Лекция 4: Лицензирование деятельности в области ТЗИ

Аннотация: Рассмотрено понятие лицензирования, его основные цели и общий порядок получения лицензии в России. Представлены основные требования к соискателю и порядок получения лицензии в области технической защиты конфиденциальной информации. Описаны способы контроля за соблюдением лицензионных требований: плановые и внеплановые проверки ФСТЭК.

4.1. Общий порядок лицензирования

Лицензирование деятельности в области защиты информации представляет собой определенную форму государственного контроля и должно обеспечить не только допуск организаций, соответствующих определенным требованиям и условиям, к осуществлению определенных видов деятельности, но и повышение качества непосредственно мероприятий и услуг по технической защите информации.

Государственная система лицензирования деятельности в области технической защиты информации включает в себя две составляющие:

допуск предприятий и организаций к оказанию услуг по защите информации;
контроль качества и эффективности оказываемых услуг в процессе их деятельности.
Рассмотрим основные понятия в области лицензирования.

Лицензия - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

Лицензируемый вид деятельности - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии.

Лицензирование - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, ведением реестров лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании.

Лицензионные требования и условия - совокупность установленных положениями о лицензировании конкретных видов деятельности требований и условий, выполнение которых лицензиатом обязательно при осуществлении лицензируемого вида деятельности.

Лицензирующие органы - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с ФЗ "О лицензировании отдельных видов деятельности" от 8 августа 2001г.

Лицензиат - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности;

Соискатель лицензии - юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности.

Реестр лицензий - совокупность данных о предоставлении лицензий, переоформлении документов, подтверждающих наличие лицензий, приостановлении и возобновлении действия лицензий и об аннулировании лицензий.

Срок действия лицензии не может быть более 5 лет. По истечении этого срока лицензия может быть продлена по заявлению лицензиата.

Порядок получения лицензии следующий:

Соискатель лицензии отправляет в лицензирующий орган заявление о предоставлении лицензии, в котором указываются:

для юридического лица: полное и сокращенное наименование и организационно-правовая форма, адреса, где планируется ведение лицензируемого вида деятельности, государственный регистрационный номер записи о создании юр.лица и данные документа, подтверждающего внесение в реестр юридических лиц РФ.
для индивидуального предпринимателя: полное ФИО, место жительства, адреса мест, где планируется ведение лицензируемой деятельности, данные документа, удостоверяющего личность (например, паспорта), государственный регистрационный номер записи о регистрации и данные документа, подтверждающего факт внесения сведений об индивидуальном предпринимателе в единый государственный реестр индивидуальных предпринимателей.
ИНН и данные документа, подтверждающего постановку соискателя на учет в налоговом органе.
лицензируемый вид деятельности.
К заявлению соискатель должен приложить следующие документы:

копии учредительных документов (для юридического лица);
документ, подтверждающий уплату государственной пошлины за рассмотрение лицензирующим органом заявления о предоставлении лицензии;
копии документов, перечень которых определяется положением о лицензировании конкретного вида деятельности и которые свидетельствуют о наличии у соискателя лицензии возможности выполнения лицензионных требований и условий, в том числе документов, наличие которых при осуществлении лицензируемого вида деятельности предусмотрено федеральными законами.
Решение о предоставлении лицензии (или отказе) принимается в срок, не превышающий 5 дней со дня поступления документов. Уведомление о принятии решения вручается или отправляется соискателю в письменной форме. Если решение отрицательное, должны указываться причины отказа и реквизиты акта проверки возможности выполнения соискателем лицензии лицензионных требований и условий, если причиной отказа

является невозможность выполнения соискателем лицензии указанных требований и условий. Соискатель лицензии должен заплатить государственную пошлину за получение лицензии и в течение трех дней после оплаты может получить лицензию.

