Департамент здравоохранения Тюменской области
Государственное бюджетное учреждение здравоохранения
Тюменской области
«Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

П Р И К А З

22 февраля 2023г. № 26 ос

с. Казанское

Об организации применения средств криптографической защиты информации

В целях исполнения требований Федерального закона РФ от 27 июля 2006 года № 149 «Об информации, информационных технологиях и защите информации», приказа ФСБ России от 09.02.2005 № 66 **п р и к а з ы в а ю :**

1. Установить в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – Учреждение) режим защиты информации с применением средств криптографической защиты информации (далее – СКЗИ).
2. Назначить ответственным за эксплуатацию СКЗИ в Учреждении (администратором СКЗИ) – администратора вычислительных сетей.
3. Возложить на администратора СКЗИ:
- организацию поэкземплярного учета используемых в Учреждении СКЗИ;
- контроль за соблюдением правил пользования в Учреждении СКЗИ;
- проведение расследования фактов нарушения правил пользования СКЗИ.
4. Утвердить:
- положение о применении шифровальных (криптографических) средств защиты информации в Учреждении (Приложение № 1 к настоящему приказу);
- инструкцию администратору СКЗИ (Приложение № 2 к настоящему приказу);
- инструкцию пользователю СКЗИ (Приложение № 3 к настоящему приказу);

– форму журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 4 к настоящему приказу);

– форму журнала учета пользователей СКЗИ(Приложение № 5 к настоящему приказу);

– форму журнала технический (аппаратный) пользователя СКЗИ (Приложение № 6 к настоящему приказу);

– инструкцию по восстановлению связи в случае компрометации действующих ключей к СКЗИ(Приложение № 7 к настоящему приказу).

5. Контроль за исполнением настоящего приказа возложить на заместителя главного врача.

Главный врач Д.М. Суворов

Приложение № 1
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 26ос

Положение
о применении шифровальных (криптографических) средств защиты информации в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Термины, определения и сокращения

Автоматизированное рабочее место (АРМ)	– программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.
Доступ к информации (доступ)	– ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение.
Информационная система (ИС)	– система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
Ключевая документация	– отчуждаемый носитель ключевой информации с записанной на него ключевой информацией.
Ключевая информация	– специальным образом организованная совокупность криптографических ключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.
Компрометация ключа (ключевой информации)	– факт (или подозрение на факт) раскрытия закрытой ключевой информации, утрата доверия к тому, что используемые криптографические ключи обеспечивают подлинность, защищенность и безопасность информации.
Криптографический ключ (криптоключ)	– совокупность данных, определяющая конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования

	данных, обеспечивающих выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.
Конфиденциальность информации	– обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.
Ответственный пользователь криптосредств	– должностное лицо Учреждения, на которого возлагается обеспечение функционирования и безопасности криптосредств.
Отчуждаемый носитель ключевой информации	– отчуждаемый физический носитель информации, определенной структуры, предназначенный для хранения на нем ключевой информации.
Пользователь криптосредств	– сотрудник Учреждения, осуществляющий эксплуатацию криптосредств.
Правила доступа	– совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
Сертификат ключа подписи (сертификат ключа проверки электронной подписи)	– электронный документ или документ на бумажном носителе, выданные удостоверяющим центром, либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Средство криптографической защиты информации (СКЗИ, криптосредство, шифровальное (криптографическое) средство)	– а) средство шифрования – аппаратное, программное и аппаратно-программное средство, система или комплекс, реализующее алгоритмы криптографического преобразования информации и предназначенное для защиты информации от несанкционированного доступа при ее передаче по каналам связи и/или при ее обработке и хранении; б) средство имитозащиты – аппаратное, программное или аппаратно-программное средство, система или комплекс, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средство электронной подписи – аппаратное, программное или аппаратно-программное средство, обеспечивающее на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение, с использованием открытого ключа электронной подписи, подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;

г) средство кодирования – средство, реализующее алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средство изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

1. Общие положения

1.1. Для защиты информации ограниченного доступа, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, на объекте информатизации (далее – ОИ) –ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – Учреждение), используются программные шифровальные (криптографические) средства, сертифицированные ФСБ России.

1.2. Криптографические методы защиты информации основаны на осуществлении над сведениями, представленными в электронной форме, определенных математических преобразований, которые выполняются с помощью программных шифровальных средств, обладающих некоторым секретным параметром этих преобразований, называемым криптографическим ключом. Без указанного криптографического ключа повторить указанное математическое преобразование и/или восстановить подвергнутые преобразованию данные за обозримое время практически невозможно.

1.3. Применение шифровальных (криптографических) средств защиты информации (далее – СКЗИ) предполагает обязательное предварительное доведение до пользователей этих средств необходимой ключевой информации, без наличия которой криптографическая система не сможет осуществить криптографические преобразования.

1.4. Сведения об использовании криптосредств для защиты информации на ОИ, схеме их размещения, используемых криптографических ключах, ключевой информации, используемых отчуждаемых носителях этой информации, принимаемых, на ОИ организационно-технических мерах защиты СКЗИ и ключевой информации к ним, являются информацией конфиденциального характера и подлежат защите.

1.5. Настоящее Положение является нормативным актом Учреждения и определяет:

- основные обязанности, права и ответственность ответственного пользователя и пользователей средств криптографической защиты информации (далее – криптосредств) на ОИ;
- порядок действий пользователя криптосредств по использованию криптосредств для организации и осуществления защищенного обмена на ОИ, сведениями, доступ к которым ограничен законодательством Российской Федерации;
- порядок обращения пользователя криптосредств с криптосредствами, технической и эксплуатационной документации к ним;
- порядок обращения пользователя криптосредств с ключевой информацией, необходимой для осуществления шифрованного обмена сведениями ограниченного доступа на ОИ;
- порядок действий пользователя криптосредств при компрометации его криптографических ключей.

