Содержание

Характеристика предметной области.

Сертификация *средств защиты информации* производится в соответствии с "Положением о сертификации *средств защиты информации*", утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 г.

Сертификация - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Сертификат соответствия - документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих *государственную тайну*, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации *средств защиты информации.*

Система сертификации *средств защиты информации* представляет собой совокупность участников сертификации, которыми являются:

- федеральный орган по сертификации;
- центральный орган системы сертификации - орган, возглавляющий систему сертификации однородной продукции;
- органы по сертификации *средств защиты информации* - органы, проводящие сертификацию определенной продукции;
- испытательные лаборатории - лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;
- изготовители - продавцы, исполнители продукции.

Центральные органы системы сертификации, органы по сертификации *средств защиты информации* и испытательные лаборатории проходят аккредитацию на право проведения работ по сертификации. Целью аккредитации является проверка возможности выполнения работ по сертификации *средств защиты информации*. Аккредитация проводится только при наличии у указанных органов и лабораторий лицензии на соответствующие виды деятельности.

Федеральный орган по сертификации осуществляет следующее:

- создает системы сертификации;
- осуществляет выбор способа подтверждения соответствия *средств защиты информации* требованиям нормативных документов;
- устанавливает правила аккредитации центральных органов систем сертификации, органов по сертификации *средств защиты информации* и испытательных лабораторий;
- определяет центральный орган для каждой системы сертификации;
- выдает сертификаты и лицензии на применение знака соответствия;
- ведет государственный реестр участников сертификации и сертифицированных *средств защиты информации*;

- осуществляет государственные контроль и надзор за соблюдением участниками сертификации правил сертификации и за сертифицированными средствами защиты информации, а также устанавливает порядок инспекционного контроля;
- рассматривает апелляции по вопросам сертификации;
- представляет на государственную регистрацию в Комитет Российской Федерации по стандартизации, метрологии и сертификации системы сертификации и знак соответствия;
- устанавливает порядок признания зарубежных сертификатов;
- приостанавливает или отменяет действие выданных сертификатов.

Центральный орган системы сертификации:

- организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации *средств защиты информации* и испытательных лабораторий, входящих в систему сертификации;
- ведет учет входящих в систему сертификации органов по сертификации *средств защиты информации* и испытательных лабораторий, выданных и *аннулированных сертификатов* и лицензий на применение знака соответствия;
- обеспечивает участников сертификации информацией о деятельности системы сертификации.

При отсутствии в системе сертификации центрального органа его функции выполняются федеральным органом по сертификации

Органы по сертификации *средств защиты информации*:

- сертифицируют средства защиты информации, выдают сертификаты и лицензии на применение знака соответствия с представлением копий в федеральные органы по сертификации и ведут их учет;
- приостанавливают либо отменяют действие выданных ими сертификатов и лицензий на применение знака соответствия;
- принимают решение о проведении повторной сертификации при изменениях в технологии изготовления и конструкции (составе) сертифицированных *средств защиты информации*;
- формируют фонд нормативных документов, необходимых для сертификации;
- представляют изготовителям по их требованию необходимую информацию в пределах своей компетенции.

Испытательные лаборатории проводят сертификационные испытания *средств защиты информации* и по их результатам оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации *средств защиты информации* и изготовителям. Испытательные лаборатории несут ответственность за полноту испытаний *средств защиты информации* и достоверность их результатов.

Изготовители:

- производят (реализуют) средства защиты информации только при наличии сертификата;
- извещают орган по сертификации, проводивший сертификацию, об изменениях в технологии изготовления и конструкции (составе) сертифицированных *средств защиты информации*;
- маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном для данной системы сертификации;

- указывают в сопроводительной технической документации сведения о сертификации и нормативных документах, которым средства защиты информации должны соответствовать, а также обеспечивают доведение этой информации до потребителя;
- применяют сертификат и знак соответствия, руководствуясь законодательством Российской Федерации и правилами, установленными для данной системы сертификации;
- обеспечивают соответствие *средств защиты информации* требованиям нормативных документов по защите информации;
- обеспечивают беспрепятственное выполнение своих полномочий должностными лицами органов, осуществляющих сертификацию, и контроль за сертифицированными средствами защиты информации;
- прекращают реализацию *средств защиты информации* при несоответствии их требованиям нормативных документов или по истечении срока действия сертификата, а также в случае приостановки действия сертификата или его отмены.