Причинами отказа в получении лицензии могут быть:

наличие в документах, представленных соискателем лицензии, недостоверной или искаженной информации;
несоответствие соискателя лицензии, принадлежащих ему или используемых им объектов лицензионным требованиям и условиям.
Перечислим пункты, которые должны содержать решение о предоставлении лицензии и в документе, подтверждающем наличие лицензии:

наименование лицензирующего органа;
полное и (в случае, если имеется) сокращенное наименование, в том числе фирменное наименование, и организационно-правовая форма юридического лица, место его нахождения, адреса мест осуществления лицензируемого вида деятельности, государственный регистрационный номер записи о создании юридического лица;
ФИО индивидуального предпринимателя, место его жительства, адреса мест осуществления лицензируемого вида деятельности, данные документа, удостоверяющего его личность, основной государственный регистрационный номер записи о государственной регистрации индивидуального предпринимателя;
лицензируемый вид деятельности;
срок действия лицензии;
ИНН;
номер лицензии;
дата принятия решения о предоставлении лицензии.
Лицензирующий орган вправе приостановить действие лицензии или аннулировать ее. Приостановление действия лицензии осуществляется по решению суда в случае выявления нарушений лицензионных требований и условий в течение суток со дня принятия судом решение. Действие лицензии возобновляется, если лицензиат уведомляет в письменном виде об устранении нарушений. Если лицензиат не устраняет нарушения в установленный судом срок, лицензирующий орган может обратиться в суд, по решению которого лицензия может быть аннулирована.

Действие лицензии прекращается в следующих случаях:

ликвидация юридического или физического лица.
окончание срока действия лицензии или принятие решения о досрочном прекращении действия лицензии на основании представленного в лицензирующий орган заявления в письменной форме лицензиата.
решение суда об аннулировании лицензии.
Лицензирующие органы обязаны вести специальные реестры лицензий на виды деятельности, лицензирование которых они осуществляют. В реестре указывается следующая информация:

полное и (в случае, если имеется) сокращенное наименование, в том числе фирменное наименование, и организационно-правовая форма юридического лица, место его

нахождения, адреса мест осуществления лицензируемого вида деятельности, государственный регистрационный номер записи о создании юридического лица;
фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, место его жительства, адреса мест осуществления лицензируемого вида деятельности, данные документа, удостоверяющего его личность, основной государственный регистрационный номер записи о государственной регистрации индивидуального предпринимателя;
лицензируемый вид деятельности (с указанием выполняемых работ и оказываемых услуг при осуществлении видов деятельности, указанных в пункте 2 статьи 17 настоящего Федерального закона);
срок действия лицензии;
идентификационный номер налогоплательщика;
номер лицензии;
дата принятия решения о предоставлении лицензии;
сведения о регистрации лицензии в реестре лицензий;
основание и срок приостановления и возобновления действия лицензии;
основание и дата аннулирования лицензии;
основание и срок применения упрощенного порядка лицензирования;
сведения об адресах мест осуществления лицензируемого вида деятельности;
сведения о выдаче документа, подтверждающего наличие лицензии;
основание и дата прекращения действия лицензии;
иные сведения, определенные положениями о лицензировании конкретных видов деятельности.
Информация из реестра лицензий является открытой для физических и юридических лиц. Выписку можно получить за установленную плату в 10 рублей в течение трех дней после подачи заявления.

Перечислим виды деятельности, относящиеся к защите информации, на осуществление которых требуется получение лицензии:

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 систем, телекоммуникационных систем;
деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
деятельность по технической защите конфиденциальной информации;
разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Важным пунктом в контексте данного курса является необходимость получения лицензии на осуществление деятельности по технической защите конфиденциальной информации.

4.2. Лицензирование деятельности в области технической защиты информации

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК России. Для получения лицензии соискателю необходимо выполнить следующие требования и условия:

наличие в штате специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;
наличие у соискателя лицензии помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;
наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;
использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;
использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;
наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю [4.3]

Для получения лицензии соискатель отправляет в ФСТЭК документы, рассмотренные в предыдущем разделе данной лекции. Помимо этих документов, соискатель обязан предоставить следующее:

копии документов, подтверждающих квалификацию специалистов по защите информации (дипломов, удостоверений, свидетельств);
копии документов, подтверждающих право собственности, право хозяйственного ведения или оперативного управления на помещения, предназначенные для осуществления лицензируемой деятельности, либо копии договоров аренды указанных помещений или безвозмездного пользования ими;
копии аттестатов соответствия защищаемых помещений требованиям безопасности информации;
копии технического паспорта автоматизированной системы с приложениями, акта классификации автоматизированной системы по требованиям безопасности информации, плана размещения основных и вспомогательных технических средств и систем, аттестата соответствия автоматизированной системы требованиям безопасности информации или сертификата соответствия автоматизированной системы требованиям безопасности

