Утверждено
Приказом председателя
Государственной технической
комиссии при Президенте
Российской Федерации
от 27 октября 1995 г. N 199

ПОЛОЖЕНИЕ О СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Настоящее положение устанавливает организационную структуру Системы сертификации средств защиты информации по требованиям безопасности информации, функции субъектов сертификации, порядок сертификации, государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, общие требования к нормативным и методическим документам по сертификации средств защиты информации. В приложениях к настоящему Положению приведены перечень средств защиты информации, подлежащих сертификации в системе сертификации, формы заявок на проведение сертификации и продление срока действия сертификата, решения по заявке на проведение сертификации (продлению срока действия сертификата), сертификата и лицензии на применение знака соответствия.

1. Общие положения

1.1. Положение разработано в соответствии с Законом Российской Федерации от 10 июня 1993 г. N 5151-1 "О сертификации продукции и услуг" с изменениями и дополнениями, внесенными Федеральными законами от 27 декабря 1995 г. N 211-ФЗ, от 2 марта 1998 г. N 30-ФЗ, от 31 июля 1998 г. N 154-ФЗ (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, N 26, ст. 966; Собрание законодательства Российской Федерации, 1996, N 1, ст. 4; 1998, N 10, ст. 1143; 1998, N 31, ст. 3832), Законом Российской Федерации от 21 июля 1993 г. N 5485-1 "О государственной тайне", с изменениями и дополнениями, внесенными Постановлением Конституционного Суда Российской Федерации от 27 марта 1996 г. N 8-П, Федеральным законом от 6 октября 1997 г. N 131-ФЗ (Российская газета, от 21 сентября 1993 г., N 182; Собрание законодательства Российской Федерации, 1996, N 15, ст. 1768; Российская газета, от 9 октября 1997 г., N 196), Федеральным законом от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" (Собрание законодательства Российской Федерации, 1995, N 8, ст. 609),

Законом Российской Федерации от 7 февраля 1992 г. N 2300/1-1 "О защите прав потребителей" с изменениями и дополнениями, внесенными Федеральным законом от 9 января 1996 г. N 2-ФЗ (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, N 15, ст. 766; Собрание законодательства Российской Федерации, 1996, N 3, ст. 140), Федеральным законом "Об участии в международном информационном обмене" от 4 июля 1996 г. N 85-ФЗ, Указов Президента Российской Федерации от 19 февраля 1999 г. N 212 и от 29 ноября 1999 г. N 1567, Постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" с изменениями и дополнениями, внесенными Постановлениями Правительства Российской Федерации от 23 апреля 1996 г. N 509, от 29 марта 1999 г. N 342 (Собрание законодательства Российской Федерации, 1995, N 27, ст. 2579; 1996, N 18, ст. 2142; 1999, N 14, ст. 1722), на основании Правил по проведению сертификации в Российской Федерации, утвержденных Постановлением Госстандарта России от 16 февраля 1994 г. N 3 и зарегистрированных в Министерстве юстиции Российской Федерации 21 марта 1994 г., регистрационный номер 521 (Российские вести, от 30 марта 1994 г., N 56), и Порядка проведения сертификации продукции в Российской Федерации, утвержденного Постановлением Госстандарта России от 21 сентября 1994 г. N 15 и зарегистрированного в Министерстве юстиции Российской Федерации 5 апреля 1995 г., регистрационный номер 826 (Российские вести, от 1 июня 1995 г., N 100), с изменениями и дополнениями, внесенными Постановлением Госстандарта России от 25 июля 1996 г. N 15 и зарегистрированными в Министерстве юстиции Российской Федерации 1 августа 1996 г., регистрационный номер 1139 (Российские вести, от 8 августа 1996 г., N 147).

1.2. Настоящее Положение устанавливает основные принципы, организационную структуру системы обязательной сертификации средств защиты информации, порядок проведения сертификации этих средств по требованиям безопасности информации, а также государственного контроля и надзора за сертификацией и сертифицированными средствами защиты информации.

Действие настоящего положения распространяется на технические, программные и другие средства защиты информации, предназначенные для защиты информации, содержащей сведения, составляющие государственную тайну, от утечки, несанкционированных и непреднамеренных воздействий, несанкционированного доступа и от технической разведки, а также средства контроля эффективности защиты информации.

