Часто задаваемые вопросы по использованию средств шифрования в продукции Cisco, вопросы лицензирования, импорта и сертификации

(не является официальным документом, ответы на вопросы подготовлены на основании открытых материалов и опыта практической деятельности компании Cisco в Российской Федерации)

В1. Что такое шифровальные средства и их функция?

О1. Согласно Постановлению Правительства Российской Федерации от 29 декабря 2007 года № 957 «Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» к средствам шифрования относятся *аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при ее передаче по каналам связи и (или) при ее обработке и хранении*.

В2. В каком случае устройство или программа считаются шифровальным средством?

О2. Если устройство или программа могут выполнять криптографическое преобразование, они в любом случае считаются шифровальным средством, даже если это является неосновной или неиспользуемой функцией устройства или программы.

В3. Отличается ли обращение (ввоз, продажа, обслуживание, техническая поддержка и использование) шифровальных средств от обращения других устройств и программ?

О3. Да. Ввоз шифровальных средств на территорию России, их продажа и техническое обслуживание, а также использование в различных информационных системах законодательно регулируется.

В4. Какие виды законодательного регулирования деятельности с шифровальными средствами существуют в России?

О4. Федеральным законом «О лицензировании отдельных видов деятельности» от 8 августа 2001 года № 128-ФЗ и Постановлением Правительства Российской Федерации от 26 января 2006 года № 45 «Об организации лицензирования отдельных видов деятельности» определены следующие виды деятельности с шифровальными средствами, для осуществления которых необходимо получать лицензию:

- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

В5. Какой федеральный орган осуществляет лицензирование деятельности с шифровальными средствами?

О5. Постановлением Правительства Российской Федерации от 26 января 2006 года № 45 таким органом утверждена ФСБ России www.fsb.ru/fsb/supplement/contact/lsz.htm. Рекомендуем изучить документы:

- ПРИКАЗ ФСБ РФ от 16.03.2009 №105 "Об утверждении административного регламента Федеральной Службы Безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по техническому обслуживанию шифровальных (криптографических) средств" (Зарегистрировано в Минюсте РФ 14.04.2009 N 13753)
- ПРИКАЗ ФСБ РФ от 16.03.2009 №106 "Об утверждении административного регламента Федеральной Службы Безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по распространению шифровальных (криптографических) средств" (Зарегистрировано в Минюсте РФ 14.04.2009 N 13753)

В6. Как законодательно регулируется ввоз шифровальных средств в Россию?

О6. В соответствии с Указом Президента Российской Федерации от 03 апреля 1995 года № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», Постановлением Правительства Российской Федерации от 6 ноября 1992 г. № 854 «О лицензировании и квотировании экспорта и импорта товаров (работ, услуг) на территории Российской Федерации» *ввоз шифровальных средств осуществляется по лицензии, выданной Минпромторга России на основании разрешения ФСБ России*. На основании и в развитие данного Постановления изданы Приказ Федеральной таможенной службы (ранее ГТК России) от 19 марта 1996 года № 150 и Приказы Минпромторга России от 27 февраля 2009 года № 84 и от 24 июня 2008 года № 7.

В7.Должны ли компании, осуществляющие ввоз шифровальных средств, иметь лицензию ФСБ России на деятельность по распространению шифровальных (криптографических) средств?

О7. Отсутствие такой лицензии допускается только в случае, если компания ввозит шифровальные средства исключительно для собственных нужд без последующей продажи, а также в случае, если компания продает шифровальные средства, на которые не распространяется «Положение о лицензировании деятельности по распространению шифровальных средств» (см. п.1 Положения). В остальных случаях наличие лицензии обязательно.

В8.Каковы отличия лицензии, выдаваемой ФСБ России, от лицензии Минпромторга России?

О8. ФСБ России выдает лицензию на право заниматься определенным видом деятельности на 5 лет, включая лицензии на деятельность по распространению шифровальных средств и по техническому обслуживанию шифровальных средств, предоставление услуг в области шифрования и разработку и производство шифровальных средств, а также защищенных с использованием шифровальных средств информационных и телекоммуникационных систем.

Минпромторг России выдает лицензию на право ввоза шифровальных средств на территорию Российской Федерации на основании разрешения ФСБ.

В9. Распространяется ли законодательное регулирование на *все* шифровальные средства?