информации, а также перечень защищаемых в автоматизированных системах ресурсов с документальным подтверждением степени конфиденциальности каждого ресурса, описание технологического процесса обработки информации в автоматизированной системе;
копии документов, подтверждающих право на используемые для осуществления лицензируемой деятельности программы для электронно-вычислительных машин и базы данных;
сведения о наличии производственного и контрольно-измерительного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемой деятельности, с приложением копий документов о поверке контрольно-измерительного оборудования;
сведения об имеющихся у соискателя лицензии нормативных правовых актах, нормативно-методических и методических документах по вопросам технической защиты информации[4.3]
ФСТЭК проверяет комплектность предоставленных документов, полноту и достоверность указанных в них сведений. Если каких-то сведений (документов) не хватает, ФСТЭК в течение 15 дней уведомляет об этом соискателя. В срок, не превышающий 45 дней после получения документов от соискателя, ФСТЭК принимает решение о выдаче лицензии. Решение оформляется соответствующим актом ФСТЭК.

Лицензия выдается на 5 лет , и после окончания этого срока может быть продлена по заявлению лицензиата.

4.3. Контроль за соблюдением лицензионных требований и условий
Функция контроля за соблюдением лицензиатом лицензионных требований и условий осуществляет лицензирующий орган, то есть в случае технической защиты конфиденциальной информации – ФСТЭК. Способом контроля являются плановые и внеплановые проверки, которые проводятся в порядке, установленным ФЗ-№294 "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

Целью плановой проверки является проверка соблюдения лицензиатом лицензионных требований и условий в процессе осуществления деятельности по технической защите конфиденциальной информации. В отношении одного юридического лица или индивидуального предпринимателя она может проводиться не чаще одного раза в течение трех лет. Плановые проверки осуществляются в соответствии с ежегодным планом проверок, который публикуется на официальном сайте ФСТЭК России.

Лицензиат включается в плановую проверку в случае истечения трех лет со дня:

государственной регистрации лицензиата;
окончания проведения последней плановой проверки лицензиата.
Лицензиат уведомляется не позднее трех рабочих дней до проведения проверки.

Предметом внеплановой проверки является соблюдение лицензиатом лицензионных требований и условий, выполнение предписаний об устранении выявленных нарушений, проведение мероприятий по обеспечению безопасности государства.

Основанием для проведения внеплановой проверки является:

истечение срока исполнения ранее выданного лицензиату предписания об устранении выявленного нарушения лицензионных требований и условий;
поступление в ФСТЭК России обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:
возникновения угрозы причинения вреда безопасности государства;
причинение вреда безопасности государства.
Плановая и внеплановые проверки проводятся в документарной или выездной формах. Документарная проверка проверяет документы лицензиата и осуществляется по месту нахождения ФСТЭК. В ходе выездной проверки проверяются не только документы лицензиата, но и соответствие его лицензионным требованиям и условиям.

Срок проведения каждой из проверок не может превышать 20 рабочих дней. По результатам проверки составляется акт в двух экземплярах, к которому прилагаются протоколы (заключения) проведенных исследований (испытаний) и экспертиз.

Подводя итог, можно сказать, что процесс получения лицензии на техническую защиту конфиденциальной информации является весьма трудоемким, длительным и, что не маловажно, затратным, ведь для получения лицензии необходимо выполнить все лицензионные требования и условия. Самым продолжительным по времени является обучение специалистов на курсах повышения квалификации. Несмотря на то, что количество организаций, имеющих дело с конфиденциальной информацией, достаточно велико, специалистов с высшим профессиональным образованием в области ТЗИ может позволить себе далеко не каждая из них. Частные курсы по повышению квалификации, утвержденные ФСТЭК, как правило, рассчитаны на 72 часа. Самым затратным в экономическом плане требованием является проведение аттестации объектов информатизации (автоматизированной системы и защищенного помещения), предназначенных для обработки конфиденциальной информации. Более того, возникает проблема приобретения контрольно-измерительного оборудования, которое после аттестации вообще не нужно, если только организация не собирается оказывать услуги по аттестации объектов информатизации. Альтернативный вариант – взять такое оборудование в аренду, но это тоже стоит денег. Таким образом, продолжительность процесса лицензирования может занять от 2 до 6 месяцев и повлечь за собой значительные материальные затраты. Вариантом решения данной проблемы является аутсорсинг. Аутсорсинг (от англ. outsourcing) дословно "использование внешних источников". Аутсорсинг предполагает передачу от компании-заказчика сторонней организации(подрядчику) определенных функций уставной деятельности, например, техническую защиту конфиденциальной информации. При этом подрядчик использует свои программные, технические и другие средства защиты, лицензии, аттестаты и т.п., а также несет ответственность за результат выполнения своей работы.

