации возлагается на ответственного за эксплуатацию средств защиты информации.

2.8. Ответственный за эксплуатацию средств защиты информации и пользователи должны быть ознакомлены с настоящей Инструкцией под роспись.

3. Учет и хранение средств защиты информации

3.1. Средства защиты информации, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

3.2. Поэкземплярный учет средств защиты информации ведет ответственный за эксплуатацию средств защиты информации в журнале поэкземплярного учета эксплуатационной и технической документации к ним (далее - журнал) согласно приложению к Инструкции (приложение N 1). При этом программные средства защиты информации должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные средства защиты информации подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие средства защиты информации учитываются также совместно с соответствующими аппаратными средствами.

3.3. Единицей поэкземплярного учета криптографических ключей, ключевых носителей, 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.

3.4. При необходимости пользователю выдается документация по эксплуатации средств защиты информации в электронном виде.

3.5. Дистрибутивы средств защиты информации на носителях, эксплуатационная и техническая документация к ним, инструкции хранятся у ответственного за эксплуатацию средств защиты информации. Криптографические ключи, электронно-цифровая подпись и ключевые носители хранятся у пользователей средств защиты информации. 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.

3.6. Пользователи средств защиты информации могут осуществлять хранение рабочих и резервных криптографических ключей, ЭЦП и ключевых носителей предназначенных для применения в случае неработоспособности рабочих криптографических ключей, ЭЦП и ключевых носителей. Резервные криптографические ключи, ЭЦП и ключевые носители могут также находится на хранении у ответственного за эксплуатацию.

3.7. Аппаратные средства, с которыми осуществляется штатное Функционирование средств защиты информации, а также аппаратные и аппаратно-программные средства защиты информации, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования), аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.8. Ключевые носители совместно с журналом должны храниться ответственным за эксплуатацию средств защиты информации 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.

3.9. На время отсутствия ответственного за эксплуатацию средств защиты информации должен быть назначен сотрудник его замещающий.

3.10. При необходимости криптографические ключи, ЭЦП и ключевые носители сдаются на временное хранение ответственному за эксплуатацию.

4. Использование СКЗИ и криптографических ключей, ЭЦП и ключевых носителей

4.1. Средства защиты информации используются для обеспечения конфиденциальности, авторства и целостности электронных документов и т.п.

4.2. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному за эксплуатацию.

4.3. Пользователю запрещается:

- осуществлять несанкционированное копирование средств защиты информации; использовать ключевые носители и ЭЦП для работы на других рабочих местах для шифрования и подписи электронных документов;
- разглашать содержимое средств защиты информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
- вставлять носители криптографических ключей, ЭЦП и ключевые носители в устройства считывания в режимах, не предусмотренных штатным режимом работы средств защиты информации, а также в устройства считывания других ПЭВМ;
- записывать на носители с криптографическими ключами, ЭЦП и ключевыми носителями постороннюю информацию;
- подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в штатной комплектации;
- работать на ПЭВМ, если во время ее начальной загрузки не проходят встроенные тесты, предусмотренные в ПЭВМ;
- вносить какие-либо изменения в программное обеспечение средств защиты информации.

5. Изготовление и плановая смена криптографических ключей и ЭЦП

5.1. Изготовление криптографических ключей и ЭЦП может производиться администратором безопасности в присутствии пользователя.

5.2. Криптографические ключи и ЭЦП изготавливаются на отчуждаемый ключевой

носитель в соответствии с эксплуатационно-технической документацией на средства защиты информации и требованиями безопасности, установленными настоящей Инструкцией.

5.3. Переход на новые криптографические ключи пользователь выполняет самостоятельно в соответствии с эксплуатационной документацией на средства защиты информации. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи.

5.4. При замене криптографических ключей используют программное обеспечение в соответствии с документами по эксплуатации. Пользователь самостоятельно обязан обновить сертификат ключ подписи. Обновление справочников сертификатов ключей производится путем добавления новых сертификатов ключей подписи из файлов, содержащих сертификаты ключей подписи, предоставляемых ответственным за эксплуатацию. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на средства защиты информации.