Процедура сертификации включает:

1. подачу и рассмотрение заявки на проведение сертификации (продления срока действия) средства защиты информации в Федеральный орган по сертификации. Заявка оформляется на бланке заявителя и заверяется печатью. Федеральный орган назначает орган по сертификации и испытательную лабораторию, после чего заявитель отправляет туда сертифицируемое средство защиты информации.
2. сертификационные испытания *средств защиты информации* и (при необходимости) аттестацию их производства. Сроки проведения испытаний устанавливаются на договорной основе между заявителем и лабораторией. По результатам испытаний оформляется заключение, которое отправляется в орган по сертификации и заявителю.
3. экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия. На основании заключения испытательной лаборатории орган сертификации делает заключение и отправляет его в Федеральный орган по сертификации. После присвоения сертификату регистрационного номера, его получает заявитель. Срок действия сертификата – **3 года**.
4. осуществление государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации. По результатам контроля Федеральный орган по сертификации может приостановить или аннулировать сертификат в следующих случаях:
    - изменения на законодательном уровне, касающиеся требований к средствам защиты информации, методам испытаний и контроля;
    - изменение технологии изготовления, конструкции (состава), комплектности *средств защиты информации* и системы контроля их качества;
    - невыполнение требований технологии изготовления, контроля и испытаний *средств защиты информации*;
    - несоответствие сертифицированных *средств защиты информации* техническим условиям или формуляру, выявленное в ходе государственного или инспекционного контроля;

- отказ заявителя в допуске (приеме) лиц, уполномоченных осуществлять государственный контроль и надзор, инспекционный контроль за соблюдением правил сертификации и за сертифицированными средствами защиты информации.

5. информирование о результатах сертификации *средств защиты информации*;
6. рассмотрение апелляций. Апелляция подается в федеральный орган по сертификации и рассматривается в месячный срок с участием независимых экспертов и заинтересованных сторон.

Сертификация импортных *средств защиты информации* проводится по тем же правилам, что и отечественных.

Основными схемами проведения сертификации *средств защиты информации* являются:

- единичных образцов *средств защиты информации* - проведение испытаний этих образцов на соответствие требованиям по защите информации;
- для серийного производства *средств защиты информации* - проведение типовых испытаний образцов *средств защиты информации* на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных *средств защиты информации*, определяющих выполнение этих требований.

В отдельных случаях по согласованию с органом по сертификации *средств защиты информации* допускается проведение испытаний на испытательной базе изготовителя. Сроки проведения испытаний устанавливаются договором между изготовителем и испытательной лабораторией.

При несоответствии результатов испытаний требованиям нормативных и методических документов по защите информации орган по сертификации *средств защиты информации* принимает решение об отказе в выдаче сертификата и направляет изготовителю мотивированное заключение.

В случае несогласия с отказом в выдаче сертификата изготовитель имеет право обратиться в центральный орган системы сертификации, федеральный орган по сертификации или в Межведомственную комиссию для дополнительного рассмотрения полученных при испытаниях результатов.

Оплата работ по сертификации конкретных *средств защиты информации* осуществляется на основании договоров между участниками сертификации.

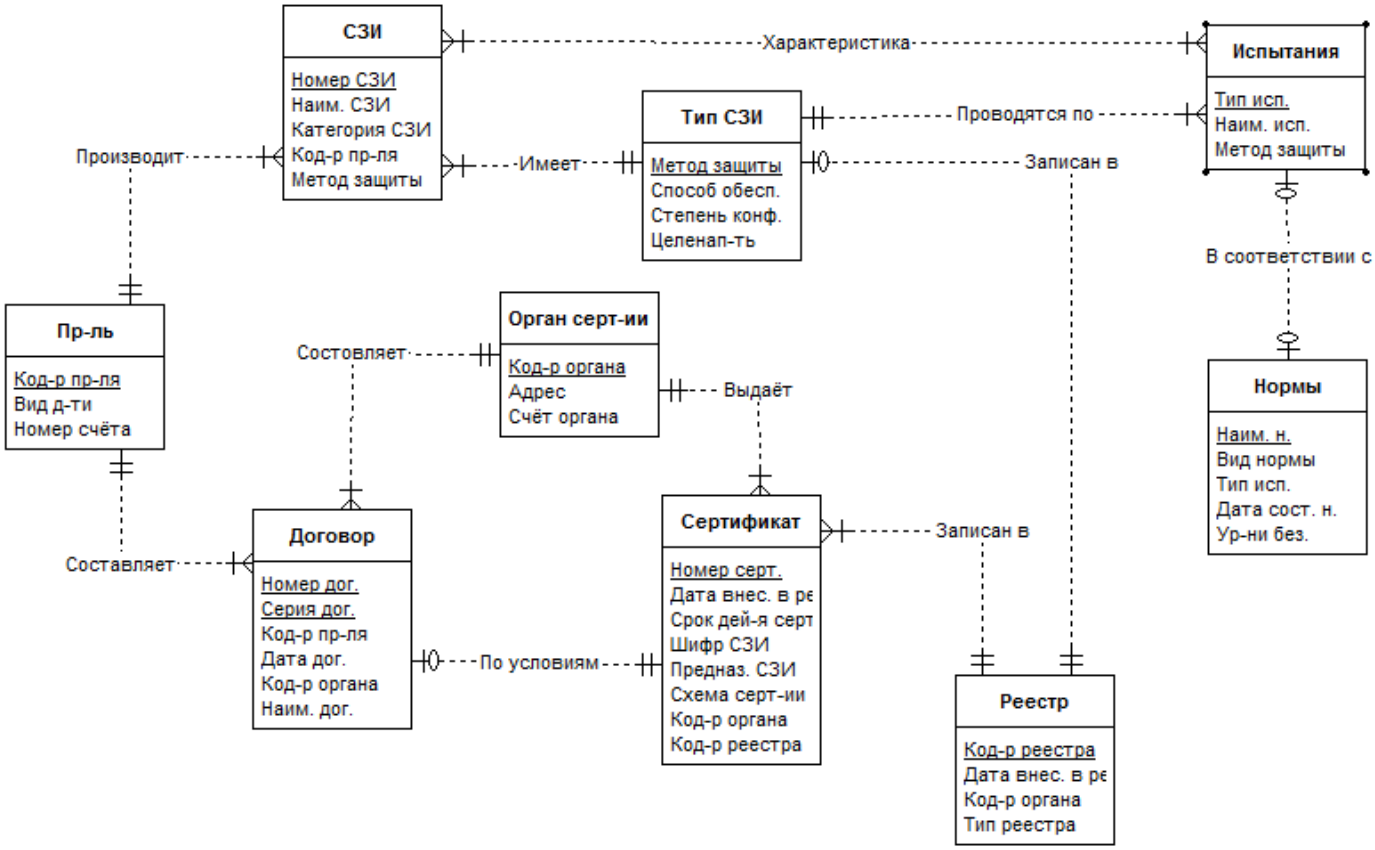
Инспекционный контроль за сертифицированными средствами защиты информации осуществляют органы, проводившие сертификацию этих *средств защиты информации*.