Сертификация средств защиты информации

Аннотация: В лекции приведены основные понятия в области сертификации, рассмотрены участники стандартной схемы сертификации и этапы сертификации средств защиты информации.

5.1. Общий порядок сертификации средств защиты информации

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 [5.1]

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 [5.1]. 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:

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.
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.
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.
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.
информирование о результатах сертификации средств защиты информации;
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 [5.1].

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.

5.2. Порядок сертификации во ФСТЭК России

Рассмотрим примерный перечень действий по сертификации во ФСТЭК России.

Подача заявки на сертификацию во ФСТЭК России.
В заявке указываются:

наименования заявителя
адрес заявителя
наименование продукции, которую Заявитель хочет сертифицировать
перечень нормативных и методических документов, на соответствие требованиям которых заявителю необходимо сертифицировать свою продукцию.
схема сертификации (единичный образец продукции или серийное производство)
испытательная лаборатория, в которой Заявитель хотел бы провести испытания
дополнительные условия или требования
Заявитель указывает в заявке, что он обязуется:

выполнять все условия сертификации;
обеспечивать стабильность сертифицированных характеристик продукции, маркированной знаком соответствия;
оплатить все расходы по проведению сертификации.
Важно: заявитель должен иметь лицензию ФСТЭК на соответствующий вид деятельности!

Пример заявки на сертификацию программного комплекса представлен на рисунке 5.1.

Пример заявки на сертификацию

ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«Центр Информационных технологий

« XXX »

111111, Москва, Ивановское шоссе 10
тел/факс 333-33-33

ИНН XXXXXXX, КПП XXXXXX
Р/счет № XXXXXXXXXXXX
в Курском отделении № XXXX/XX, СБ РФ г. Москва
К/с XXXXXXXXXXXXXXX, БИК XXXXXX

_____ № _____
На № _____ от _____

Заместителю
Директора Федеральной службы по
техническому и экспортному контролю
XXXXX X.X.

103175, г. Москва, ул. Старая Басманная, 17

ЗАЯВКА
на проведение сертификации продукции
в системе сертификации средств защиты информации
по требованиям безопасности информации
№ РОСС RU. 0001. 01БИ00

1. Закрытое акционерное общество «Центр Информационных технологий «XXX» (ЗАО «XXX»), адрес: 111111, г. Москва, Ивановское шоссе, д. 10, просит провести сертификацию следующей продукции:

«Программный комплекс «XXXX», XXXXXXXX
(наименование продукции, код ОКП, шифр)

по требованиям безопасности информации на соответствие:
- требованиям технических условий XXXXXXXXXXX;
- требованиям руководящего документа «Защита от несанкционированного доступа к информации» Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. По 2 уровню контроля.

2. Заявитель предлагает провести испытания изделия по схеме:
сертификация единичного образца в испытательной лаборатории Санкт-Петербургского научно-технического центра ФГУП «Научно-производственное предприятие «Гамма» (197110 г. Санкт-Петербург, ул. Пионерская, д. 44, тел. (812) 235-55-18).

3. Заявитель обязуется:
- выполнять все условия сертификации;
- обеспечивать стабильность сертифицированных характеристик средств защиты информации, маркированных знаком соответствия;
- оплатить все расходы по проведению сертификации.

Генеральный директор /Иванов И.И./

место гербовой печати
«__» _____ 2008 г.