1.6. Настоящая инструкция разработана с учетом требований, следующих нормативных методических документов ФСБ России:

– «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденное приказом ФСБ России от 09.02.2005 № 66 и зарегистрированное в Министерстве юстиции Российской Федерации 03.03.2005 № 6382;

– «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные приказом ФСБ России № 149/54-144, 2008 г.;

– «Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утвержденные приказом ФСБ России от 10.07.2014 № 378.

1.7. Допуск сотрудников Учреждения к криптосредствам и ключевой информации для них, осуществляется только после прохождения этими сотрудниками необходимой подготовки, изучения организационно-распорядительных документов, регламентирующих порядок обращения с шифровальными средствами, технической, эксплуатационной и ключевой документации к ним, подписания ими письменного обязательства о неразглашении сведений ограниченного доступа, на основании приказа главного врача Учреждения.

1.8. Перед тем, как приступить к работе на автоматизированном рабочем месте, оснащённом криптосредствами, пользователь криптосредств обязан:

– ознакомиться с настоящим Положением, другими нормативными и инструктивными документами Учреждения, регламентирующими порядок использования криптосредств, технической, эксплуатационной и ключевой документацией к ним под роспись;

– изучить техническую и эксплуатационную документацию к используемым на ОИ шифровальным средствам, а также правила работы с ними;

– получить у ответственного пользователя криптосредств ОИ необходимые ключевые документы.

1.9. Деятельность адмиристратора криптосредств регламентируется Инструкцией администратора средств криптографической защиты информации.

1.10. Деятельность пользователей криптосредств регламентируется Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну с использованием средств криптографической защиты и контролируется ответственным пользователем криптосредств ОИ, а также федеральным надзорными органами в области связи и массовых коммуникаций (Роскомнадзор) и федеральными органами безопасности, в соответствии с законодательством Российской Федерации.

2. Основные обязанности пользователей криптосредств

2.1 Все пользователи криптосредств, допущенные установленным порядком к использованию криптосредств, технической, эксплуатационной документации, обязаны:

– не разглашать сведения, к которым они допущены или которые стали им известны по работе, включая персональные данные циркулирующие, обрабатываемые и хранимые на ОИ, в том числе сведения об используемых 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;

– строго выполнять требования технической и эксплуатационной документации к сертифицированным криптосредствам;

– обеспечивать надежное хранение инсталляционных носителей криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, а также надежное хранение имеющихся у них магнитных носителей со сведениями ограниченного доступа;

– сообщать ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения ограниченного доступа циркулирующие, обрабатываемые и хранимые на ОИ, а также сведения об используемых криптосредствах или ключевых документах к ним;

– немедленно уведомлять своего непосредственного руководителя и ответственного пользователя криптосредств ОИ о фактах нарушения целостностей печатей на системных блоках АРМ, утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений ограниченного доступа, в том числе обрабатываемых персональных данных;

– немедленно принимать меры по предупреждению возможного разглашения защищаемых сведений ограниченного доступа, в том числе персональных данных циркулирующих, обрабатываемых и хранимых на ОИ, при выявлении фактов нарушения целостностей печатей на системных блоках АРМ, утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.;

– при увольнении, перед уходом в отпуск или отъездом в длительную командировку (более 1 месяца) сдать ответственному пользователю криптосредств ОИ все инсталляционные носители криптосредств, эксплуатационную и техническую документацию к ним, отчуждаемые носители ключевой информации с ключевой документацией к шифровальным средствам.

3 Порядок обращения с СКЗИ, технической, эксплуатационной и ключевой документацией к ним

3.1 Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-2005.

При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. 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.

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.

3.2 Все полученные обладателем конфиденциальной информации 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.

3.3 Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ.

3.4 Для обеспечения шифрованного обмена сведениями ограниченного доступа на ОИ на АРМ пользователя криптосредств инсталлируется сертифицированное ФСБ России программное криптосредство. Пользователю криптосредств под роспись в Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов ответственным пользователем криптосредств выдаются инсталляционный носитель указанного средства, а также техническая и эксплуатационная документация к этому носителю. Кроме того, пользователям криптосредств под роспись в Журнале учёта криптосредств, выдаётся ответственным пользователем криптосредств необходимая для работы с СКЗИ ключевая информация, занесенная на отчуждаемый носитель ключевой информации.

3.5 Передача инсталляционных носителей криптосредств, аппаратных вычислительных средств, в которые инсталлированы криптосредства, эксплуатационной и технической документации, ключевых документов к этим средствам допускается только между пользователем криптосредств и ответственным пользователем криптосредств ОИ под расписку в Журнале учёта криптосредств.

Передача инсталляционных носителей криптосредств, аппаратных вычислительных средств, в которые инсталлированы шифровальные средства, эксплуатационной и технической документации, ключевых документов к этим средствам между пользователями запрещается.

3.6 Пользователь криптосредств несёт персональную ответственность за сохранность, выданных ему инсталляционных носителей, эксплуатационной, технической и ключевой документации к криптосредствам.

3.7 Помещения, где установлены АРМ с размещенными шифровальными средствами и/или хранится эксплуатационная, техническая и ключевая документация к ним, обрабатываются защищаемые сведения ограниченного доступа, в том числе персональные данные, являются режимными помещениями.

Размещение, специальное оборудование, охрана и организация режима в таких помещениях направлены на то, чтобы свести к минимуму возможность неконтролируемого доступа посторонних лиц к защищаемым сведениям, шифровальным средствам и документации к ним. Порядок доступа в режимные помещения определяется Инструкцией по управлению доступом к техническим средствам, информационным ресурсам и помещениям.

