

**Государственное бюджетное учреждение здравоохранения
Тюменской области
Областная больница №7 (с. Армизонское)**

УТВЕРЖДАЮ

Главный врач ГБУЗ ТО
«Областная больница №7»

«_____» _____ Д.А. Бойко
2013г.



**ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных
при их обработке в информационной системе персональных данных
«Работники ЛПУ»
ГБУЗ ТО «Областная больница №7»**

1. Общие положения

1.1 Данные требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Работники ЛПУ» ГБУЗ ТО «Областная больница №7» (далее – ИСПДн) разработаны на основании приказа ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» и частной модели угроз ИСПДн.

1.2 Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных при их обработке в ИСПДн «Работники ЛПУ» ГБУЗ ТО «Областная больница №7».

2. Организационные мероприятия по обеспечению безопасности персональных данных

2.1 Задаются требования по: охране помещений, допуску лиц, выбору технических средств, их расположению в помещениях. Кроме того, задаются дополнительные требования по обеспечению конфиденциальности, целостности и доступности персональных данных (далее – ПДн).

2.2 К числу мер, необходимых и достаточных для обеспечения выполнения обязанностей оператора могут относиться:

2.2.1. Назначение оператором ответственного за организацию обработки персональных данных;

2.2.2. Издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- 2.2.3. Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- 2.2.4. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона от 27.07.2006 N 152-ФЗ (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ) «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом от 27.07.2006 N 152-ФЗ (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ) «О персональных данных»;
- 2.2.5. Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
- 2.2.6. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- 2.2.7. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.
- 2.2.8. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.
- 2.2.9. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.
- 2.2.10. Учет машинных носителей персональных данных.
- 2.2.11. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.
- 2.2.12. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- 2.2.13. Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с

персональными данными в информационной системе персональных данных.

2.2.14. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.3 Обеспечение безопасности персональных данных с использованием криптосредств должно осуществляться в соответствии с:

- Приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);
- Постановлением Правительства РФ от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;
- Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (№ 149/54-144, 2008 г. ФСБ России), Настоящими Требованиями.

2.4 Оператор персональных данных несет ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки с использованием криптосредств персональных данных, лицензионным требованиям и условиям, эксплуатационной и технической документации к криптосредствам, а также настоящим Требованиям.

2.5 При этом должна обеспечиваться комплексность защиты персональных данных, в том числе посредством применения некриптографических средств защиты.

2.6 При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе осуществляется:

- разработка для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;
- разработка на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;
- определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;
- установка и ввод в эксплуатацию средств защиты информации (в том числе криптографических) в соответствии с эксплуатационной и технической документацией к этим средствам;
- проверка готовности средств защиты информации (в том числе криптографических) к использованию с составлением заключений о возможности их эксплуатации;
- поэкземплярный учет используемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;
- разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах, с указанием в частности:
 - индекса, условного наименования и регистрационных номеров используемых криптосредств;
 - соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;
 - соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

2.7 Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

2.8 Сведения предусмотренные пунктами 5, 7¹, 10 и 11 части 3 статьи 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» должны быть предоставлены в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

2.9 Пользователи информационных систем персональных данных обязаны:

- не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;
- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
- немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.
- сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

2.10 Обеспечение функционирования и безопасности информационной системы персональных данных возлагается на ответственного пользователя, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь).

2.11 Ответственные пользователи должны иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

2.12 При определении обязанностей пользователя необходимо учитывать, что безопасность обработки с использованием криптосредств персональных данных обеспечивается:

- соблюдением пользователями криптосредств, конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;
- точным выполнением пользователями криптосредств, требований к обеспечению безопасности персональных данных;
- надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;
- обеспечением принятых в соответствии с Требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных мер.
- своевременным выявлением попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;
- немедленным принятием мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

2.13 Лица, оформляемые на работу в качестве пользователей (ответственных пользователей), должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.14 Текущий контроль за организацией и обеспечением функционирования средств защиты информации (в том числе криптографических) возлагается на оператора и ответственного пользователя в пределах их служебных полномочий.

2.15 Контроль за организацией, обеспечением функционирования и безопасности средств защиты информации (в том числе криптографических), предназначенных для защиты персональных данных, при их обработке в информационных системах персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации.