Рис. 5.1. Пример заявки на сертификацию

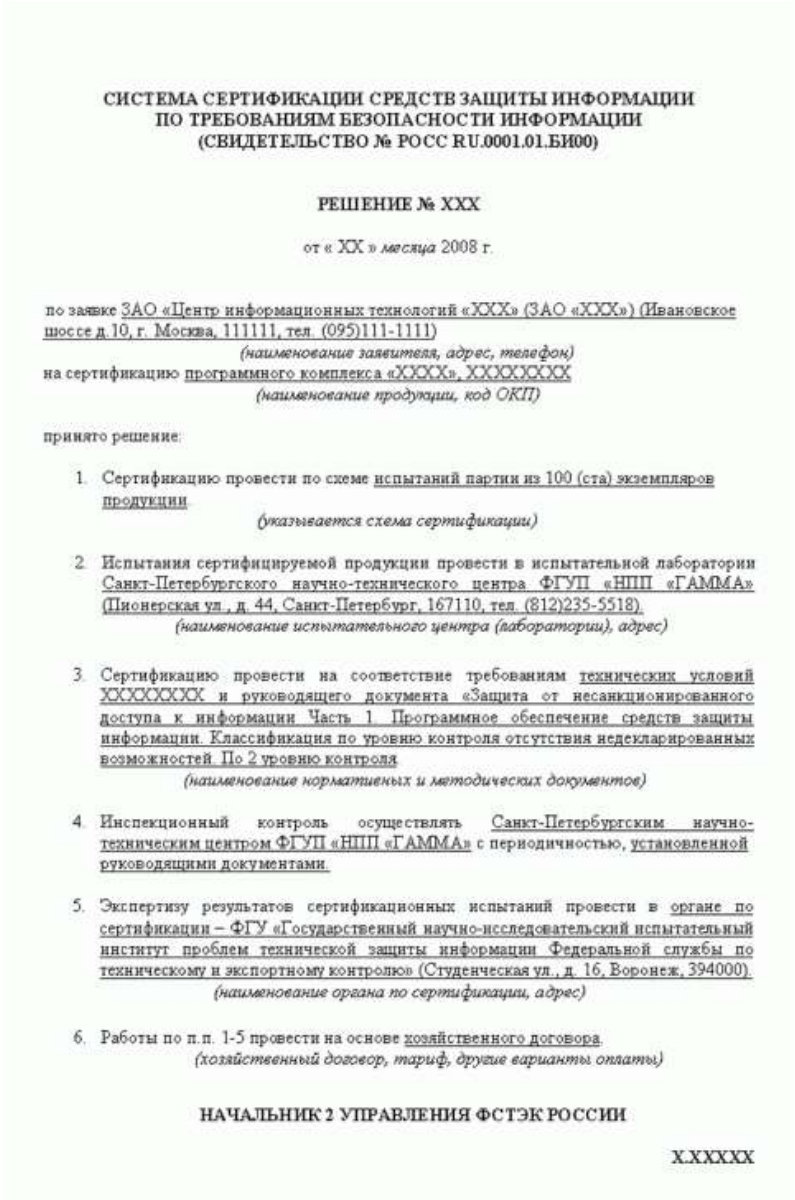
Решение на проведение сертификационных испытаний

ФСТЭК в течение месяца после получения заявки направляет Заявителю, назначенным органу по сертификации и испытательной лаборатории решение на проведение сертификационных испытаний, которое содержит следующее:

наименование Заявителя, адрес Заявителя;
наименование сертифицируемой продукции, код ОКП, ТУ;
схема проведения сертификации (испытания единичного образца продукции/ партии из N образцов/ образца продукции для серийного производства);
назначенная испытательная лаборатория и ее адрес;
перечень нормативных и методических документов, на соответствие требованиям которых должна проводиться сертификация;
испытательная лаборатория, назначенная для проведения последующего инспекционного контроля;
орган по сертификации, назначенный для проведения экспертизы результатов сертификационных испытаний;
способ оплаты работ.

Орган по сертификации и испытательная лаборатория могут быть изменены по согласованию с Заказчиком. Решение служит основанием для начала испытаний и "поводом" для заключения договора между Заявителем и испытательной лабораторией. Пример решения на проведение сертификации представлен на рисунке 5.2.

Пример решения на проведение сертификационных испытаний



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
(СВИДЕТЕЛЬСТВО № РОСС RU.0001.01.БИ00)

РЕШЕНИЕ № ХХХ

от « ХХ » *месяца* 2008 г.