О9. Нет. В Постановлении Правительства Российской Федерации от 29 декабря 2007 года № 957 приведен перечень шифровальных средств, на которые не распространяется действие утвержденных им Положений:

- шифровальные (криптографические) средства, предназначенные для защиты информации, содержащей сведения, составляющие государственную тайну;
- шифровальные (криптографические) средства, являющихся компонентами доступных для продажи без ограничений посредством розничной торговли, либо сделок по почтовым запросам, либо электронных сделок, либо сделок по телефонным заказам программных операционных систем, криптографические возможности которых не могут быть изменены пользователями, которые разработаны для установки пользователем самостоятельно без дальнейшей существенной поддержки поставщиком и техническая документация (описание алгоритмов криптографических преобразований, протоколы взаимодействия, описание интерфейсов и т.д.) на которые является доступной, в том числе для проверки;
- персональные кредитные карточки со встроенной микроЭВМ, криптографические возможности которых не могут быть изменены пользователями;
- портативные или мобильные радиотелефоны гражданского назначения (в том числе предназначенные для использования в коммерческих гражданских системах сотовой радиосвязи), которые не способны к сквозному шифрованию;
- приемная и передающая аппаратура радиовещания, коммерческого телевидения или иной аппаратуры коммерческого типа для вещания на ограниченную аудиторию без шифрования цифрового сигнала, в которой шифрование ограничено функциями управления видео- или аудиоканалами;
- специально разработанные и применяемые только для банковских и финансовых операций шифровальные (криптографические) средства в составе терминалов единичной продажи (банкоматов), криптографические возможности которых не могут быть изменены пользователями;
- специально разработанные и применяемые только в составе контрольно-кассовых машин шифровальные (криптографические) средства защиты фискальной памяти;
- шифровальные (криптографические) средства независимо от их назначения, реализующих симметричные криптографические алгоритмы и обладающие максимальной длиной криптографического ключа менее 56 бит, а также реализующие асимметричные криптографические алгоритмы, основанные либо на разложении на множители целых чисел, либо на вычислении дискретных логарифмов в мультипликативной группе конечного поля, либо на дискретном логарифме в группе, отличной от названной, и обладающие максимальной длиной криптографического ключа 128 бит;
- беспроводное оборудование, осуществляющее шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя (за исключением оборудования, используемого на критически важных объектах);

- шифровальные (криптографические) средства, используемых для защиты технологических каналов информационно-телекоммуникационных систем и сетей, не относящихся к критически важным объектам.

В10. Все ли шифровальные средства производства Cisco попадают под законодательное регулирование обращения и использования шифровальных средств?

О10. Нет. Из законодательного регулирования обращения и использования исключены изделия любого производителя, в т.ч. Cisco, которые используют функцию шифрования только для защиты каналов удаленного управления и мониторинга или защиты беспроводного канала передачи данных с дальностью действия менее 400 метров.

В11. Как законодательно регулируется использование шифровальных средств для защиты информации?

О11. Существует большое количество нормативных документов об использовании средств защиты информации, включая шифровальные средства. В соответствии с положениями Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ эти документы можно разделить на следующие группы в зависимости от категории доступа к информации:

- информация, составляющая государственную тайну;
- информация, доступ к которой ограничен федеральными законами (конфиденциальная информация).

Использование шифровальных средств будет рассматриваться ниже в соответствии с этими группами.

В12. Какими документами определены перечни информации, содержащей сведения, составляющие государственную тайну, и конфиденциальной информации?

О12. Эти перечни утверждены следующими Указами Президента России:

- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 № 1203;
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188.

В13. Возможно ли использование шифровальных средств производства Cisco для защиты информации, содержащей сведения, составляющие государственную тайну?

О13. Нет. Применение шифровальных средств для защиты такой информации регулируется следующими документами:

- Закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне»;
- Постановление Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации»;
- Приказ ФСБ России от 13 ноября 1999 года № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»,

которыми определена обязательность использования сертифицированных шифровальных средств российского производства. Т. о. продукция компании Cisco, не

являясь российской, не может быть использована для защиты информации, содержащей сведения, составляющие государственную тайну.

В14. Какие требования существуют к шифровальным средствам, обеспечивающим защиту конфиденциальной информации.