3.8 Для хранения пользователями криптосредств отчуждаемых носителей конфиденциальной информации (сведений ограниченного доступа), инсталляционных носителей криптосредств, технической, эксплуатационной и ключевой документации к ним в режимных помещениях, где находятся криптосредства, размещаются металлические хранилища, оборудованные внутренними замками с двумя экземплярами ключей или кодовыми замками и приспособлениями для опечатывания дверей хранилищ.

Хранение конфиденциальных документов, отчуждаемых носителей ключевой информации, нормативной и эксплуатационной документации к средствам электронной цифровой подписи разрешается только в металлических шкафах (хранилищах, сейфах).

При вынужденных перерывах в работе отчуждаемые носители ключевой информации и другие конфиденциальные документы должны быть помещены в хранилище, а хранилище должно быть опечатано личной печатью.

Допускается хранение отчуждаемых носителей ключевой информации в одном хранилище с другими документами в условиях, исключающих их непреднамеренное уничтожение, если иное не предусмотрено правилами их использования.

В случае отсутствия у пользователя криптосредств индивидуального хранилища, отчуждаемые носители ключевой информации, по окончании рабочего дня, должны сдаваться им ответственному пользователю криптосредств ОИ.

3.9 Системные блоки АРМ пользователей криптосредств должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) системных блоков должно быть таким, чтобы его можно было визуально контролировать. Все незадействованные штатным образом разъемы системных блоков рекомендуется демонтировать или закрыть под кожухами, или оснастить средствами контроля за вскрытием.

3.10 В целях соблюдения установленного порядка допуска в режимные помещения, а также допуска к аппаратно-программным ресурсам АРМ, в том числе и криптосредствам, пользователь криптосредств обязан:

–в конце рабочего дня осуществить штатным образом, согласно технической и эксплуатационной документации на установленное криптосредство, выход из программного обеспечения криптосредств. Извлечь штатным образом из разъема АРМ отчуждаемый носитель ключевой информации, отключить штатным образом электропитание АРМ;

–убрать на хранение в хранилище отчуждаемые носители с конфиденциальной информацией, в том числе с персональными данными, носитель ключевой информации, техническую и эксплуатационную документацию к криптосредствам, иные документы и носители, содержащие сведения ограниченного доступа. Закрыть и опечатать личной печатью хранилище;

–закрыть и опечатать режимное помещение и сдать его установленным образом под охрану, ключ от помещения сдать в опечатанном виде дежурному техническому администратору ОИ с указанием времени сдачи и с отметкой о включении охранной сигнализации в соответствующем журнале;

–перед вскрытием режимного помещения, в котором размещен АРМ, проверить целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывать, а о случившемся немедленно поставить в известность руководство Учреждения и ответственного пользователя криптосредств ОИ;

–при утрате ключа от входной двери режимного помещения немедленно поставить в известность ответственного пользователя криптосредств ОИ и руководство Учреждения;

–для предотвращения просмотра извне, в течение рабочего времени, держать двери режимного помещения закрытыми;

запрещается оставлять открытыми двери и препятствовать технической системе контроля доступа выполнять свои функции;

–перед началом работы убедиться в целостности оттисков печатей на устройствах опечатывания системного блока АРМ.

3.11 В процессе работы пользователь криптосредств обязан:

–не разглашать информацию о ключевых документах;

–не передавать отчуждаемые носители ключевой информации лицам к ним не допущенным;

передача по техническим средствам связи криптографических ключей и/или ключевой информации для используемых в ИС шифровальных средств не допускается;

–не допускать снятие копий с ключевых документов;

–не допускать вывод ключевых документов на дисплей (монитор), принтер или другие внешние устройства отображения информации;

–не допускать записи на отчуждаемый ключевой носитель посторонней информации;

–не допускать установки ключевых документов в другие ПЭВМ;

–не подключать к АРМ с шифровальными средствами дополнительные устройства и соединители без соответствующего предписания ответственного пользователя криптосредств на возможность их совместного использования;

–не работать с СКЗИ, если во время загрузки ПО не проходит встроенный тест;

–не оставлять, при включенном питании, АРМ без присмотра;

–не оставлять отчуждаемые носители ключевой информации без присмотра, подключенными к системному блоку АРМ на своем рабочем месте;

–не допускать несанкционированной установки, создания и выполнения на аппаратно-программной платформе АРМ посторонних программ;

–не осуществлять вскрытие системных блоков АРМ.

3.12 В процессе эксплуатации АРМ с установленными шифровальными средствами пользователь криптосредств обязан осуществлять предусмотренные эксплуатационной и технической документацией, к указанным средствам, текущие профилактические процедуры.

3.13 Срок действия ключевых документов определяется требованиями эксплуатационной и технической документации к шифровальным средствам.

Пользователь криптосредств обязан заблаговременно получить у ответственного пользователя криптосредств новые ключевые документы.

Запрещается использование ключевых документов, срок действия которых истёк.

3.14 Плановая смена ключевых документов должна осуществляться пользователями криптосредств в соответствии с технической и эксплуатационной документацией на используемые криптосредства, нормативными и инструктивными документами Учреждения, регламентирующими использование криптосредств на ОИ.

3.15 Пользователи криптосредств могут получить отчуждаемый носитель ключевой информации с записанной на него ключевой информацией у ответственного пользователя криптосредств.

3.16 Отчуждаемый носитель ключевой информации передается пользователю криптосредств ответственным пользователем криптосредств только лично под расписку в Журнале учёта криптосредств после идентификации пользователя криптосредств с использованием документа удостоверяющего личность пользователя криптосредств, указанного в заявке.

