УТВЕРЖДАЮ

Директор ООО «ЦИБ-Сервис»

М. М. Шушпанов

м.п.

13 апреля 2018 г.

ИНСТРУКЦИЯ

по обращению с сертифицированными ФСБ (ФАПСИ) шифровальными средствами (СКЗИ) в ООО «ЦИБ-Сервис»

№ 11

2018

1. Общие положения

Настоящая Инструкция определяет порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФСБ средств криптографической защиты (шифровальных средств) (далее – СКЗИ) подлежащей обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, в ООО «ЦИБ-Сервис».

Данным порядком рекомендуется руководствоваться также при организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ не подлежащей обязательной защите информации конфиденциального характера, доступ к которой ограничивается по решению руководства ООО «ЦИБ-Сервис».

2. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера

Должностные лица, допущенные к работам с СКЗИ, несут персональную ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящей Инструкции.

При этом должностные лица, допущенные к работам с СКЗИ, должны обеспечивать комплексность защиты информации конфиденциального характера, в том числе посредством применения некриптографических средств защиты.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации конфиденциального характера в ООО «ЦИБ-Сервис» назначаются ответственные за защиту информации на объекте информатизации и ответственный за эксплуатацию объекта информатизации (далее – Ответственные за СКЗИ).

Указанные сотрудники осуществляют:

– разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

– обучение лиц, использующих СКЗИ, правилам работы с ними;

– поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

– учет обслуживаемых обладателей информации конфиденциального характера, а также физических лиц, непосредственно допущенных к работе с СКЗИ (далее – пользователей СКЗИ);

– контроль соблюдения условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФСБ и настоящей Инструкцией;

– расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации конфиденциального характера; разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

Инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой с использованием СКЗИ информации конфиденциального характера подготавливаются согласно эксплуатационной и технической документации на соответствующие сети связи, автоматизированные и информационные системы, в которых передается, обрабатывается или хранится информация конфиденциального характера, с учетом используемых СКЗИ и положений настоящей Инструкции.

К выполнению обязанностей сотрудников, ответственных за СКЗИ, допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты информации конфиденциального характера с использованием конкретного вида (типа) СКЗИ.

Лиц, выполняющих функции ответственных за СКЗИ, следует ознакомить с настоящей Инструкцией под расписку.

При определении обязанностей ответственных за СКЗИ должно учитываться, что безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера обеспечивается:

– соблюдением сотрудниками 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 документах к ним;

– точным выполнением сотрудниками требований к обеспечению безопасности информации конфиденциального характера;

– надежным хранением сотрудниками СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей информации конфиденциального характера;

– своевременным выявлением сотрудниками попыток посторонних лиц получить сведения о защищаемой информации конфиденциального характера, об используемых СКЗИ или ключевых документах к ним;

– немедленным принятием сотрудниками 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, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

Обучение и повышение квалификации сотрудников осуществляют организации, имеющие лицензию на ведение образовательной деятельности по соответствующим программам.

Обязанности между сотрудниками, ответственными за СКЗИ, должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевой документации и документов, а также за порученные участки работы.

Должностные лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому руководителем ООО «ЦИБ-Сервис».

Пользователи СКЗИ обязаны:

– не разглашать информацию конфиденциального характера, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;

– соблюдать требования к обеспечению безопасности информации конфиденциального характера с использованием СКЗИ;

– сообщать ответственным за СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– немедленно уведомлять ответственного по защите информации на объекте информатизации 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.

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники, ответственные за СКЗИ. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное сотрудниками, ответственными за СКЗИ.

3. Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей.

Под компрометацией криптоключей в настоящей Инструкции понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

В ООО «ЦИБ-Сервис» ключевые документы, СКЗИ с введенными криптоключами относятся к материальным носителям, содержащим информацию конфиденциального характера. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с информацией конфиденциального характера в ООО «ЦИБ-Сервис».

При необходимости передачи по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера, соответствующие указания необходимо передавать, только применяя СКЗИ. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

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.

Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (приложения 1, 2 к Инструкции) ведут сотрудники, ответственные за СКЗИ.

Все полученные обладателем информации конфиденциального характера 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.

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 (приложение 2 к Инструкции), ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический

(аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками, ответственными за СКЗИ под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована.

Обладатель информации характера конфиденциального характера с согласия ответственных за СКЗИ может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета.

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

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

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные 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.

СКЗИ и ключевые документы могут доставляться со специально выделенными нарочными из числа сотрудников пользователей СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

Для пересылки СКЗИ ключевые документы должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают пользователя СКЗИ, для которых эти упаковки предназначены. На упаковках для пользователя СКЗИ делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Оформленную таким образом упаковку, при предъявлении дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

Полученные упаковки вскрывают только лично пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать – их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает в Организацию, осуществившую отправку. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от Организации, осуществившей отправку, применять не разрешается.

При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено в соответствии с порядком, указанным в сопроводительном письме. Ответственный за отправку обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано только после подтверждений от всех заинтересованных пользователей СКЗИ о получении ими очередных ключевых документов.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в организацию, осуществившую их передачу, либо должны быть уничтожены на месте.

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).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, оптических дисков, 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 СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают 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 СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

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

СКЗИ уничтожают (утилизируют) в соответствии с требованиями Положения ПКЗ-2005 по решению обладателя информации конфиденциального характера, владеющей СКЗИ.

Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее

с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации на соответствующие СКЗИ. 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 СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

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

Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственными за СКЗИ под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственных за СКЗИ для списания уничтоженных документов. Не реже одного раза в год пользователи СКЗИ должны предоставлять в ООО «Сертум-Про» письменные отчеты об уничтоженных ключевых документах.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников ООО «ЦИБ-Сервис». 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 соответствующих журналах поэкземплярного учета.

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 СКЗИ. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственных за СКЗИ, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации конфиденциального характера, пользователи СКЗИ обязаны сообщать ответственным за СКЗИ ООО «ЦИБ-Сервис». Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации информации конфиденциального характера, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной информации конфиденциального характера.

Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается сотрудниками ответственными за СКЗИ ООО «ЦИБ-Сервис».

4. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее спецпомещения), должны обеспечивать сохранность информации конфиденциального характера (требования к обеспечению сохранности информации конфиденциального характера указаны в «Приказе об организации защиты информации на объекте информатизации» и «Инструкции по работе с информацией конфиденциального характера для пользователей объекта информатизации ООО «ЦИБ-Сервис»»), СКЗИ, ключевых документов.

При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

Перечисленные в настоящей Инструкции требования к спецпомещениям могут не предъявляться, если это предусмотрено правилами пользования СКЗИ, согласованными с ФСБ.

Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Размещение, специальное оборудование, охрана и организация режима в спецпомещениях ООО «ЦИБ-Сервис» должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Режим охраны спецпомещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается внутренним регламентом действий по обеспечению безопасности в режимных помещениях. Установленный режим охраны предусматривает периодический контроль за состоянием технических средств охраны.

В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя информации конфиденциального характера и руководителю ООО «ЦИБ-Сервис». Сотрудники, ответственные за СКЗИ, должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации конфиденциального характера и к замене скомпрометированных криптоключей.

5. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера

Государственный контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера осуществляют федеральные органы безопасности. В ходе государственного контроля изучаются и оцениваются:

– организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера;

– достигнутый уровень криптографической защиты информации конфиденциального характера;

– условия использования СКЗИ.

Сотрудники, ответственные за СКЗИ ООО «ЦИБ-Сервис», обязаны контролировать выполнение обладателями информации конфиденциального характера данных им указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера, а также соблюдение такими обладателями условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФСБ и настоящей Инструкцией.

В целях координации государственного контроля федеральные органы службы безопасности могут планировать и проводить проверки совместно с сотрудниками ООО «ЦИБ-Сервис».

По результатам государственного контроля составляется акт (справка). С актом проверки (справкой) под расписку должен быть ознакомлен руководитель ООО «ЦИБ-Сервис». Если в ходе проверки выявлены нарушения требований и условий лицензий и сертификатов ФСБ, то федеральные органы службы безопасности сообщают в Лицензионный и сертификационный центр ФСБ об этих нарушениях и принятых мерах.

Если в использовании СКЗИ обнаружены недостатки, то ООО «ЦИБ-Сервис», обладатели информации конфиденциального характера обязаны принять безотлагательные меры к устранению вскрытых проверкой недостатков и выполнению рекомендаций, изложенных в акте проверки. Сообщения о принятых мерах должны быть представлены в установленные проверяющими сроки. При необходимости может быть составлен план мероприятий, где предусматривается решение соответствующих вопросов.

Сотрудники, ответственные за СКЗИ, должны обобщать результаты всех видов контроля, анализировать причины выявленных недостатков, разрабатывать меры по их профилактике, контролировать выполнение рекомендаций, содержащихся в актах проверок.

Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка информации конфиденциального характера, безопасность которой обеспечивается с использованием СКЗИ, то ФСБ вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений.

Настоящая инструкция разработана на основании «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», приложение к приказу ФАПСИ от 13.06.2001 №152.

Разработал:

Руководитель отдела ОЗИК С. Н. Вихнер