МИНИСТЕРСТВО ПО ИНФОРМАТИЗАЦИИ, СВЯЗИ И ВОПРОСАМ ОТКРЫТОГО УПРАВЛЕНИЯ ТУЛЬСКОЙ ОБЛАСТИ

ПРИКАЗ

07.05.2018 № 57-осн

Об утверждении Инструкции по порядку использования и организации работы со средствами криптографической защиты информации в региональных информационных системах Тульской области

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ – 2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66, Инструкцией по 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 Федеральным агентством правительственной связи и информации при президенте Российской Федерации от 13.06.2001 № 152, приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава 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»,

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по порядку использования и организации работы со средствами криптографической защиты информации в региональных информационных системах Тульской области (приложение).

2. Признать утратившим силу приказ министерства по информатизации, связи и вопросам открытого управления Тульской области

от 20.02.2017 № 17-осн «Об утверждении Инструкции по порядку использования и организации работы со средствами криптографической защиты информации в министерстве информатизации, связи и вопросам открытого управления Тульской области».

3. Приказ вступает в силу со дня его подписания.

Министр по информатизации, связи и вопросам открытого управления Тульской области **Я. Ю. Раков**

Приложение к приказу
от «____» _____20___г. № _____

ИНСТРУКЦИЯ
по порядку использования и организации работы со средствами криптографической защиты информации в региональных информационных системах Тульской области

В настоящей Инструкции используется следующие термины и определения:

Администратор безопасности (АБ) – лицо, ответственное за защиту информации в информационной системе и осуществляющее мероприятия по обеспечению безопасности информации, обрабатываемой в информационной системе.

АБ должен обладать достаточными навыками для осуществления мероприятий по обеспечению безопасности информации, в том числе с использованием криптографических средств защиты информации.

АБ назначается из числа сотрудников организации, имеющей подключение к региональным информационным системам Тульской области (далее – РИС ТО), либо из числа сотрудников организации, лицензиата Федеральной службы безопасности Российской Федерации, на основании заключенных договоров.

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, а также по предотвращению или существенному затруднению несанкционированного к ней доступа.

Криптографическая (шифровальная защита) – защита информации при помощи алгоритмов криптографического преобразования от ее модификации и от несанкционированного доступа к ней посторонних лиц.

Конфиденциальность – состояние защищенности информации, при котором обеспечивается сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Компрометация ключа – хищение, утрата, разглашение, несанкционированное копирование и другие инциденты безопасности, в результате которых возникают сомнения в сохранении тайны ключа и возможности обеспечения с его помощью защиты информации.

Ключевой документ (криптоключ) – сохраняемая в тайне, закрытая информация, используемая криптографичеким алгоритмом при шифровании/расшифровании сообщений, постановке и проверке электронной подписи, вычислении кодов аутентичности.

Криптосредство (СКЗИ) – шифровальное (криптографическое) средство, предназначенное для защиты информации.

Шифровальные (криптографические) средства:

а) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие 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) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

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

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

Машинный носитель информации (далее – МНИ) – материальный носитель, предназначенный для фиксации, хранения, накопления, преобразования и передачи информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами. В РИС ТО допускается использование только учтенных МНИ в соответствии с требованиями Инструкции по применению машинных носителей информации в органах исполнительной власти Тульской области, подразделениях аппарата правительства Тульской области и подведомственных им учреждениях.

Несанкционированный доступ (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств РИС ТО.

Обработка информации – любое действие (операция) или совокупность действий (операций) с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Ответственный за обеспечение защиты информации – сотрудник, на которого приказом руководителя организации возложена персональная ответственность за обеспечение защиты информации в данной организации.

Пользователь криптосредств – субъект, наделенный правом применения средства криптографической защиты для выполнения возложенных обязанностей.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет порядок использования и организации работы со средствами криптографической защиты информации (далее – СКЗИ) в РИС ТО.