3.17 Допускается осуществление смены ключевой информации пользователя криптосредств без замены ему отчуждаемого носителя ключевой информации.

В этом случае подготовка и запись новой ключевой информации на предоставляемый пользователем криптосредств отчуждаемый носитель с ключевой информацией, срок действия которой истек (или которая выведена из действия установленным образом), осуществляется ответственным пользователем криптосредств непосредственно по прибытии пользователя криптосредств на рабочее место, после идентификации личности пользователя криптосредств.

Перед осуществлением записи новой ключевой информации на предоставленный пользователем криптосредств отчуждаемый носитель

ответственный пользователь криптосредств должен провести предусмотренную эксплуатационной и технической документацией к используемому криптосредству процедуру стирания с него старой ключевой информации.

3.18 Получение резервной ключевой документации осуществляется пользователем криптосредств тем же порядком, что и при плановой смене криптографических ключей. Пользователи криптосредств должны обеспечить раздельное безопасное хранение действующей ключевой документации от резервной ключевой документации, предназначенной для применения в случае компрометации действующих криптографических ключей.

3.19 Неиспользованные или выведенные из действия ключевые документы возвращаются пользователем криптосредств под расписку в Журнале учёта криптосредств ответственному пользователю криптосредств или, по его указанию, должны быть уничтожены на месте пользователем криптосредств самостоятельно.

В последнем случае, пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптографические ключи.

3.20 Уничтожение, неиспользованных или выведенных из действия, ключевых документов осуществляется:

–путем физического уничтожения (разрушения) отчуждаемых носителей ключевой информации для чего носителю наносится неустранимые физические повреждения, исключающие возможность его использования или восстановления;

–путем стирания ключевой информации с отчуждаемых носителей (без его повреждения для обеспечения возможности многократного использования), согласно процедуре, предусмотренной эксплуатационной и технической документацией к криптосредству.

3.21 Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения указанной 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 Журнале учёта криптосредств.

4 Действия пользователя криптосредств в случае компрометации его ключевой информации

4.1 Под компрометацией криптографических ключей понимается утрата доверия к тому, что данный ключ обеспечивает необходимую защиту информации. Криптографические ключи, которые подверглись компрометации или в отношении которых возникло подозрение в компрометации, должны быть незамедлительно выведены из действия.

4.2 К событиям, которые должны рассматриваться, как компрометация (или подозрение на компрометацию) криптографических ключей относятся:

- утрата отчуждаемых носителей ключевой информации;

– утрата отчуждаемых носителей ключевой информации с их последующим обнаружением;

– увольнение сотрудника, имевшего доступ к ключевой информации и/ или к отчуждаемому носителю ключевой информации на котором она записана;

– выявление фактов нарушения правил использования, хранения и/или уничтожения криптографических ключей;

– нарушение целостности упаковки отчуждаемых носителей ключевой информации и/или печати на хранилище, где хранились эти носители;

– нарушение целостности печати на системном блоке АРМ, на кожухе или незадействованных штатным образом разъемах системных блоков;

– вскрытие фактов или возникновение подозрений об утечке, искажении защищаемых на ОИ сведений.

Первые четыре события должны трактоваться как безусловная компрометация криптографических ключей. Остальные - как возможная их компрометация.

Внешний осмотр отчуждаемого носителя ключевой информации, системного блока АРМ (кожуха АРМ) посторонними лицами не следует рассматривать как подозрение на компрометацию записанных или используемых в них криптографических ключей, если при этом исключалась возможность несанкционированного доступа к указанным изделиям с копированием, чтением, размножением или передачей ключевой информации в канал связи.

4.3 При наступлении любого из перечисленных случаев, или иных нарушениях, которые могут привести к компрометации криптографических ключей, пользователь криптосредств должен прекратить использование указанного АРМ и встроенного в него СКЗИ и немедленно сообщить об этом ответственному пользователю криптосредств и своему непосредственному руководителю.