О14. В следующих нормативных документах:

- Указ Президента Российской Федерации от 17 марта 2008 года № 351«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденные приказом Гостехкомиссии России от 30 августа 2002 года № 282 (при проведении работ по защите негосударственных информационных ресурсов, составляющих коммерческую тайну, банковскую тайну и т.д., требования документа носят рекомендательный характер);
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144; http://www.fsb.ru/fsb/science/single.html!id%3D10434826%40fsbResearchart.html
- Стандарт Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности в организациях банковской системы Российской Федерации, общие положения»

требуется использовать для защиты конфиденциальной информации сертифицированные средства защиты, в т. ч. сертифицированные шифровальные средства.

В15. На соответствие каким требованиям должны сертифицироваться шифровальные средства?

О15. Шифровальные средства сертифицируются на соответствие требованиям российских стандартов ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 в системе сертификации РОСС RU.0001.030001.

В16. Для защиты какой конфиденциальной информации необходимо использовать шифровальные средства, имеющие сертификаты ФСБ России?

О16. В отношении конфиденциальной информации, определенной соответствующим перечнем (В-О12), в настоящее время существуют законодательные требования об обязательном использовании сертифицированных шифровальных средств для персональных данных, служебной тайны, к которой относится служебная информация государственных и муниципальных органов власти, и банковской информации (В-О14).

В17. В каких случаях разрешается использовать шифровальные средства, не имеющие сертификатов ФСБ России?

О17. В том случае, если защищаемая информация не содержит сведений, составляющих государственную тайну, и не является конфиденциальной информаций, входящей в соответствующие перечни.

В18. Требуется ли получать лицензию ФСБ, если в организации используются средства шифрования, не имеющие сертификатов ФСБ России?

О18. Да, даже при использовании средств шифрования, не имеющих сертификатов ФСБ России, техническое обслуживание этих средств должно осуществляться организацией, имеющей лицензию ФСБ на техническое обслуживание средств шифрования. Существуют два варианта, опробованных на практике: либо организация, эксплуатирующая несертифицированные средства шифрования, получает лицензию ФСБ на техническое обслуживание средств шифрования, либо эта организация заключает договор на обслуживание средств шифрования с подрядчиком, имеющим такую лицензию. Например, все основные партнеры Cisco располагают лицензией ФСБ на техническое обслуживание средств шифрования.

В19. В каких устройствах Cisco имеются средства шифрования, как их отличить от других?

О19. Средства шифрования присутствуют во всех аппаратных, программных и аппаратно-программных средствах Cisco, в Part Number (номер по каталогу) которых присутствуют коды K8, K9. Также существуют и аппаратные ускорители шифрования, не содержащие кодов K8/K9 в номере по каталогу, например AIM-VPN.

В20. Одинаковы ли законодательные требования по обращению и использованию с шифровальными средствами для всех компаний-разработчиков?

О20. Да, *с одним исключением*: для защиты информации, содержащей сведения, составляющие государственную тайну, могут использоваться только шифровальные средства на основе российских криптографических алгоритмов, сертифицированные ФСБ России.

В21. Один западный вендор уверяет нас, что в его продукцию встроена российская криптография и для ее ввоза не требуется разрешение ФСБ России и лицензия Минпромторга России. Это так?

О21. Для перемещения любого шифровального средства через таможенную границу всегда требуется оформление разрешения Центра ЛСЗ (при необходимости требуется также лицензия Минпромторга России). Примечание: такие же документы требуются и для экспорта шифровальных средств из России. www.fsb.ru/fsb/supplement/contact/lsz.htm

В22. Если я предоставляю доступ к своей корпоративной сети своим клиентам или партнерам с помощью VPN-решений, то должен ли я получать лицензию на данный вид деятельности? Важно ли, что я оказываю такую услугу на безвозмездной основе?

О22. В связи с тем, что Федеральным законом от 8 августа 2001 года № 128-ФЗ «О лицензировании отдельных видов деятельности» оказание услуг по шифрованию информации отнесено к лицензируемым видам деятельности, то получение лицензии в данном случае обязательно. Форма предоставления услуги значения не имеет.

В23. Являются ли решения для IP-телефонии или беспроводные решения Cisco шифровальными средствами?

О23. По основному функционалу эти решения Cisco не являются средствами шифрования, но в них могут содержаться средства шифрования, используемые для служебных целей. В зависимости от применения этих средств и использования функций шифрования для устройств IP-телефонии и беспроводной связи может потребоваться получение соответствующей лицензии.