1.2. Действие настоящей инструкции распространяется на организации, осуществляющие эксплуатацию РИС ТО, в том числе:

правительство Тульской области, подразделения аппарата правительства Тульской области, органы исполнительной власти Тульской области (далее – ОИВ ТО) и подведомственные им государственные учреждения (далее – ПУ ТО);

администрации муниципальных образований Тульской области и подведомственные им учреждения;

уполномоченные в Тульской области и аппарат уполномоченных в Тульской области.

1.3. В РИС ТО должны применяться только сертифицированные по требованиям Федеральной службы безопасности Российской Федерации СКЗИ, класс которых определяется на основании Модели угроз безопасности информации при ее обработке в РИС ТО. К таким СКЗИ в том числе относятся:

программные комплексы и программно-аппаратные комплексы ViPNet – применяется для обеспечения защиты каналов связи РИС ТО;

КриптоПро CSP и ViPNet CSP – применяются в РИС ТО как средства электронной подписи, а также средства защиты каналов связи;

Континент АП – применяется для обеспечения и защиты каналов связи при информационном обмене с Управления федерального казначейства по Тульской области.

1.4. Работы по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, работы, по оказанию услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд) в РИС ТО должны выполняться с привлечением лицензиата Федеральной службы безопасности Российской Федерации.

1.5. Работы по монтажу, установке (инсталляции), наладке, обслуживанию, учету СКЗИ в РИС ТО выполняются сотрудниками организации, в которой эксплуатируются СКЗИ, самостоятельно, либо организацией, лицензиатом Федеральной службы безопасности Российской Федерации на основании заключенного договора по согласованию с министерством информатизации, связи и вопросам открытого управления Тульской области.

1.6. ГАУ ТО «ЦИТ» является органом криптографической защиты информации в ОИВ ТО и осуществляет мероприятия по организации и обеспечению эксплуатации СКЗИ в РИС ТО.

1.7. В организациях, осуществляющих эксплуатацию РИС ТО, орган криптографической защиты информации создается из числа собственных сотрудников организации, либо из числа сотрудников организации, лицензиата Федеральной службы безопасности Российской Федерации на основании заключенного договора.

1.8. Порядок выпуска, приостановления и отзыва сертификатов ключей проверки ЭП, эксплуатируемых в РИС ТО, устанавливается регламентами аккредитованных удостоверяющих центров.

1.9. В организациях, осуществляющих эксплуатацию РИС ТО, должны быть назначены администраторы безопасности, осуществляющие мероприятия контроля эксплуатации СКЗИ.

1.10. В ОИВ ТО администраторы безопасности назначаются из числа сотрудников ГАУ ТО «ЦИТ», в иных организациях, осуществляющих эксплуатацию РИС ТО, администраторами безопасности назначаются собственные сотрудники, либо сотрудники организации, лицензиата Федеральной службы безопасности Российской Федерации на основании заключенного договора.

2. ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ, ВЫПОЛНЯЕМЫХ ПРИ РАБОТЕ С СКЗИ В РИС ТО

2.1. Установка и ввод в эксплуатацию СКЗИ должны осуществляться в соответствии с требованиями эксплуатационной и технической документации СКЗИ, с составлением актов, в которых указываются тип и номер используемых СКЗИ, номера аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства и результаты проверки функционирования СКЗИ (Приложение № 1).

2.2. Непосредственно к работе с СКЗИ допускаются пользователи организации, осуществляющей эксплуатацию РИС ТО, согласно утверждаемому руководителем организации перечню лиц и только после соответствующего обучения правилам работы с СКЗИ, в том числе ознакомления с настоящей инструкцией, а также проверки их готовности к самостоятельному использованию СКЗИ в формате теста.

2.3. Обучение и тестирование пользователей должно проводиться АБ. Заключение о готовности пользователя к работе с СКЗИ может быть включено в Акт по установке и вводу в эксплуатацию СКЗИ, либо должно оформляться отдельным документом.

2.4. Перечень лиц, допущенных к работе с СКЗИ в организации, осуществляющей эксплуатацию РИС ТО, актуализируется на постоянной основе по мере необходимости.

2.5. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету.