3. Мероприятия по обеспечению безопасности персональных данных от несанкционированного доступа при их обработке в информационной системе персональных данных

В комплекс мероприятий по защите ПДн при их обработке в ИСПДн «Работники ЛПУ» от несанкционированного доступа (далее – НСД) и неправомерных действий входят мероприятия, реализуемые в рамках подсистем:

- управления доступом,
- регистрации и учета,

- обеспечения целостности,
- обеспечения межсетевой безопасности.

Подсистема управления доступом

Для всех сотрудников ГБУЗ ТО «Областная больница №7», допущенных к обработке ПДн в ИСПДн «Работники ЛПУ», в подсистеме управления доступом должны быть реализованы идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов

Подсистема регистрации и учета

Для всех сотрудников Государственного бюджетного учреждения здравоохранения Тюменской области «Областная больница №7» (с. Армизонское), допущенных к обработке ПДн в ИСПДн «Работники ЛПУ», в подсистеме регистрации и учета должны быть реализованы следующие мероприятия:

1. регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АРМ. В параметрах регистрации указываются:
 - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
 - результат попытки входа (успешная или неуспешная – несанкционированная);
 - идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;
2. учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

Подсистема обеспечения целостности

В подсистеме обеспечения целостности должны быть реализованы следующие мероприятия:

1. обеспечение целостности программных средств СЗПДн, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных;
2. физическая охрана компонентов ИСПДн «Работники ЛПУ» (устройств и носителей информации), предусматривающая:
 - контроль доступа в помещения расположения АРМ ИСПДн «Работники ЛПУ» посторонних лиц;
 - наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн «Работники ЛПУ» и хранилище носителей информации, особенно в нерабочее время;

3. периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн «Работники ЛПУ» с помощью тест-программ, имитирующих попытки НСД;
4. наличие средств восстановления СЗПДн, предусматривающих ведение двух копий программных средств защиты информации и их периодическое обновление и контроль работоспособности.

Подсистема обеспечения безопасного межсетевого взаимодействия

В подсистеме обеспечения безопасного межсетевого взаимодействия при подключении ИСПДн к сетям международного информационного обмена безопасность ПДн достигается путем применения средств межсетевого экранирования, которые обеспечивают:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- контроль целостности своей программной и информационной части;
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Дополнительные требования.

Наряду с методами и способами, указанными выше, основными методами и способами защиты информации от несанкционированного доступа являются:

- обнаружение вторжений в операционную систему ИСПДн, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности ИСПДн, предполагающий применение специализированных программных средств (сканеров безопасности);
- использование средств антивирусной защиты;
- централизованное управление средствами защиты информации ИСПДн.
- применение программного обеспечения средств защиты информации, соответствующего 4 уровню контроля отсутствия недеklarированных возможностей.

4. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей

4.1 Пользователи криптосредств обязаны:

- не разглашать информацию о ключевых документах;
- не допускать снятие копий с ключевых документов;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевых документов в другие ПЭВМ.

4.2 При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

4.3 Крипсредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

4.4 Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

4.5 Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземпляльному учету. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

4.6 Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

4.7 Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под

расписку в соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.

4.8 Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущем непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).

4.9 Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

4.10 Пользователи криптосредств хранят устанавливающие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

4.11 Пользователи криптосредств предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

4.12 Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

4.13 Крипсредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными оператором ответственными пользователями криптосредств и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки.

4.14 Эксплуатационную и техническую документацию к криптосредствам допускается пересылать заказными или ценными почтовыми отправлениями.

4.15 Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

4.16 Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а

также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

4.17 Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

4.18 Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин.

4.19 Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

4.20 Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

4.21 Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах уничтожаются пользователями этих криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.

4.22 Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного пользователя криптосредств для списания уничтоженных документов с их лицевых счетов.

4.23 Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, устанавливающих криптосредства носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

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

4.25 О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств и (или) оператору.

4.26 Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

4.27 В случаях недосдачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

4.28 Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет оператор.

Заместитель главного врача по
организационно-методической работе
с населением
ГБУЗ ТО «Областная больница №7»

Л.А. Новосильцева