В24. Если я не получу лицензию на осуществление деятельности, связанной с шифровальными средствами, то что мне грозит?

О24. Существует уголовная и административная ответственность за деятельность без лицензии или с нарушением условий лицензии, которая подразумевает наказание для физических и юридических лиц в виде штрафов, конфискаций, временного приостановления деятельности и ареста (УК РФ статья 171, КоАП РФ статьи 13.12, 13.13 и 14.1).

В25. Я узнал, что купленное мной оборудование было ввезено в обход законодательства о лицензировании ввоза шифровальных средств. Чем мне это грозит как покупателю? Чем это грозит партнеру, продавшему мне это оборудование? Могу ли я легализовать это оборудование?

О25. Как покупателю ничем, т. к. покупка шифровальных средств никак не регламентируется и легализация оборудования не требуется. Компетентные органы могут попросить Вас сообщить данные продавца или получить их из бухгалтерских документов. Продавцу-нарушителю необходимо читать Уголовный кодекс и Кодекс об административных правонарушениях.

В26. Что делать, если я не могу получить разрешение на ввоз вашего оборудования, содержащего шифрование?

О26. Необходимо купить его на территории России.

В27. Что такое разрешение на эксплуатацию шифровальных средств?

О27. В законодательстве не существует понятие «разрешение на эксплуатацию шифровальных средств». Для шифровальных средств есть лицензия на техническое обслуживание, выдаваемая ФСБ, а также лицензии на ввоз и определенные виды деятельности, также выдаваемые ФСБ. Обладать лицензией на техническое обслуживание шифровальных средств должна эксплуатирующая организация или ее подрядчик.

В28. Если я получу разрешение ФСБ России на ввоз шифровального средства, то значит ли это, что мне не нужен будет сертификат?

О28. Это разные понятия. Разрешение ФСБ России выдается на ввоз шифровального средства, а сертификат ФСБ России означает соответствие конкретного шифровального средства определенным требованиям ФСБ России, позволяющем применять это шифровальное средство для защиты информации определенной категории.

В29. Моя компания имеет филиалы за рубежом, и я хочу защитить взаимодействие с ними с помощью VPN-оборудования Cisco. Как мне быть в такой ситуации?

О29. Если шифровальные средства будут приобретаться в России, а потом пересекать ее границы, необходимо получить разрешение ФСБ России, которое в данном случае выдается достаточно быстро, и лицензию Минпромторга России на ввоз или вывоз шифровальных средств. Если шифровальные средства будут приобретаться в странах, в которых затем будут установлены, обращаться за получением соответствующих разрешения и лицензии в России не нужно (необходимо соблюдать требования законодательства соответствующих стран).

Установка шифровальных средств в России и их последующая эксплуатация собственными силами компании требует получения лицензии на техническое обслуживание шифровальных средств. В случае привлечения для поставки, установки и технического обслуживания сторонней специализированной организации требование о наличии соответствующих лицензий относится к ней.

В30. В нашей компании планируется использование шифровальных средств Cisco. Нужно ли нам получать лицензию на деятельность по техническому обслуживанию шифровальных средств?

О30. В Положении, утвержденном Постановлением Правительства России от 29.12.2007 №957 определение термина "техническое обслуживание" отсутствует, согласно действующему ГОСТ 18322-78 "Система технического обслуживания и ремонта техники. Термины и определения", техническое обслуживание — комплекс операций или операция по поддержанию работоспособности или исправности изделия при использовании по назначению, ожидании, хранении и транспортировании. Исходя из данного определения, настройка или конфигурация шифровальных средств Cisco является техническим обслуживанием, что означает необходимость получения лицензии. Многие наши заказчики заключают сервисные контракты с организациями, имеющими соответствующую лицензию, например, все основные партнеры компании Cisco имеют необходимые лицензии ФСБ.

В31. Моя компания является представительством международной компании. Применяются ли ко мне нормы законодательства, связанные с использованием шифровальных средств?