по заявке ЗАО «Центр информационных технологий «ХХХ» (ЗАО «ХХХ») (Ивановское шоссе д.10, г. Москва, 111111, тел. (095)111-1111)
(наименование заявителя, адрес, телефон)
на сертификацию программного комплекса «ХХХХ», ХХХХХХХХ
(наименование продукции, код ОКП)

принято решение:

1. Сертификацию провести по схеме испытаний партии из 100 (ста) экземпляров продукции
(указывается схема сертификации)
2. Испытания сертифицируемой продукции провести в испытательной лаборатории Санкт-Петербургского научно-технического центра ФГУП «НПП «ГАММА» (Пионерская ул., д. 44, Санкт-Петербург, 167110, тел. (812)235-5518)
(наименование испытательного центра (лаборатории), адрес)
3. Сертификацию провести на соответствие требованиям технических условий ХХХХХХХХ и руководящего документа «Защита от несанкционированного доступа к информации Часть 1 Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. По 2 уровню контроля
(наименование нормативных и методических документов)
4. Инспекционный контроль осуществлять Санкт-Петербургским научно-техническим центром ФГУП «НПП «ГАММА» с периодичностью, установленной руководящими документами.
5. Экспертизу результатов сертификационных испытаний провести в органе по сертификации – ФГУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (Студенческая ул., д. 16, Воронеж, 394000).
(наименование органа по сертификации, адрес)
6. Работы по п.п. 1-5 провести на основе хозяйственного договора.
(хозяйственный договор, тариф, другие варианты оплаты)

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ

Х.ХХХХХ

Рис. 5.2. Пример решения на проведение сертификационных испытаний

Заключение договора с испытательной лабораторией

В договоре с испытательной лабораторией о проведении сертификационных испытаний устанавливаются сроки, порядок проведения сертификационных испытаний, а также стоимость работ. Обычно испытательная лаборатория сначала готовит коммерческое предложение с обоснованием сроков и стоимости работ, а также проект договора. Как правило, в комплект договорных документов входят: договор, техническое задание на проведение работ, ведомость исполнения, протокол согласования цены. Помимо указанных сведений, в договоре рекомендуется предусмотреть такие пункты, как ответственность за порчу испытательных образцов или порядок приостановки испытаний в случае внесения каких-то изменений.

Подготовка исходных данных.

Этот этап включает в себя разработку, согласование и утверждение программы и методики сертификационных испытаний.

Испытательная лаборатория разрабатывает программу и методику проведения испытаний, передает заявителю информацию о том, какие данные необходимы для испытаний. Также программа и методика отправляются в орган по сертификации на утверждение.

Заявитель получает от испытательной лаборатории программу и методику испытаний, согласовывает ее и готовит все необходимые исходные данные. Он предоставляет испытательной лаборатории средства защиты информации в комплектации, соответствующей техническим условиям или формуляру, а также комплект всей необходимой документации в соответствии с ЕСПД или ЕСКД.

Сертификационные испытания.
Испытательная лаборатория отбирает образцы сертифицируемой продукции, идентифицирует их и проводит сертификационные испытания продукции по утвержденным программе и методике. При этом Заявитель готовит и настраивает стенд для проведения сертификационных испытаний. Важно отметить, что запрещается вносить изменения в состав или конструкцию объекта сертификации, а также в документацию во время испытаний. Это может привести к остановке испытаний и их полному "перезапуску", что повлияет на стоимость и сроки проведения работ.

Оформление результатов испытаний
Результаты испытаний оформляются в виде протоколов сертификационных испытаний и технических заключений. Эти документы направляются в орган по сертификации, а копии – Заявителю. В случае отсутствия обоснованных замечаний к результатам, предоставленным испытательной лабораторией, со стороны Заявителя или органа по сертификации, ее работа по договору считается выполненной.

Заключение договора с органом по сертификации
Испытательная лаборатория заключает договор с органом по сертификации о проведении экспертизы результатов сертификационных испытаний, в котором оговариваются сроки (как правило, 1 месяц), порядок и стоимость. Иногда орган по сертификации требует заключить договор с Заявителем, а не с испытательной лабораторией. Этот пункт является спорным и не регламентированным. Данный вопрос лучше всего изначально оговорить с испытательной лабораторией.