Органы по сертификации и испытательные лаборатории несут ответственность за выполнение своих функций, обеспечение сохранности *информации ограниченного доступа*, материальных ценностей, предоставленных заявителем, а также за соблюдение авторских прав разработчика при испытаниях его *средств защиты информации*.

Основными органами сертификации в области технической защиты информации являются ФСБ России и ФСТЭК России. При этом ФСБ России действует в области криптографической защиты информации, а ФСТЭК России – в области технической защиты информации некриптографическими методами. Требования по сертификации

ФСБ России являются закрытыми, ознакомление с ними предполагает наличие специальных допусков, требования ФСТЭК России публикуются на официальном сайте и являются публичными.

ER-модель.



Реляционные отношения.

1. **Пр-ль** (Код-р пр-ля, вид д-ти, номер счёта):
   Первичный ключ: Код-р пр-ля;
   Вторичный ключ: вид д-ти.
2. **СЗИ** (Номер СЗИ, наим. СЗИ, категория СЗИ, код-р пр-ля, метод защиты):
   Первичный ключ: Номер СЗИ;
   Вторичный ключ: наим. СЗИ;
   Родительский ключ: код-р пр-ля, метод защиты.
3. **Тип СЗИ** (Метод защиты, способ обесп.,степень конф., целенап-ть):
   Первичный ключ: Метод защиты;
   Вторичный ключ: целенап-ть.
4. **Испытания** (Тип исп., наим. исп., метод защиты):
   Первичный ключ: Тип исп.;
   Вторичный ключ: наим. исп.;
   Родительский ключ: метод защиты.
5. **Нормы** (Наим. н., вид нормы, тип исп., дата сост. н., ур-ни без.) :
   Первичный ключ: Наим. н.;
   Вторичный ключ: вид нормы;

Родительский ключ: тип исп.

6. **Договор** (Номер дог., серия дог., код-р пр-ля, дата дог., код-р органа, наим. дог.):
   Первичный ключ: Номер дог., серия дог.;
   Вторичный ключ: наим. дог.;
   Родительский ключ: код-р пр-ля, код-р органа.
7. **Орган серт-ии** (Код-р органа, адрес, счёт органа):
   Первичный ключ: Код-р органа;
   Вторичный ключ: адрес.
8. **Сертификат** (Номер серт., дата внес. в реестр, срок дей-я серт., шифр СЗИ, предназ. СЗИ, схема серт-ии, код-р органа, код-р реестра):
   Первичный ключ: Номер серт.;
   Вторичный ключ: срок дей-я серт., схема серт-ии;
   Родительский ключ: код-р органа.
9. **Реестр** (Код-р реестра, дата внес. в реестр, код-р органа, тип реестра):
   Первичный ключ: Код-р реестра;
   Вторичный ключ: тип реестра;
   Родительский ключ: код-р органа.