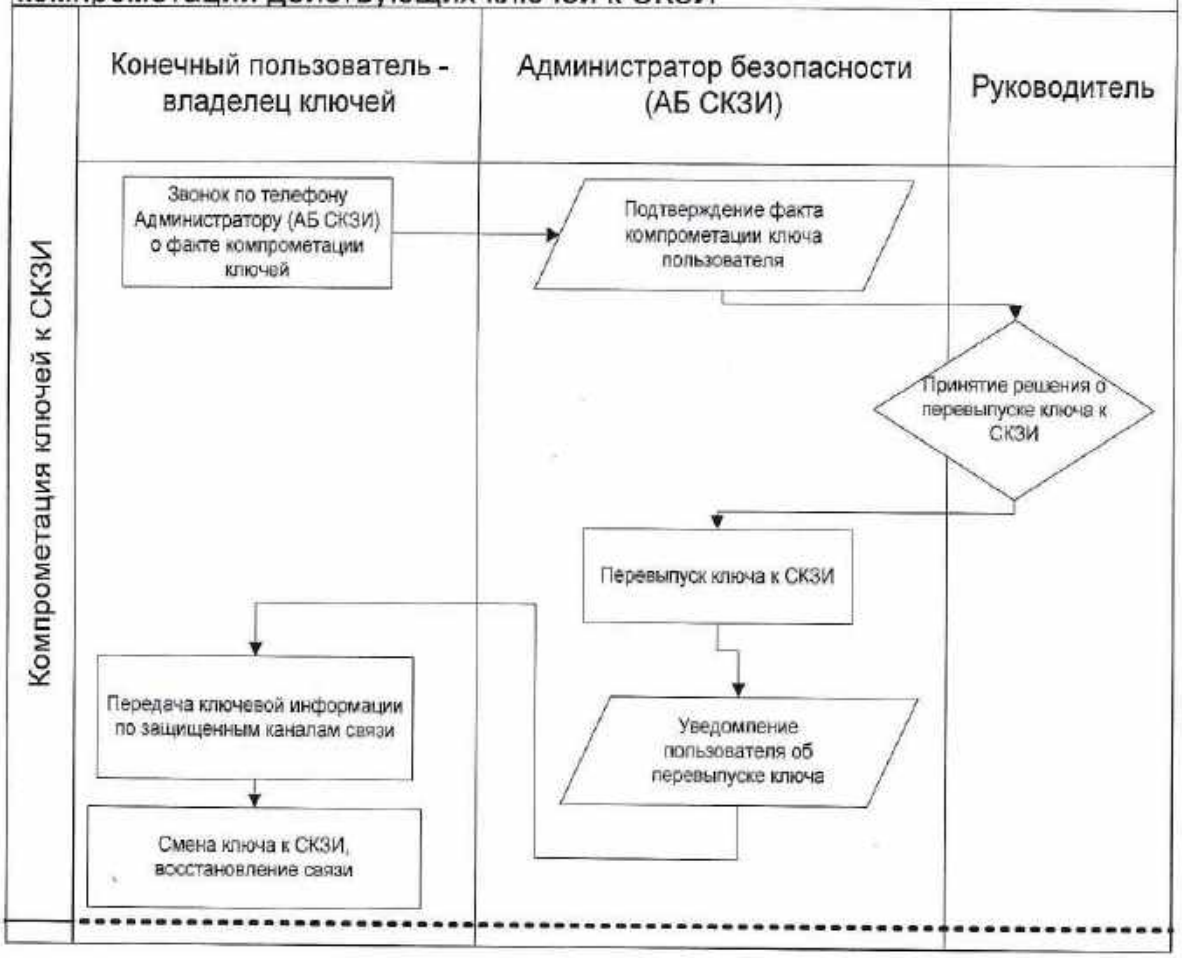
4.4 Служебное расследование факта компрометации (или предполагаемой компрометации) производится внутренней комиссией, создаваемой на основании приказа главного врача Учреждения.

При установлении факта компрометации ключевой информации, скомпрометированные ключевые документы выводятся из действия и уничтожаются установленным порядком.

4.5 При необходимости оперативного восстановления шифрованного обмена информацией с узлом сети ключевые документы которого подверглись компрометации, ответственным пользователем криптосредств по согласованию с председателем комиссии может быть дано указание пользователю криптосредств об использовании резервной ключевой информации, если только она не подверглась компрометации одновременно с действующими ключевыми документами.

Порядок восстановлению связи в случае компрометации ключевой информации приведен на схеме:

Последовательность действий по восстановлению связи в случае компрометации действующих ключей к СКЗИ



Приложение № 2
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 26 ос

Инструкцию
администратору средств криптографической защиты информации

1. Общие положения

1.1. Инструкция определяет:

– основные обязанности, права и ответственность Администратора средств криптографической информации (далее – СКЗИ) на объекте информатизации (далее – ОИ) – ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – Учреждения);

– порядок подготовки, учета, хранения, использования, смены и уничтожения ключевой информации;

– действия при компрометации ключей;

– порядок обращения с СКЗИ;

– требования к помещениям, в которых ведется работа с ключами и СКЗИ.

1.2. Инструкция разработана с учетом нормативно-методических документов ФСБ России и эксплуатационной документации на СКЗИ.

1.3. Администратор СКЗИ назначается приказом и допускаются к работе только после прохождения необходимой подготовки.

1.4. Администратор СКЗИ обязан:

– выполнять требования настоящей инструкции и других внутренних документов Учреждения, регламентирующих порядок работы с СКЗИ, а также правила, изложенные в эксплуатационной документации на СКЗИ, в части, его касающейся; он знакомится с указанными документами под роспись;

– выполнять указанные в лицензиях ФСБ России требования и условия осуществления разрешенных видов деятельности и условия сертификатов на эксплуатируемые СКЗИ;

– взаимодействовать с сотрудником, отвечающим за защиту информации в Учреждении;

– принять на себя обязательство по нераспространению доверенных ему сведений в период работы и в течение двух лет после увольнения, если больший срок не оговаривается в контракте (договоре).

2. Основные функциональные обязанности администратора СКЗИ

2.1. Взаимодействие с органами лицензирования и сертификации ФСБ России, разработчиками (производителями) СКЗИ при развитии и совершенствовании ОИ.

2.2. Участие в разработке типовых договоров с Пользователями ОИ в части использования криптографических методов защиты информации.

2.3. Разработка и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ.

2.4. Регистрация Пользователей ОИ. Координация деятельности Пользователей ОИ по разработке схем связи и распределению ключей, обеспечению необходимыми документами, анализу информации по обеспечению безопасности ОИ в целом, разработке и направлению указаний и рекомендаций по организации системы защиты и повышению ее надежности.

2.5. Поддержание функционирования и управление ключевой системой: формирование секретных и открытых ключей шифрования и электронной подписи (далее – ЭП) Пользователей, изготовление сертификатов открытых ключей, учет, хранение, ввод в действие и смена ключей Пользователей, уничтожение ключевой информации.

2.6. Разработка парольной системы оповещения о компрометации на ОИ.

2.7. Организация подготовки Пользователей ОИ по применению СКЗИ.

2.8. Управление доступом Пользователей ОИ к программному обеспечению (далее – ПО) и данным, включая установку и периодическую смену паролей, управление средствами защиты программного обеспечения, коммуникаций, передаваемых, хранимых и обрабатываемых данных.