2.6. Входные двери помещений, где установлены СКЗИ или хранятся ключевые документы к ним, должны быть оснащены замками, обеспечивающими надежное закрытие таких помещений в нерабочее время, а также приспособлением для опечатывания или соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

2.7. Должно быть обеспечено постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений либо включение технических устройств, сигнализирующих о несанкционированном вскрытии помещений.

2.8. Руководителями организаций, осуществляющих эксплуатацию РИС ТО, должен быть утвержден перечень лиц, имеющих право доступа в помещения, где размещены используемые средства криптографической защиты информации, хранятся средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации.

2.9. В организациях, осуществляющих эксплуатацию РИС ТО, должен осуществляться контроль за соблюдением требований к порядку использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ и настоящей Инструкцией.

2.10. Должны осуществляться расследования и оформляться заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации в РИС ТО; разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

2.11. Администраторами безопасности должны обеспечиваться:

соблюдение режима 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 СКЗИ и ключевых документов к ним;

надежное хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации;

своевременное выявление попыток посторонних лиц получить сведения о РИС ТО, об используемых СКЗИ или ключевых документах к ним;

немедленное принятие мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п. В случае выявления таких фактов АБ обязан уведомить руководителя организации, осуществляющей эксплуатацию РИС ТО, а также составить акт об инциденте информационной безопасности.

2.12. Пользователи СКЗИ обязаны:

не разглашать конфиденциальную информацию, к которой они допущены, в том числе сведения о СКЗИ, ключевую информацию к ним и сведения о других мерах защиты РИС ТО;

соблюдать требования по обеспечению безопасности РИС ТО, требования к обеспечению безопасности СКЗИ и ключевой информации к ним;

сообщать АБ о полученных СКЗИ, ключевых носителях и ключевой информации для учета в соответствующих журналах;

незамедлительно сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ в РИС ТО и ключевых документах к ним;

немедленно уведомлять руководителя своего структурного подразделения организации, осуществляющей эксплуатацию РИС ТО, а также АБ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к несанкционированному доступу к РИС ТО;

в нерабочее время хранить ключевую информацию (ключевые носители) в индивидуальных хранилищах, запираемых на замок (шкафах, ящиках, сейфах). При отсутствии у пользователя личного хранилища необходимо сдавать ключевые носители на хранение лицу, назначенному ответственным за хранение съемных носителей из числа сотрудников приказом руководителя организации, осуществляющей эксплуатацию РИС ТО, в опечатанном конверте (пенале) с фиксацией факта сдачи/выдачи в «Журнале выдачи съемных носителей информации»;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевую информацию (ключевые носители) АБ под запись в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов» (Приложение 2) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

2.13. Пользователям СКЗИ запрещается:

разглашать ключевую информацию и самостоятельно передавать другим пользователям СКЗИ, носители ключевой информации и пароли;

самостоятельно изменять настройки СКЗИ;

оставлять без контроля ключевые носители информации;

применять скомпрометированные ключи и пароли;

осуществлять несанкционированное копирование ключевой информации;

записывать на ключевые носители какую-либо информацию, не предусмотренную правилами пользования на СКЗИ;

допускать снятие копий с ключевой информации, вывод ключевой информации на дисплей (монитор) автоматизированного рабочего места (далее – АРМ) или принтер, запись на ключевой носитель посторонней информации, установку ключевой информации на АРМ других пользователей.

2.14. Пользователи несут персональную ответственность за сохранность, неразглашение и нераспространение ключей и ключевой информации.

3. ПОРЯДОК ОБРАЩЕНИЯ С СКЗИ И КРИПТОКЛЮЧАМИ. МЕРОПРИЯТИЯ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

3.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов». 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 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 поступившие в организацию экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевой информации должны выдаваться пользователям СКЗИ под расписку в соответствующем «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов».

3.3. Если в эксплуатационной и технической документации к СКЗИ предусмотрено применение разовых ключевых носителей или ключевую информацию вводят и хранят (весь срок ее действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в Аппаратном журнале (Приложение № 3). В Аппаратном журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях Аппаратный журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).

3.4. Хранение ключевой информации пользователей должно осуществляться на машинных отчуждаемых МНИ. Допускается размещение нескольких криптоключей пользователя на одном носителе при условии выполнения требований п. 2.13. Допускается хранение криптоключей в памяти АРМ пользователя, если это предусмотрено эксплуатационной документацией на СКЗИ.

3.5. В случае необходимости использования АРМ, работа которого будет осуществляться в многопользовательском (посменном) режиме, СКЗИ для такого АРМ должны быть закреплены за руководящим должностным лицом, ответственным за обеспечение защиты информации. У пользователей, работающих с данным АРМ, должны быть индивидуальные учетные записи для авторизации на АРМ, а также отсутствовать права на изменение настроек СКЗИ. Запрещается хранение ключевой информации пользователей в памяти таких АРМ.

3.6. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) администратором безопасности под расписку в соответствующих журналах поэкземплярного учета.

3.7. СКЗИ, непригодные для дальнейшего использования или с окончившимся сроком действия, должны уничтожаться. Уничтожение ключевой информации может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или с применением специализированных утилит, входящих в состав СКЗИ. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожаются путем сжигания или с помощью бумагорезательных машин.

3.8. Уничтожение ключевых документов должно осуществляться в сроки, указанные в правилах пользования, установленных производителем соответствующих СКЗИ, но не позднее 10 суток после вывода их из действия (окончания срока действия). Отметки о деинсталляции СКЗИ, уничтожении эксплуатационной, технической документации, правил пользования, ключевых документов оформляются в соответствующих журналах учета.

3.9. Уничтожение большого объема ключевых документов может быть оформлено актом (Приложение № 4). Уничтожение по акту производит комиссия в количестве не менее двух человек, состоящая из АБ и пользователей СКЗИ. 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, инсталлирующих СКЗИ 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 Журнале поэкземплярного учета.

3.10. Передача по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности с использованием СКЗИ защищаемой информации, может производиться только в зашифрованном виде.

3.11. Запрещена передача ключевой информации по каналам связи, за исключением специально организованных систем, правилами пользования которыми предусматривается управление ключевой системой с использованием технических каналов связи.

Под компрометацией криптографического ключа понимаются:

утеря (хищение) носителей ключевой информации, в том числе с последующим их обнаружением;

увольнение сотрудника, имевшего доступ к ключевой информации;

передача закрытых ключей по линиям связи;

нарушение правил хранения или уничтожения криптоключа;

несанкционированное или безучётное копирование ключевой информации;

нарушение целостности печати на сейфе с ключевыми носителями;

вскрытие фактов утечки (искажения или изменения) передаваемой информации;

все случаи, когда нельзя достоверно установить, что произошло с носителем ключевой информации.

3.12. При наступлении любого из перечисленных случаев или иных событий, приводящих к компрометации криптоключей, пользователь должен прекратить использование СКЗИ и немедленно сообщить о произошедшем администратору безопасности.

3.13. Криптоключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно вывести из эксплуатации, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

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

3.15. В каждом случае по факту (или при предполагаемой) компрометации ключевых документов специально назначенной комиссией проводится служебное расследование. Результатом расследования является квалификация или не квалификация данного события как компрометация.

3.16. В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет администратор безопасности или орган

криптографической защиты совместно с сотрудниками организации, осуществляющей эксплуатацию РИС ТО пользователь которого эксплуатировал соответствующий криптоключ.

3.17. О факте компрометации ключевой информации пользователями совместно с администратором безопасности СКЗИ производится информирование организации, выпустившей указанную ключевую информацию.

3.18. Выведенные из эксплуатации скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в «Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов».

Приложение № 1
к инструкции по порядку использования и организации работы со средствами криптографической защиты информации в региональных информационных системах Тульской области

АКТ № _____
ВЫПОЛНЕНИЯ РАБОТ (ОКАЗАНИЯ УСЛУГ) ПО УСТАНОВКЕ И ВВОДУ В ЭКСПЛУАТАЦИЮ СКЗИ

г. Тула «____»_____20__ г.