Экспертиза результатов сертификационных испытаний
Орган по сертификации в соответствии с договором проводит экспертизу результатов сертификационных испытаний, а также технических и эксплуатационных документов на сертифицируемую продукцию. Результатом становится оформление экспертного заключения, которое вместе с техническим заключением, материалами сертификационных испытаний, комплектом необходимой технической и эксплуатационной документации на объект сертификации представляет во ФСТЭК России для принятия решения о выпуске сертификата.

Решение о выдаче сертификата.

На основании полученных от органа сертификации документов, а именно технического заключения и экспертного заключения, ФСТЭК принимает решение о выдаче сертификата. Как было сказано выше, срок сертификата 3 года. Пример сертификата соответствия на рисунке 5.3.

Пример сертификата соответствия ФСТЭК

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 0000

Выдан 00 xxxxxx 0000 г.
Действителен до 00 xxxxxx 0003 г.

Настоящий сертификат удостоверяет, что **программный комплекс «XXXX»** (партия из 100 (ста) экземпляров продукции с заводскими №№ 000-000, маркированных знаками соответствия с № X 000000 по № X 000100), производства ЗАО «XXX» (г. Москва), является защищенным программным средством обработки информации и соответствует требованиям формуляра XXXX.000000.000ФХ и руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 2 уровню контроля.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма» (аттестат аккредитации от 10.05.2007 № СЗИ.RU.082.Б28.051) – техническое заключение от 00.00.00, и экспертного заключения ФСТЭК России от 00.00.00.

Заявитель: ЗАО «XXX»
Адрес: 111111, г. Москва, Ивановское шоссе, д. 10
Телефон: (095) 111-1111

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящих документов и формуляра осуществляется испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

ПЕЧАТЬ Подпись **X.Xxxxx**

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 00 xxxxxx 0000 г.

Рис. 5.3. Пример сертификата соответствия ФСТЭК

Если в результате проверки ФСТЭК выявит несоответствие результатов испытаний требованиям законодательства, будет принято решение об отказе в выдаче сертификата. При этом Заявителю будет направлено мотивированное заключение. В случае несогласия с отказом Заявитель имеет право обратиться в апелляционный совет Федерального органа по сертификации для дополнительного рассмотрения материалов сертификации. Апелляция рассматривается в месячный срок с привлечением заинтересованных сторон и независимых экспертов. Податель апелляции извещается о принятом решении.

Лекция 6: Аттестация объекта информатизации по требованиям безопасности информации

Аннотация: В лекции приведены основные понятия в области аттестации объекта информатизации по требованиям безопасности, рассмотрены участники стандартной схемы аттестации и этапы аттестации.

Деятельность по аттестации объектов информатизации по требованиям безопасности информации осуществляет ФСТЭК России (бывш. Гостехкомиссия России). Для начала дадим определение объекта информатизации.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров [6.1].

Аттестация объектов информатизации (далее аттестация) - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России). Наличие аттестата соответствия в организации дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате.

Аттестация производится в порядке, установленном "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 года. Аттестация должна проводится до начала обработки информации, подлежащей защите. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте информатизации.

Аттестация является обязательной в следующих случаях:

государственная тайна;
при защите государственного информационного ресурса;
управление экологически опасными объектами;
ведение секретных переговоров.
Во всех остальных случаях аттестация носит добровольный характер, то есть может осуществляться по желанию заказчика или владельца объекта информатизации.

Аттестация предполагает комплексную проверку (аттестационные испытания) объекта информатизации в реальных условиях эксплуатации. Целью является проверка соответствия применяемых средств и мер защиты требуемому уровню безопасности. К проверяемым требованиям относится:

защита от НСД, в том числе компьютерных вирусов;
защита от утечки через ПЭМИН;

защита от утечки или воздействия на информацию за счет специальных устройств, встроенных в объект информатизации.
Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом, и состоит из следующего перечня работ:

анализ исходных данных по аттестуемому объекту информатизации;
предварительное ознакомление с аттестуемым объектом информатизации;
проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.
Органы по аттестации должны проходить аккредитацию ФСТЭК в соответствии с "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Все расходы по проведению аттестации возлагаются на заказчика, как в случае добровольной, так и обязательной аттестации.

Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации, а также за соблюдение авторских прав заказчика.

В структуру системы аттестации входят:

федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации – ФСТЭК России;
органы по аттестации объектов информатизации по требованиям безопасности информации;
испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).
В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации.