6. Действия при компрометации криптографических ключей и ЭЦП

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

- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭЦП;
- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭЦП с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к рабочим и/или резервным криптографическим ключам или ЭЦП;
- 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, ЭЦП, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами, ЭЦП;
- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

6.2. В случае возникновения обстоятельств, указанных в п. 6.1 настоящей Инструкции, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей, по телефону информировать администратора безопасности о факте компрометации используемых закрытых криптографических ключей, ЭЦП.

6.3. Решение о компрометации криптографических ключей принимает администратор безопасности на основании письменного уведомления о компрометации, подписанного ответственным за эксплуатацию средств защиты информации, с приложением, при необходимости, письменного объяснения пользователя по факту компрометации его криптографических ключей, ЭЦП.

6.4. Уведомление должно содержать:

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

6.5. После принятия решения о компрометации криптографического ключа, ЭЦП принимаются меры о его изъятии из обращения в соответствии с требованиями эксплуатационной и технической документации на средства защиты информации.

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

6.7. Использование средства защиты информации может быть возобновлено только после ввода в действие другого криптографического ключа, ЭЦП взамен скомпрометированного.

7. Уничтожение криптографических ключей, ЭЦП и ключевых носителей

7.1. Неиспользованные или выведенные из действия криптографические ключи, ЭЦП и ключевые носители подлежат уничтожению.

7.2. Уничтожение криптографических ключей, ЭЦП на ключевых носителях производится ответственным за эксплуатацию средств защиты информации.

7.3. Криптографические ключи, ЭЦП 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 средства защиты информации.

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

- установить наличие оригинала и количество копий криптографических ключей, ЭЦП;
- 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, ЭЦП находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

7.5. В журнале поэкземплярного учета ответственным за эксплуатацию средств защиты информации производится отметка об уничтожении криптографических ключей.

8. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены или хранятся средства защиты информации

8.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средств защиты информации или хранятся криптографические ключи (далее - режимные помещения), должны обеспечивать сохранность средств защиты информации.

8.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу средств защиты информации, а также другого оборудования, функционирующего с средствами защиты информации.

8.3. Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам защиты информации. 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.

8.4. 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.

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

8.6. Двери режимных помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей находятся у ответственных лиц, имеющих право допуска в режимные помещения. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

8.7. Для предотвращения просмотра извне помещений, где используются средства защиты информации, окна должны быть защищены или экраны мониторов должны быть повернуты в противоположную сторону от окна.

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

8.9. В обычных условиях помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или ответственным за эксплуатацию.

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

8.11. Размещение и монтаж средств защиты информации, а также другого оборудования, функционирующего со средствами защиты информации, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена средств защиты информации осуществляются в отсутствие лиц, не допущенных к работе с данными средствами защиты информации.

8.12. 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 необходимо предусмотреть организационно-технические меры, исключающие возможность использования средств защиты информации посторонними лицами.

8.13. В нерабочее время помещения, в которых осуществляется функционирование средств защиты информации, должны ставиться на охрану.

Приложение N 1
к Инструкции по обеспечению
безопасности эксплуатации
средств криптографической
защиты информации
в департаменте охраны здоровья
населения Кемеровской области

Форма журнала
учета используемых криптосредств, эксплуатационной
и технической документации к ним

N п/п	Наименование СКЗИ	Регистрационный номер СКЗИ	Отметка о получении	Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств ИСПДН			Примечание
			От кого получены	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	6	7	8	9	10	11	12	13	14

Приложение N 2
к Инструкции по обеспечению
безопасности эксплуатации
средств криптографической
защиты информации

в департаменте охраны здоровья
населения Кемеровской области

Журнал
сертифицированных средств защиты информации

Номер п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание

Приложение N 3
к Инструкции по обеспечению
безопасности эксплуатации
средств криптографической
защиты информации
в департаменте охраны здоровья
населения Кемеровской области

Журнал
учета съемных носителей персональных данных
к Инструкции по обеспечению безопасности эксплуатации
средств криптографической защиты информации
в департаменте охраны здоровья населения
Кемеровской области

N п/п	Регистрационный номер	Тип/емкость носителя персональных данных	Номер экземпляра/количество экземпляров	Место установки (использования)/дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)