Мы, нижеподписавшиеся,_____

_____
(должность, ФИО пользователя, наименование и адрес учреждения)

далее Пользователь и _____

_____
(сотрудник, выполнивший установку и ввод в эксплуатацию СКЗИ)

составили настоящий АКТ о том, что выполнены следующие работы (оказаны услуги):

1. На рабочее место Пользователя №_____ в помещении № _____ установлено СКЗИ_____ в соответствии с формуляром _____ (далее – СКЗИ). Настройки СКЗИ выполнены в соответствии с эксплуатационно-технической документацией на СКЗИ и правами пользователя.

2. На рабочее место Пользователя установлена: справочно-ключевая информация abn_____.dst.

3. Проведена проверка целостности программного обеспечения и работоспособности СКЗИ в соответствии с эксплуатационно-технической документацией на СКЗИ. Установленное программное обеспечение функционирует в штатном режиме.

4. Пользователь ознакомлен с Приказом ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», руководством пользователя СКЗИ и обучен работе с СКЗИ.

5. СКЗИ введено в эксплуатацию, требования к размещению выполняются согласно _____.

6. Рабочее место Пользователя (ПЭВМ Пользователя) с установленным СКЗИ опломбированы _____. Замечаний по работоспособности ПЭВМ нет.

Сотрудник, выполнивший установку
и ввод в эксплуатацию СКЗИ
_____/_____/
«____»_____20__ г.

Пользователь СКЗИ
_____/_____/
«____»_____20__ г.

Приложение № 2
к инструкции по порядку использования и организации
работы со средствами криптографической защиты
информации в региональных информационных системах
Тульской области

ЖУРНАЛ ПОЭКЗЕМПЛЯРНОГО УЧЕТА КРИПТОСРЕДСТВ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

№ п/п.	Наименование криптосредства, эксплуатационной и технической документации к ним, Вид носителя ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф. И. О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены крипто-средства	Дата изъятия (уничтожения)	Ф. И. О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 3
к инструкции по порядку использования и организации
работы со средствами криптографической защиты
информации в региональных информационных системах
Тульской области

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ) ЖУРНАЛ

№ п/п	Дата	Тип и регистрационные номера используемых криптосредств	Записи по обслуживанию криптосредств	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны криптосредств, в которую введены криптоключи	Дата	Подпись пользователя криптосредств	
1	2	3	4	5	6	7	8	9	10

Приложение № 4
к инструкции по порядку использования и организации
работы со средствами криптографической защиты
информации в региональных информационных системах
Тульской области

АКТ НА УНИЧТОЖЕНИЕ КРИПТОСРЕДСТВ

№ _____

г._____ «____» _____ 20 __г.

Комиссия в составе _____
(должности, фамилии, инициалы членов комиссии)

на основании _____подготовила к уничтожению
(основание для уничтожения)

_____
(наименование, тип криптосредства, их номера, номера серий, комплектов, экземпляров)

в количестве _____экземпляров.
(цифрами и прописью)

Всего подлежит уничтожению _____наименований экземпляров.
(цифрами и прописью)

Председатель комиссии:

_____ _____
(подпись) (фамилия)

Члены комиссии:

_____ _____
(подпись) (фамилия)

_____ _____
(подпись) (фамилия)

Перечисленные криптосредства (программное обеспечение криптосредств, ключевая информация, содержащиеся на носителях информации, аппаратные, программно-аппаратные криптосредства и т.д.) после утверждения акта полностью уничтожены путем

_____
(переформатирования, удаления программного обеспечения криптосредств, физического уничтожения носителей

_____ с использованием программы_____,
многократного использования) (название программы)

входящей в комплект криптосредства «_____» _____ 20 ____ г.
Председатель комиссии:

_____ _____
(подпись) (фамилия)

Члены комиссии:

_____ _____
(подпись) (фамилия)

_____ _____
(подпись) (фамилия)

Отметки об уничтожении криптосредств (программного обеспечения криптосредств, ключевой информации, содержащихся на магнитных носителях информации, аппаратных, программно-аппаратных криптосредств), перечисленных в акте, в журнале

_____ произвел
(наименование журнала учета, его №)

_____ «___» _____ 20 __ г.
(подпись, фамилия, инициалы)