В качестве органов по аттестации могут выступать отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию.

Органы по аттестации:

аттестуют объекты информатизации и выдают "Аттестаты соответствия";
осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;
отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";
формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;
ведут информационную базу аттестованных этим органом объектов информатизации;
осуществляют взаимодействие с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.
ФСТЭК осуществляет следующие функции в рамках системы аттестации:

организует обязательную аттестацию объектов информатизации;
создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;
устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;
аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;
осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;
рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации;
организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.
Испытательные лаборатории проводят испытания несертифицированной продукции, используемой на аттестуемом объекте информатизации.

Со списком органов по аттестации и испытательных лабораторий, прошедших аккредитацию, можно ознакомиться на официальном сайте ФСТЭК России в разделе "Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации".

Заявители:

проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;
привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;
предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;
привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";
извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");
предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.
Для проведения испытаний заявитель предоставляет органу по аттестации следующие документы и данные:

приемо-сдаточную документацию на объект информатизации;
акты категорирования выделенных помещений и объектов информатизации;
инструкции по эксплуатации средств защиты информации;
технический паспорт на аттестуемый объект;
документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;
сертификаты соответствия требованиям безопасности информации на ВТСС;
сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;
акты на проведенные скрытые работы;
протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);
протоколы измерения величины сопротивления заземления;
протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
данные по уровню подготовки кадров, обеспечивающих защиту информации;
данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;
нормативную и методическую документацию по защите информации и контролю эффективности защиты.
Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией.

пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;

перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
технологические поэтажные планы здания с указанием мест расположения объектов информатизации и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;
планы объектов информатизации с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
план-схему инженерных коммуникаций всего здания, включая систему вентиляции;
план-схему системы заземления объекта с указанием места расположения заземлителя;
план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
схемы систем активной защиты (если они предусмотрены)[6.3].
Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов информатизации по требованиям безопасности". Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.
предварительное ознакомление с аттестуемым объектом – производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;
испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.
разработка программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.
заключение договоров на аттестацию. Результатом предыдущих четырех этапов становится заключение договора между заявителем и органом по аттестации, заключением договоров между органом по аттестации и привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.
проведение аттестационных испытаний объекта информатизации. В ходе аттестационных испытаний выполняется следующее:

анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;
проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации[6.2]
К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протокол аттестационных испытаний должен включать:

вид испытаний;
объект испытаний;
дату и время проведения испытаний;
место проведения испытаний;
перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
перечень нормативно-методических документов, в соответствии с которыми проводились испытания;
методику проведения испытания (краткое описание);
результаты измерений;
результаты расчетов;
выводы по результатам испытаний [6.4]
Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов.

Заключение по результатам аттестации подписывается членами аттестационной комиссии, утверждается руководителем органа аттестации и представляется заявителю [2]. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

оформление, регистрация и выдача "Аттестата соответствия" (если заключение по результатам аттестации утверждено).

осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
рассмотрение апелляций. В случае, если заявитель не согласен с отказом в выдаче "Аттестата соответствия", он может подать апелляцию в вышестоящий орган по аттестации или в ФСТЭК. Апелляция рассматривается в срок, не превышающий один месяц с привлечением заинтересованных сторон.
Аттестат соответствия должен содержать:

регистрационный номер;
дату выдачи;
срок действия;
наименование, адрес и местоположение объекта информатизации;
категорию объекта информатизации;
класс защищенности автоматизированной системы;
гриф секретности (конфиденциальности) информации, обрабатываемой на объекте информатизации;
организационную структуру объекта информатизации и вывод об уровне подготовки специалистов по защите информации;
номера и даты утверждения программы и методики, в соответствии с которыми проводились аттестационные испытания;
перечень руководящих документов, в соответствии с которыми проводилась аттестация;
номер и дата утверждения заключения по результатам аттестационных испытаний;
состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических средств защиты информации, а также схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств;
организационные мероприятия, при проведении которых разрешается обработка информации ограниченного доступа;
перечень действий, которые запрещаются при эксплуатации объекта информатизации;
список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и средств защиты информации.
Аттестат соответствия подписывается руководителем аттестационной комиссии и утверждается руководителем органа по аттестации.

Аттестат соответствия выдается на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.