2.9. Контроль за работой Пользователей СКЗИ, выявление и регистрация попыток несанкционированного доступа к защищаемым информационным ресурсам. Администратор СКЗИ должен периодически (рекомендуется не реже 1 раза в 2 месяца)проводить контроль сохранности входящего в состав СКЗИ оборудования и целости печатей системных блоков, а также контроль целостности установленных копий ПО на всех АРМ со встроенным СКЗИ с помощью программ контроля целостности, входящих в комплект СКЗИ, для предотвращения внесения программно-аппаратных закладок и программ вирусов.

2.10. Контроль целостности программного обеспечения СКЗИ рекомендуется осуществлять при каждом запуске персональной электронно-вычислительной машины (далее – ПЭВМ) в соответствии с эксплуатационной документацией.

2.11. Восстановление работоспособности средств и систем защиты информации.

2.12. Организация защиты компьютеров от вирусов и программ, направленных на разрушение установленного программного обеспечения.

2.13. Ведение журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов и аппаратного журнала.

2.14. Участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации, в том числе в случае компрометации действующих ключей.

2.15. Доклад непосредственному руководителю о выявленных нарушениях и несанкционированных действиях Пользователей, принятие необходимых мер по устранению нарушений.

2.16. Участие в разборе конфликтных ситуаций и доказательстве авторства электронного документа, снабженного электронной цифровой подписью.

3. Права администратора СКЗИ

Администратор СКЗИ имеет право:

3.1. Требовать от Пользователей безусловного соблюдения установленной технологии обработки электронных документов и выполнения инструкций по обеспечению безопасности и защиты информации.

3.2. Инициировать обращение к руководителю Пользователя с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации.

3.3. Обращаться к сотруднику, отвечающим за защиту информации с просьбой об оказании технической и методической помощи в работе по обеспечению технической защиты информации.

3.4. Вносить предложения руководству Учреждения по совершенствованию использования СКЗИ.

4. Ответственность администратора СКЗИ

4.1. На Администратора СКЗИ возлагается персональная ответственность за соблюдение регламента эксплуатации программно-аппаратных средств криптографической защиты информации.

4.2. Администратор СКЗИ несет персональную ответственность за сохранность конфиденциальной ключевой информации от несанкционированного доступа посторонних лиц.

5. Порядок подготовки ключевой информации для пользователей системы

5.1. Администратор СКЗИ должен выполнить следующие действия по формированию ключей пользователей:

- выработать личные секретные и открытые ключи шифрования и ЭП Пользователей и сформировать личные ключевые носители Пользователей (с секретными и открытыми ключами шифрования и ЭП);
- сформировать резервные копии личных секретных ключей Пользователей;
- получить распечатки открытых ключей шифрования и ЭП Пользователей (регистрационные карточки) в двух экземплярах (по одной для Учреждения и Пользователя, каждая заверена подписями Администратора СКЗИ и Пользователя);
- сформировать справочник открытых ключей шифрования и ЭП всех Пользователей ОИ.

5.2. Аналогичным образом вырабатываются резервные ключи шифрования и ЭП, предназначенные для использования в случае компрометации действующих ключей. Открытые резервные ключи шифрования и ЭП заносятся в соответствующий справочник с атрибутом «резервные».

5.3. Выработанные ключевые носители с ключами шифрования и ЭП передаются Пользователям. Одновременно с этим, Пользователям передаются регистрационные карточки открытых ключей ЭП Администратора СКЗИ, а также эти ключи в электронном виде (на ключевом носителе).

6. Порядок обращения с ключевой, архивной и иной конфиденциальной информацией по СКЗИ

6.1. Все носители ключевой информации и СКЗИ должны браться на поэкземплярный учет в выделенных для этих целей журналах.

6.2. Администратор СКЗИ ведет учет изготовленных для Пользователей ключей, регистрацию их выдачи для работы, возврата от Пользователей и уничтожения в Журнале учета ключевых документов.

6.3. Условия хранения и транспортировки магнитных носителей должны исключать возможность их коробления, изгиба под воздействием температуры или другим причинам, а также воздействия пыли, магнитных и электрических полей.

Для защиты ключевой и архивной информации от механических, электромагнитных и других факторов воздействия, приводящих к разрушению информации, либо ее искажению, целесообразно хранить носители в футлярах из экранирующего материала.

6.4. Для хранения конфиденциальных документов, носителей ключевой информации, нормативной и эксплуатационной документации, инсталляционных носителей СКЗИ помещения обеспечиваются металлическими шкафами (хранилищами, сейфами). При вынужденных перерывах в работе, лицо производящее обработку информации должно поместить документы в свой сейф и опечатать сейф своей личной печатью. Дубликаты ключей от хранилищ должны храниться в сейфе ответственного лица, назначаемого руководством Учреждения.

6.5. Вне процесса работы документы, ключевая информация, носители архивной информации должны находиться в специально оборудованных металлических шкафах, либо сейфе сотрудника отвечающего за защиту информации.

6.6. Хранение носителей ключей допускается в одном хранилище с другими документами в условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

Наряду с этим должна быть предусмотрена возможность раздельного безопасного хранения рабочих ключевых носителей и резервных ключевых носителей, предназначенных для использования в случае компрометации ключей в соответствии с правилами пользования СКЗИ.

6.7. В случае отсутствия у Пользователя индивидуального хранилища носители ключей по окончании рабочего дня должны сдаваться им лицу, ответственному за их хранение.

6.8. Пересылка (передача) носителей ключей может осуществляться через фельдъегерскую или специальную связь, а также со специально

выделенным нарочным (в опечатанном администратором безопасности конверте).

6.9. Плановую смену ключей у Пользователей ОИ рекомендуется производить не реже чем через 1 год и три месяца.

6.10. После плановой смены ключей или компрометации ключей Пользователи СКЗИ уничтожают выведенные из действия секретные ключи шифрования и ЭП со всех магнитных носителей не позднее, чем через одни сутки после момента вывода ключей из действия.

Ключевая информация на носителях уничтожается Пользователем путем переформатирования с использованием ПО СКЗИ и дальнейшего уничтожения носителя. Допускается данные носители после переформатирования использовать в дальнейшем Пользователями Системы при условии записи на них новой ключевой информации.

Об уничтожении ключей делается соответствующая запись в Журнале учета ключевых документов.

Перед уничтожением секретных ключей следует расшифровать архивную информацию, хранящуюся в зашифрованном виде, и перешифровать ее на новых ключах.

7. Восстановление конфиденциальной связи после компрометации действующих ключей

7.1. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями.
- случаи, когда нельзя достоверно установить, что произошло с МНИ, содержащими ключевую информацию (в том числе случаи, когда МНИ вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

7.2. При наступлении любого из перечисленных выше событий Пользователь должен немедленно прекратить связь с другими Пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) Администратору СКЗИ.

7.3. Администратор СКЗИ обязан оперативно оповестить всех Пользователей ОИ о факте (или предполагаемой) компрометации.

7.4. Расследование факта (или предполагаемой) компрометации должно проводиться на месте происшествия уполномоченными лицами.

При установлении факта компрометации действующих ключей, скомпрометированные секретные ключи шифрования и подписи уничтожаются.

7.5. Меры по восстановлению конфиденциальной связи при компрометации ключей.

Регистрация новых ключей шифрования и ЭП происходит так же, как и при плановой смене ключей.

Администратор СКЗИ должен оповестить остальных Пользователей о замене ключей у восстанавливаемого Пользователя и сообщить им его открытые ключи.

8. Порядок обращения со средствами криптографической защиты информации

8.1. Установка СКЗИ производится только лицами, имеющими соответствующие полномочия и подготовку.

8.2. К эксплуатации СКЗИ допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на СКЗИ.

8.3. Все программное обеспечение ПЭВМ, на которой будет осуществляться генерация ключей, должно быть лицензионным, при этом не допускается наличие средств разработки и отладки программ.

8.4. Перед установкой СКЗИ необходимо проверить программное обеспечение ПЭВМ на отсутствие вирусов и программных закладок.

8.5. Системные блоки ПЭВМ с установленными СКЗИ должны опечатываться специально выделенной для этих целей печатью. Наряду с этим допускается применение других средств контроля их вскрытия.

8.6. Размещение и установка СКЗИ осуществляются в соответствии с требованиями документации на СКЗИ. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

8.7. Для генерации ключей выделяется отдельная ПЭВМ, доступ к которой должны иметь только специально уполномоченные лица. Данная ПЭВМ не должна быть подключена ни к какой сети компьютерной связи и должна использоваться только для работы в режиме администратора.

8.8. Перед непосредственной установкой ПО СКЗИ необходимо осуществить контроль целостности дистрибутива. После завершения процесса установки должны быть выполнены действия, необходимые для осуществления ежедневного контроля, установленного ПО, а также его окружения.

8.9. В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ с СКЗИ должна быть прекращена. По данному факту должно быть проведено служебное расследование и проведены работы по анализу и ликвидации негативных последствий данного нарушения.

9. Требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ

9.1. Размещение, специальное оборудование, охрана и режим в помещениях, в которых ведется работа с СКЗИ и ключами (далее – помещения), должны обеспечивать безопасность информации, СКЗИ и ключей, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

9.2. Порядок допуска в помещения определяется внутренней инструкцией или приказом по Учреждению. Доступ лиц в эти помещения должен быть ограничен в соответствии со служебной необходимостью. Рекомендуется использовать технические системы ограничения доступа в эти помещения. Допуск в помещения вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) производится только в случае служебной необходимости в сопровождении ответственного за режим после принятых мер, исключающих визуальный просмотр конфиденциальных документов.

9.3. Входные двери помещений должны быть прочными и оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время. Для контроля за входом в рабочее время рекомендуется устанавливать кодовые замки.

9.4. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения.

9.5. Для предотвращения просмотра извне окна помещений должны быть защищены (оборудованы жалюзи или шторами и т.п.).

9.6. Внутренняя планировка и расположение рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений.

9.7. По окончании рабочего дня помещения закрываются и опечатываются. Помещения с опечатанными входными дверьми сдаются под охрану (по установленному порядку) с указанием времени приема-сдачи с отметкой о включении и выключении охранной сигнализации в журнале учета.

9.8. Сдачу ключей и помещений под охрану, также получение ключей и вскрытие помещений производят сотрудники, работающие в этих помещениях, по утвержденному руководством Учреждения списку с образцами подписей этих сотрудников, который находится у охраны. Дубликаты ключей от входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством Учреждения.

9.9. Перед вскрытием помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно ставится в известность руководство и службу безопасности.

9.10. В случае утраты ключа от входной двери помещения немедленно ставится в известность ответственный по режиму.

9.11. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством Учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок спасения конфиденциальных документов и дальнейшего их хранения.

9.12. Рекомендуется не использовать в помещении, где размещены СКЗИ, радиотелефоны и другую радиоаппаратуру.

9.13. Устанавливаемый руководством Учреждения порядок охраны помещений, в которых расположены СКЗИ, должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны с отражением в журнале проверок, находящимся у ответственного по режиму.

Приложение № 3
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 26 ос

Инструкция пользователю СКЗИ

1. Общие положения

1.1. Средства криптографической защиты информации (далее – СКЗИ) предназначены для обеспечения безопасности хранения, обработки и передачи по каналам связи информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.

1.2. Пользователи обязаны выполнять указания ответственного пользователя (администратора) СКЗИ по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

1.3. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения и ознакомления с настоящей инструкцией. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный пользователь СКЗИ.

1.4. Изготовление ключевых документов осуществляется ответственным пользователем СКЗИ с применением штатных СКЗИ (если такая возможность предусмотрена эксплуатационной и технической документацией СКЗИ).

1.5. Ключевые документы, СКЗИ с введёнными криптографическими ключами относятся к материальным носителям, содержащие конфиденциальную информацию. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с конфиденциальной информацией в Учреждении.

1.6. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учёту в Журнале поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним, ключевых документов.

1.7. Все экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы должны быть выданы под расписку в соответствующем журнале учета пользователей СКЗИ, несущих персональную ответственность за их сохранность.

1.8. Передача экземпляров СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующем журнале.

1.9. Пользователи СКЗИ хранят установочные пакеты СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в шкафах (ящиках, сейфах) индивидуального пользования, в условиях,

исключающих бесконтрольный доступ к ним, а также и непреднамеренное уничтожение.

1.10. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется создать их резервные копии. Копии должны быть соответствующим образом маркированы и могут использоваться и храниться так же, как и оригиналы.

1.11. Криптографические ключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно изъять и при доказательстве компрометации надлежащим образом уничтожить.

1.12. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов и ключевых носителей.

1.13. Средства вычислительной техники, на которых осуществляется штатное функционирование 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.

2. Обязанности пользователей

2.1. Пользователи СКЗИ **ОБЯЗАНЫ**:

– не разглашать конфиденциальную информацию, к которой они допущены, рубежи её защиты, в том числе сведения о криптоключах;

– соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

– сообщать ответственному пользователю СКЗИ о ставших им известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним;

– при отстранении, увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;

– немедленной уведомлять ответственного пользователя 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.

2.2. Пользователям **ЗАПРЕЩАЕТСЯ**:

– осуществлять несанкционированное копирование ключевых документов;

– осуществлять несанкционированный вынос ключевых носителей за пределы контролируемой зоны;

– хранить ключевые документы и ключевые носители вне специально выделенных хранилищ и помещений;

– вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– изменять настройки, установленные программой установки СКЗИ или администратором информационной безопасности;

– осуществлять несанкционированное вскрытие системных блоков ПЭВМ, подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в комплектации.

Приложение № 4
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 26 ос

Типовая форма

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

Начат_____
Окончен_____

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, документации СКЗИ, серий ключевых документов	Номера экземпляров СКЗИ, экземпляров ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		Отметка о возврате		Дата ввода в действие	Дата вывода из действия	**Отметка об уничтожении СКЗИ, ключевых документов**		**Примечание**
				От кого получены или Ф.И.О. сотрудника, изготовившего ключевые документы	Дата получения или дата изготовления ключевых документов и расписка	Кому разосланы (переданы)	Дата и номер подтверждения или расписка в получении	Дата возврата, номер документа	Дата и номер подтверждения или расписка в получении			Дата уничтожения	Номер акта или расписка об уничтожении	
1.														
2.														
3.														
4.														
5.														
6.														
7.														
8.														
9.														
10.														
11.														
12.														
13.														

Приложение № 5
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 26 ос

Типовая форма

Журнал технический (аппаратный) учета пользователей СКЗИ

Начат_____
Окончен_____

№ п/п	Должность	ФИО	Тип СКЗИ	Серийный номер СКЗИ	Тип ключа	номер ключа	Место применения	Примечание
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								

Приложение № 6
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 26 ос

Типовая форма

Журнал технический (аппаратный) пользователя СКЗИ

Начат_____
Окончен_____

N п/п	Дата	Тип и серийные номера СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									
10.									
11.									
12.									
13.									

Приложение № 7
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 26 ос

Инструкция
по восстановлению связи в случае компрометации действующих ключей к СКЗИ

1. Под компрометацией индивидуального ключа понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность конфиденциальной информации. К событиям, связанным с компрометацией действующих криптографических ключей, относится:

– утрата (в том числе хищение) ключевых дискет (флэш - накопителей) с последующим их обнаружением;

– увольнение сотрудников, имевших доступ к ключевой информации;

– передача ключевой информации по линии связи в открытом виде (если это не предусмотрено правилами пользования);

– нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;

– возникновение подозрений на утечку информации или ее искажение;

– не расшифровывание входящих или исходящих сообщений;

– отрицательный результат при проверке электронной подписи документа;

– нарушение целостности упаковки ключевых дискет (флэш - накопителей) и (или) печати на сейфе, где хранились ключевые дискеты (флэш - накопители);

– несанкционированное копирование ключевых дискет (флэш - накопителей);

– случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе, случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий).

Первые пять событий должны трактоваться как безусловная компрометация действующих ключей; при наличии остальных событий требуется специальное расследование в каждом конкретном случае.

2. При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за эксплуатацию СКЗИ.

3. Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией во главе с ответственным за эксплуатацию СКЗИ.

Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих ключей.

При установлении факта компрометации действующих ключей, скомпрометированные секретные ключи шифрования и подписи уничтожаются.

4. Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается к ответственному за эксплуатацию СКЗИ с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования осуществляется тем же порядком, как и при плановой смене ключей.

ЛИСТ ОЗНАКОМЛЕНИЯ
с приказом ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина»
(с.Казанское)

«Об организации применения
средств криптографической защиты информации»

от__________________ №______

ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина» (с.Казанское)

№ п/п	Ф.И.О.	Должность	Подпись	Дата

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина» (с.Казанское)

«Об организации применения средств криптографической защиты информации»

от____________________ №_____

Филиал №1 Сладковская районная больница:

№ п/п	Ф.И.О.	Должность	Подпись	Дата