О31. Это зависит от юридического статуса компании. Если компания является представительством в соответствии с положениями Гражданского кодекса (статья 25):

- представительством является обособленное подразделение юридического лица, расположенное вне места его нахождения, которое представляет интересы юридического лица и осуществляет их защиту,
- представительства не является юридическими лицами. Они наделяются имуществом создавшим их юридическим лицом и действуют на основании утвержденных им положений,

то она не может вести самостоятельную хозяйственную деятельность, владеть имуществом и соответственно многие нормы законодательства, в т.ч. связанные с использованием шифровальных средств, на нее не распространяются.

Если компания является российским юридическим лицом и при этом выполняет функции представительства международной компании, то нормы российского законодательства применяются без каких-либо исключений.

В32. Две компании собираются обеспечить защищенный информационный обмен между собой. При этом, такой обмен не является договорной услугой по защите информации, оказываемой одной компанией другой компании, обе компании используют собственное оборудование. Информация, которая будет передаваться по защищенному каналу связи, является собственностью одной их двух этих компаний. Можно ли в данном случае использовать несертифицированные шифровальные средства производства компании Cisco?

О32. Да, можно, но требуются лицензии на техническое обслуживание средств шифрования, кроме того, информация не должна содержать сведения, составляющие государственную тайну, а также не должна являться конфиденциальной информацией, для защиты которой требуются средства шифрования, имеющие сертификаты ФСБ.

В33. Оператор связи собирается шифровать каналы передачи данных, по которым передается информация, владельцем которой данный оператор связи не является. Например трафик (голос, данные) своих клиентов. Можно ли в данном случае использовать несертифицированные шифровальные средства производства компании Cisco?

О33. Необходимо использовать сертифицированные шифровальные средства, если для обработки этой информации имеется законодательное требование использования сертифицированных средств защиты информации (В-О16).

В34. Компания собирается оказывать услуги по защите информации, в том числе и криптографической. Можно ли в данном случае использовать несертифицированные шифровальные средства производства компании Cisco?

О34. Да, можно, за исключением следующих случаев: если информация, входит в перечни сведений конфиденциального характера, а также не входит в такие перечни, но обрабатывается в информационных и телекоммуникационных системах и сетях критически важных объектов, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления.

В35. К кому обращаться при возникновении дополнительных вопросов?

О35. Сергей Снежков, прямой: +7(499) 929-5282, мобильный: +7(985) 767-7539, ssnezhko@cisco.com

В36. Могу ли я использовать решения Cisco для защиты персональных данных?

О36. Существуют методические документы по защите персональных данных, выпущенные ФСТЭК России (гриф ДСП) и ФСБ России, в которых регламентируется использование только сертифицированных средств защиты информации при обработке персональных данных.

В системе сертификации ФСТЭК России продукция Cisco сертифицировалась неоднократно (http://www.fstec.ru/_razd/_serto.htm).

В системе сертификации ФСБ России продукция Cisco не сертифицировалась. Вместе с тем, при определенных условиях имеется возможность использовать модуль RVPN:

- специальная (не типовая) информационная система обработки персональных данных (ИСПДн)
- разработанная оператором персональных данных частная модель угроз, в которой модель нарушителя относится к типу Н1-Н2.

Эта возможность обусловлена тем, что методическими документами разрешено встраивание криптосредств класса КС1 и КС2 без контроля со стороны ФСБ России.

Для получения более полной информации обращайтесь к Алексею Лукацкому. alukatsk@cisco.com

Cisco
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб.,
52, стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco
Казахстан, 480099,
Алматы,
бизнес-центр «Самал 2»
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: + 7 (727) 244 21 01
Факс: + 7 (727) 244 21 02
www.cisco.ru
www.cisco.com

Cisco
Украина, 03038, Киев,
бизнес-центр
«Горизонт Парк»
(Horizon Park)
Ул. Николая Гринченко, 4В
Тел.: + 7 (38044) 391 36 00
Факс: + 7 (38044) 391 36 00
www.cisco.ua
www.cisco.com

Cisco
Азербайджан,
AZ 1065, Баку,
бизнес-центр «Карат»
Ул. М. Мухтарова, 201,
этаж 2
Тел.: + 7 (99412) 437 48 20
Факс: + 7 (99412) 437 48 21
www.cisco.ru
www.cisco.com

Cisco
Узбекистан, 100000,
Ташкент, бизнес-центр
«ИНКОНЕЛЬ»
Ул. Пушкина, 75, офис 605,
этаж 6
Тел.: + 7 (99871) 140 44 60
Факс: + 7 (99871) 133 44 64
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel •Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe