

Государственное учреждение «Территориальный фонд обязательного медицинского страхования Оренбургской области»

СОГЛАСОВАНО

Управление Федеральной службы
безопасности по Оренбургской области

Начальник подразделения Управления



А.А. Назаренков

« 26 » 09 2012 г.

УТВЕРЖДАЮ

Государственное учреждение
«Территориальный фонд обязательного
медицинского страхования Оренбургской
области»

Директор



И.И. Головин

« 28 » 09 2012 г.

**Положение об организации криптографической защиты
информации в системе обязательного медицинского
страхования Оренбургской области**

г. Оренбург
2012 год

1 Общие положения

Настоящее Положение разработано с целью защиты прав застрахованных лиц в части сохранения конфиденциальности их персональных данных при передаче по открытым каналам связи, а также для организации юридически значимого электронного документооборота в системе обязательного медицинского страхования Оренбургской области.

Настоящее Положение разработано в соответствии с:

- Федеральным законом 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и защиты информации»;
- Инструкцией 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 июня 2001 года №152 (далее — Инструкция ФАПСИ);
- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года №149/6/6-622);
- Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных в информационных системах персональных данных с использованием средств автоматизации (Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года №149/5-144);
- Приказом ФСБ России от 9 февраля 2005 года №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Регламентом информационной безопасности при использовании программно-аппаратных средств комплекса VipNet (ФРКЕ. 00029 04 90 01);

Настоящее Положение распространяется на все субъекты системы обязательного медицинского страхования (далее — ОМС) Оренбургской области.

2 Общая схема организации криптографической защиты

В обязательном порядке защите средствами криптографической защиты информации (далее — СКЗИ) подлежат персональные данные застрахованных лиц, передаваемые по открытым каналам связи или через съёмные носители.

В качестве СКЗИ в системе ОМС Оренбургской области используются средства криптографической защиты из состава продукта VipNet Custom.

ТФОМС Оренбургской области создал на базе отдела информационной безопасности орган криптографической защиты, являющийся координирующим в части информационного обмена в системе ОМС Оренбургской области. Орган криптографической защиты располагается по адресу: Оренбургская область, город Оренбург, переулок Фабричный, дом 19.

Обладателями конфиденциальной информации в системе ОМС Оренбургской области являются:

- Государственное учреждение «Территориальный фонд обязательного медицинского

страхования Оренбургской области» (далее — ТФОМС);

- Лечебно-профилактические учреждения Оренбургской области (далее — ЛПУ);
- Страховые медицинские организации Оренбургской области (далее — СМО);
- прочие субъекты информационного взаимодействия системы ОМС Оренбургской области;

ТФОМС Оренбургской области при создании органов криптографической защиты должен письменно уведомить УФСБ России по Оренбургской области.

Инструкции, создаваемые у обладателя конфиденциальной информации, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой, с использованием СКЗИ, конфиденциальной информации (в частности, персональных данных) при информационном обмене в системе ОМС Оренбургской области должны согласовываться с ТФОМС Оренбургской области.

3 Организация обеспечения безопасности у обладателей конфиденциальной информации

Обеспечение функционирования и безопасности СКЗИ у обладателя конфиденциальной информации возлагается на ответственного пользователя СКЗИ, имеющего необходимый уровень квалификации (высшее профессиональное образование или переподготовку в области информационной безопасности), назначаемого руководителем организации, либо на орган криптографической защиты. При этом, кандидатуры лиц, на которых собираются возложить обязанности ответственного пользователя криптосредств должны согласовываться с отделом информационной безопасности ТФОМС Оренбургской области. Органы криптографической защиты имеют право создавать только организации-лицензиаты ФСБ России.

Органом криптографической защиты может быть структурное подразделение организации. Возложение функции ответственного пользователя СКЗИ (органа криптографической защиты) допускается на:

- одного из пользователей СКЗИ;
- на структурное подразделение или должностное лицо (работника), ответственных за обеспечение безопасности персональных данных, назначаемых оператором;

Из числа сотрудников органа криптографической защиты (ответственных пользователей СКЗИ) в организации-обладателе конфиденциальной информации назначается администратор информационной безопасности абонентских пунктов, закреплённых за ним.

Копия приказа о назначении лиц, ответственных за информационную безопасность, должна быть отправлена в отдел информационной безопасности ТФОМС Оренбургской области. Все изменения к приказу также должны своевременно передаваться (в течении 10 дней).

Орган криптографической защиты организации (ответственный пользователь криптосредств) выполняет указания координирующего органа криптографической защиты при использовании СКЗИ в системе ОМС Оренбургской области.

При создании органа криптографической защиты необходимо иметь выделенное помещение, удовлетворяющее требованиям, указанным в данном Положении, а также других законодательно-нормативных документов Российской Федерации в области информационной безопасности. Также выделенное помещение необходимо иметь ответственному пользователю криптосредств, чтобы обеспечить условия хранения ключевой информации пользователей СКЗИ своей организации.

При большом количестве пользователей СКЗИ обладатель конфиденциальной информации по согласованию с отделом информационной безопасности ТФОМС Оренбургской области имеет право организовать пункт автоматизированной подачи запросов на криптографические ключи с возможностью защищённой доставки изготовленных ключей. В этом случае в организации разворачивается абонентский пункт с программным обеспечением VipNet Registration Point.

4 Обязанности ответственных лиц

4.1 Требования к пользователям СКЗИ

Пользователи СКЗИ обязаны:

- Не разглашать информацию, к которой они допущены, рубежи её защиты, в том числе сведения о криптоключях;
- Не допускать снятие ключей с ключевых документов;
- Не допускать вывод ключевой информации на дисплей (монитор) компьютера или принтер;
- Не допускать запись на ключевой носитель посторонней информации;
- Не допускать установки ключевых документов в другие персональные компьютеры;
- Соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- Незамедлительно сообщать в орган криптографической защиты и ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- Сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным Инструкцией ФАПСИ, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- Немедленно уведомлять орган криптографической защиты и ответственного пользователя криптосредств о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

4.2 Требования к ответственным пользователям криптосредств

Ответственный пользователь криптосредств выполняет функции пользователя СКЗИ, а также следующие функции:

- разрабатывает для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;
- разрабатывает на основе модели угроз систему безопасности персональных данных, обеспечивающую нейтрализацию всех перечисленных в модели угроз;
- устанавливает СКЗИ в соответствии с эксплуатационной и технической документацией к СКЗИ;
- обучает лиц, использующих СКЗИ правилам работы с ними;
- ведёт поэкземплярный учёт используемых СКЗИ, эксплуатационной и технической

документации к ним, носителей персональных данных;

- ведёт учёт лиц, допущенных к работе с СКЗИ (пользователей СКЗИ);
- контролирует соблюдение условий использования СКЗИ;
- расследует и составляет заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации;
- разрабатывает и применяет меры по предотвращению возможных опасных последствий нарушений;
- ведёт журнал учёта хранилищ, в котором учитываются все металлические хранилища организации для хранения СКЗИ, документации к СКЗИ и криптографических ключей;

4.3 Требования к органу криптографической защиты

Орган криптографической защиты выполняет обязанности ответственного пользователя криптосредств, а также следующие функции:

- проверяет готовность обладателей конфиденциальной информации к самостоятельному использованию СКЗИ;
- проверяет корректность установки СКЗИ и вводит СКЗИ в эксплуатацию;
- разрабатывает мероприятия по обеспечению функционирования и безопасности применяемых СКЗИ;
- ведёт учёт обслуживаемых обладателей конфиденциальной информации, а также физических лиц, допущенных к работе с СКЗИ;
- изготавливает из исходной ключевой информации ключевые документы, распределяет их и учитывает;
- разрабатывает схему организации криптографической защиты конфиденциальной информации (данную схему утверждает ТФОМС Оренбургской области);

4.4 Требования к администратору безопасности

Администратор безопасности абонентского пункта выполняет следующие функции:

- осуществляет контроль и несёт ответственность за соблюдением правил безопасной эксплуатации группы подчинённых ему средств вычислительной техники с СКЗИ;
- осуществляет настройки ОС и прикладного ПО;
- осуществляет контроль за попытками несанкционированного изменения режима безопасности СКЗИ;
- осуществляет контроль за соблюдением правил эксплуатации и соблюдением мер защиты от НСД;
- периодически осуществляет контроль целостности программного обеспечения СКЗИ;
- контролирует попытки несанкционированного доступа к СКЗИ, попытки сетевых атак и проявления сетевой активности приложений;
- разрабатывает и согласовывает с ТФОМС Оренбургской области инструкции по допуску в помещения с установленными СКЗИ;

5 Требования к спецпомещениям

Каждый орган криптографической защиты должен иметь спецпомещение. Перечень

спецпомещений утверждается руководителем организации. Спецпомещения органов криптографической должны удовлетворять следующим требованиям:

- прочная входная дверь с замком, гарантирующие надёжное закрытие спецпомещения в нерабочее время;
- двери спецпомещения должны быть всегда закрыты на замок и открываться только для санкционированного прохода сотрудников и посетителей;
- окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому доступу в спецпомещения;
- окна спецпомещений должны быть всегда защищены от просмотра извне (постоянно закрытые плотные шторы или жалюзи);
- спецпомещения должны быть оборудованы достаточным количеством надёжно запираемых сейфов, оборудованных приспособлениями для опечатывания замочных скважин.
- в спецпомещения допускаются только сотрудники органа криптографической защиты;
- уборка спецпомещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии администратора;
- по окончании рабочего дня, помещения закрываются, опечатываются и сдаются под охрану. Порядок сдачи помещений определяется организацией самостоятельно;
- спецпомещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации;
- оборудование помещений средствами вентиляции и кондиционирования воздуха должно соответствовать санитарно-гигиеническим нормам СНИП, устанавливаемым законодательством Российской Федерации.

Данные требования также предъявляются к помещениям, в которых эксплуатируется VipNet Registration Point, VipNet Administrator (ЦУС и УКЦ) или хранятся ключевые документы ответственным пользователем криптосредств.

Режим охраны спецпомещений пользователей СКЗИ устанавливает обладатель конфиденциальной информации по согласованию с отделом информационной безопасности ТФОМС Оренбургской области.

6 Порядок распространения СКЗИ

ТФОМС Оренбургской области приобретает СКЗИ для собственных нужд самостоятельно. СМО приобретают СКЗИ самостоятельно за счёт средств, выделяемых им на содержание. Для ЛПУ ТФОМС Оренбургской области, по возможности, на время их участия в системе ОМС, предоставляет на безвозмездной основе СКЗИ. В случае отсутствия возможности в предоставлении СКЗИ, ЛПУ приобретает СКЗИ самостоятельно.

Дополнительные СКЗИ (более одного экземпляра на учреждение) ЛПУ могут приобрести самостоятельно через любую организацию, имеющую лицензию ФСБ деятельность по передаче шифровальных (криптографических) средств.

Использование версий СКЗИ, не прошедших сертификацию ФСБ России или СКЗИ с истёкшими сроками действия сертификатов, является недопустимым. При получении

(покупке) СКЗИ необходимо убедиться, что в комплект поставки входят:

- маркированный производителем диск с установочным комплектом и документацией в электронном виде;
- формуляр на СКЗИ (в бумажном виде);
- заверенные производителем копии сертификатов соответствия;
- бумажный экземпляр лицензии на использования или договор, в рамках которого владельцу конфиденциальной информации передаётся программное обеспечение;
- сопроводительное письмо, на основании которого проверяется комплектность и заносится запись в учётный журнал.

Опционально (в случае покупки СКЗИ уровня защищённости КС2) может поставляться аппаратно-программный механизм доверенной загрузки (далее - АПМДЗ). В случае СКЗИ класса КС1 данное техническое средство не входит в комплект поставки.

Передача СКЗИ (установочного диска и формуляра) между пользователями СКЗИ внутри организации допускается только с санкции органа криптографической защиты с обязательной записью в журнале поэкземплярного учёта. При передаче СКЗИ между организациями необходимо составлять акт приёма-передачи.

7 Порядок допуска пользователей к СКЗИ

Порядок допуска пользователей к СКЗИ строго регламентирован и состоит из следующих этапов:

1. Руководитель организации подготавливает перечень пользователей СКЗИ (ФИО, должность) с указанием характеристик технических средств на которых планируется эксплуатировать СКЗИ;
2. Перечень пользователей СКЗИ направляется в ТФОМС Оренбургской области на согласование с отделом информационной безопасности (официальным письмом);
3. После согласования руководитель организации утверждает приказом перечень пользователей СКЗИ;
4. Пользователи СКЗИ самостоятельно изучают эксплуатационную документацию к СКЗИ, настоящее Положение и другие нормативные документы в области информационной безопасности;
5. Пользователи СКЗИ получают от органа криптографической защиты список вопросов (тесты), на которые необходимо ответить и передают заполненный бланк в орган криптографической защиты;
6. При успешной сдаче зачёта по изученному материалу, орган криптографической защиты составляет заключение о возможности допуска к самостоятельной работе с СКЗИ, утверждаемый директором ТФОМС Оренбургской области.

Пользователь допускается к работе с СКЗИ только после выполнения указанных этапов.

Нахождение в помещении, где установлены СКЗИ, лиц, не допущенных к работе с СКЗИ допустимо только в присутствии допущенных к СКЗИ лиц. В случае, если в одном помещении находятся пользователи СКЗИ, имеющие доступ к разным информационным системам, защищаемым при помощи СКЗИ, то для таких пользователей рекомендуется использование АПМДЗ, сертифицированного ФСБ России. Режим охраны помещений с установленным СКЗИ необходимо согласовывать с органом криптографической защиты.

8 Установка и обслуживание СКЗИ

Перед установкой СКЗИ необходимо убедиться, что на используемом компьютере

установлена и функционирует антивирусная защита с актуальной базой (базой данных сигнатур вредоносных программ). Для соответствия нормативным документам по защите персональных данных, антивирус должен быть сертифицирован ФСТЭК или ФСБ по требованиям безопасности. На компьютере также должны отсутствовать средства, позволяющие осуществлять несанкционированный доступ к системным ресурсам.

На средствах вычислительной техники с СКЗИ операционная система должна быть оригинальная (с официального установочного диска или его копии), а также должны отсутствовать средства отладки и трассировки программного обеспечения.

Установка средств криптографической защиты у обладателей конфиденциальной информации осуществляется уполномоченными лицами организации по инструкциям, полученным из органа криптографической защиты. Установка производится с носителя, полученного из органа криптографической защиты.

Отметим, что установка СКЗИ должна осуществляться с носителя от производителя СКЗИ, на котором содержится копия СКЗИ, соответствующая сертифицированному эталону. Носитель с установочной программой СКЗИ, а также с технической и эксплуатационной документацией к нему, должен храниться пользователем СКЗИ в индивидуальном металлическом хранилище. Также пользователь должен хранить формуляр, прилагаемый к данному диску в личном сейфе.

Ввод ключей, предварительно полученных в органе криптографической защиты, осуществляется пользователем СКЗИ самостоятельно или при помощи сотрудника органа криптографической защиты (лично или по телефону).

Специалисты органа криптографической защиты лично или удалённо (по открытым каналам связи с использованием СКЗИ) осуществляют контрольную проверку соответствия требованиям безопасности информации, указанным в технической документации к СКЗИ.

На средствах вычислительной техники с установленными СКЗИ в BIOS должен быть установлен пароль для ограничения возможности пользователя или злоумышленника по настройке. Также должна быть ограничена загрузка с любых носителей, кроме локального жёсткого диска.

По окончании установки и настройки СКЗИ, средство вычислительной техники, на которое проводилась установка, необходимо опломбировать таким образом, чтобы визуально можно было бы постоянно контролировать целостность пломбы. По результатам составляется акт в двух экземплярах (подписывается ответственным пользователем криптосредств и органом криптографической защиты). Один экземпляр передаётся в орган криптографической защиты ТФОМС Оренбургской области.

Изменения в составе средств вычислительной техники и программного обеспечения к ним должны согласовываться администратором безопасности с соответствующим органом криптографической защиты.

Использование АПМДЗ опционально, и зависит от модели нарушителя, разработанной в организации. Модель нарушителя необходимо согласовывать с отделом информационной безопасности ТФОМС Оренбургской области.

Обслуживанием СКЗИ, используемых в рамках системы ОМС Оренбургской области в ЛПУ, СМО, ТФОМС и его филиалах имеют право только:

- сотрудники отдела информационной безопасности ТФОМС Оренбургской области;
- администраторы безопасности, ответственные пользователи криптосредств или орган криптографической защиты организации (по согласованию с отделом информационной безопасности ТФОМС Оренбургской области);

Координирующий орган криптографической защиты периодически предоставляет методическую информацию по решению типовых проблем со средствами криптографической защиты. В случае невозможности решения проблем по методической информации, пользователь СКЗИ обращается в орган криптографической защиты и получает необходимую консультацию.

Для реализации функции оперативного контроля настроек операционной системы и средств защиты информации отдел информационной безопасности оставляет за собой право установки программного обеспечения, контролирующего целостность настроек, обеспечивающих должный уровень защищённости.

Для реализации функции технической поддержки отдел информационной безопасности оставляет за собой право установки программ, обеспечивающих удалённый доступ к компьютеру с СКЗИ, при условии, что в правилах сетевого экрана защищённой сети VipNet установлено ограничение на подключение только с компьютеров координирующего органа криптографической защиты информации. Удалённый доступ допустим только по защищённому каналу.

9 Порядок передачи и хранения ключевой информации

Криптографические ключи для первичной инициализации (дистрибутивы) СКЗИ записываются на съёмные носители типа CD-R (DVD-R). Ключи для каждого пользователя записываются на отдельные носители и упаковываются в индивидуальные бумажные конверты. На конвертах должно быть указано лицо, которому адресуются ключи, а также должна стоять пометка «Лично». Конверт опечатывается личной печатью сотрудника органа криптографической защиты (ответственного пользователя криптосредств), для этого предназначенной. Образцы печатей доводятся до обладателя конфиденциальной информации заранее.

Все опечатанные конверты вкладываются в общий конверт. В конверт также вкладывается сопроводительное письмо, в котором указывается:

- что пересылается и в каком количестве;
- учётные номера изделий или документов;
- назначение и порядок использования высылаемого отправления;
- порядок и сроки подтверждения получения.

Письмо запечатывается, а на самом письме указываются реквизиты отправителя, получателя, а также пометка «Конфиденциально». Конверт передаётся представителям организации-получателя в следующем составе:

- ответственный пользователь криптосредств или специалист органа криптографической защиты;
- сопровождающие сотрудники, выделенные руководителем организации.

Ответственный пользователь криптосредств или специалист органа криптографической защиты, получающий конверт должен расписаться в журнале о получении. При этом получающее лицо предъявляет документ, удостоверяющий его личность.

Во время доставки должны быть приняты меры, исключающие бесконтрольный доступ к содержимому конверта во время доставки.

Пользователи СКЗИ вскрывают конверты с ключами, предназначенные для них, лично. При этом необходимо сверить содержимое упаковки перечню, указанному в сопроводительном письме, а также целостность печатей на конвертах с ключами.

В случае, если содержимое конверта не соответствует информации, указанной в

сопроводительном письме или имеется подозрение в получении несанкционированного доступа к криптографическим ключам (нарушение целостности упаковки или печати), то составляется акт, который передаётся отправителю.

Полученные ключевые документы разрешается использовать только по указанию органа криптографической защиты. Криптографические ключи должны быть зарегистрированы в журнале поэкземплярного учёта (приложение 2 к Инструкции ФАПСИ).

После того, как СКЗИ было проинициализировано полученным дистрибутивом, пользователь должен убрать носитель с дистрибутивом первичной инициализации в индивидуальный сейф. Сейф должен быть оборудован устройством для опечатывания замочной скважины. Замочная скважина должна опечатываться индивидуальной печатью пользователя СКЗИ.

Отметим, что при настройке СКЗИ персональные ключи защиты пользователя, а также закрытый ключ сертификата электронной подписи должен переноситься на съёмный носитель с аутентификацией по паролю. Список поддерживаемых носителей указан в технической документации к СКЗИ. Рекомендуются, по возможности, записывать персональные ключи пользователя на съёмный носитель в момент выработки ключевой информации.

Съёмные носители, содержащие криптографические ключи в отсутствие пользователя в течении рабочего дня и в конце рабочего дня необходимо убирать в индивидуальный сейф. Сейф необходимо опечатывать индивидуальной печатью пользователя СКЗИ.

Носитель с индивидуальными криптографическими ключами пользователя категорически запрещено передавать иным сотрудникам организации. Пользователь несёт персональную ответственность за сохранение конфиденциальности своих криптографических ключей.

При выводе из действия ключей, необходимо провести их удаление (не позднее, чем 10 суток после вывода их из действия или окончания срока действия). Удаление ключей производится штатными средствами СКЗИ. При невозможности воспользоваться штатными средствами, допустимо использование сертифицированных средств гарантированного уничтожения информации. При невозможности гарантированного удаления ключевой информации производится физическое уничтожение самого носителя. После удаления ключей необходимо сделать отметку в журнале учёта.

В случае, если пользователь СКЗИ самостоятельно удаляет ключи, то он должен оповестить специалистов органа криптографической защиты о совершении данной операции устно (в тот же день) и письменно (не позднее 10 суток с момента совершения операции). Уничтожение большого количества ключевых документов должно быть оформлено актом. Не реже, чем один раз в год необходимо отправлять в орган криптографической защиты письменные отчёты об уничтоженных ключевых документах.

10 Резервные ключи

В случае, если пользователь обладает возможностью хранения резервных криптографических ключей, то таковые ему выдаются в ТФОМС Оренбургской области. Отметим, что резервные ключи должны храниться на отчуждаемом носителе в опечатываемом хранилище отдельно от основных криптографических ключей. Допускается хранение в опечатанном пользователем СКЗИ конверте в органе криптографической защиты информации (или у ответственного пользователя криптосредств) при соблюдении требований к хранению ключевой информации.

11 Действия при компрометации

Под компрометацией понимается утеря доверия к конфиденциальности используемых ключей. Пользователям СКЗИ рекомендуется обращаться в орган криптографической защиты

для консультаций по поводу отнесения криптографических ключей в категорию скомпрометированных. Например, увольнение сотрудника или оставление сотрудником носителя с криптографическими ключами без присмотра также является компрометацией ключей.

В случае возможной компрометации пользователь СКЗИ незамедлительно обращается в отдел информационной безопасности ТФОМС Оренбургской области по телефону и сообщает о факте компрометации. Орган криптографической защиты ТФОМС Оренбургской области объявляют ключ скомпрометированным и производит смену ключей.

В случае отсутствия возможности оперативной и безболезненной смены криптографических ключей, ТФОМС Оренбургской области может принять решение об использовании в течение максимально короткого промежутка времени скомпрометированных ключей.

12 Контроль за организацией и обеспечением безопасности хранения, обработки и передачи, с использованием СКЗИ, конфиденциальной информации

Пользователи СКЗИ должны неукоснительно соблюдать требования по обеспечению безопасности при работе с СКЗИ, и несут персональную ответственность за сохранность криптографических ключей, а также СКЗИ с эксплуатационной и технической документации к ним.

Ответственные пользователи криптосредств (органы криптографической защиты) обладателей конфиденциальной информации должны контролировать выполнение требований пользователями СКЗИ. О всех выявленных нарушениях необходимо информировать отдел информационной безопасности ТФОМС Оренбургской области.

ТФОМС Оренбургской области должен контролировать выполнение обладателями конфиденциальной информации данных им указаний по организации криптографической защиты в рамках информационного обмена в системе ОМС Оренбургской области.

Если в использовании СКЗИ выявлены серьёзные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то ТФОМС Оренбургской области вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений.

ТФОМС Оренбургской области вправе инициировать контрольные мероприятия в отношении обладателя конфиденциальной информации путём отправки письменного запроса в УФСБ по Оренбургской области с обоснованием необходимости такого контроля.

13 Заключительные положения

По всем вопросам, явно не освещённым в данном документе следует обращаться к нормативно-методической документации ФСБ и ФСТЭК России, а также к технической документации на СКЗИ.

Данное Положение должно регулярно пересматриваться для адаптации требований безопасности к выявленным уязвимостям в системе криптографической защиты информации.

Настоящее Положение согласовывается с УФСБ России по Оренбургской области на предмет соответствия требованиям нормативных документов в области криптографической защиты информации.