Под сертификацией средств защиты информации по требованиям безопасности информации (далее - сертификацией) понимается деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России).

1.3. Система сертификации средств защиты информации по требованиям безопасности информации включает в себя аттестацию объектов информатизации <*> по требованиям безопасности информации.

Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации, правила проведения, а также другие вопросы аттестации определяются "Положением по аттестации объектов информатизации по требованиям безопасности информации".

1.4. Деятельность системы сертификации средств защиты информации по требованиям безопасности информации организует Гостехкомиссия России в пределах ее компетенции, определенной законодательными и иными нормативными актами Российской Федерации.

1.5. Целями создания системы сертификации являются:

реализация требований статьи 28 Закона Российской Федерации "О государственной тайне";

реализация требований государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам;

создание условий для качественного и эффективного обеспечения потребителей сертифицированной техникой защиты информации;

обеспечение национальной безопасности Российской Федерации в информационной сфере;

содействие формированию рынка защищенных информационных технологий и средств их обеспечения;

формирование и осуществление единой научно-технической и промышленной политики в информационной сфере с учетом современных требований по противодействию техническим разведкам и технической защите информации.

1.6. Обязательной сертификации подлежат средства защиты информации <**>, предназначенные для защиты сведений, составляющих государственную тайну, а также другой информации с ограниченным доступом, подлежащей защите в соответствии с действующим законодательством, систем управления экологически опасными производствами, объектами, имеющими важное оборонное или экономическое значение и влияющими на безопасность государства, средства общего применения, предназначенные для противодействия техническим разведкам. Перечень средств защиты информации, подлежащей обязательной сертификации, приведен в Приложении N 1 к настоящему Положению. В остальных случаях сертификация носит добровольный характер (добровольная сертификация) и осуществляется по инициативе заявителя (разработчика, изготовителя, поставщика или потребителя) средств защиты информации.

1.7. Основными схемами сертификации средств защиты информации являются:

для единичных образцов средств защиты информации - проведение испытаний образца на соответствие требованиям по безопасности информации;

для партии средств защиты информации - проведение испытаний репрезентативной выборки образцов средств на соответствие требованиям по безопасности информации;

для серийного производства средств защиты информации - проведение типовых испытаний образцов продукции на соответствие требованиям по безопасности информации и последующий инспекционный контроль за стабильностью характеристик сертифицированной продукции, обеспечивающих (определяющих) выполнение этих требований. Кроме того, по решению федерального органа по сертификации допускается предварительная проверка (аттестация) производства по утвержденной программе. По согласованию с федеральным органом по сертификации могут быть использованы и другие схемы сертификации, включая применяемые в международной практике.

1.8. Сертификация средств защиты информации осуществляется федеральным и аккредитованными органами по сертификации. Сертификационные испытания проводятся аккредитованными испытательными центрами (лабораториями) на их материально-технической базе. В отдельных случаях по согласованию с федеральным органом по сертификации (или органом по сертификации) допускается проведение испытаний на испытательной базе заявителя данного средства защиты информации.

Правила аккредитации определяются действующим в системе "Положением об аккредитации испытательных центров (лабораторий) и органов по сертификации средств защиты информации".

1.9. Оплата работ по сертификации средств защиты информации производится заявителем на основании договоров между участниками сертификации. Сумма средств, израсходованных заявителем на проведение сертификации средств защиты информации, относится на их себестоимость.

1.10. Органы по сертификации и испытательные центры (лаборатории) несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственной тайны, конфиденциальных сведений, материальных ценностей, предоставленных заявителем, а также за соблюдение авторских прав разработчика при испытаниях его средств защиты информации.

2. Организационная структура системы сертификации

2.1. Организационную структуру системы сертификации образуют:

федеральный орган по сертификации средств защиты информации (Гостехкомиссия России);

центральный орган системы сертификации средств защиты информации;

органы по сертификации средств защиты информации;

испытательные центры (лаборатории);

заявители.

2.2. Федеральный орган по сертификации средств защиты информации в пределах своей компетенции осуществляет следующие функции:

создает и совершенствует систему сертификации средств защиты информации по требованиям безопасности информации и устанавливает правила проведения сертификации средств защиты информации;

определяет перечень средств защиты информации, подлежащих обязательной сертификации в данной системе;

утверждает нормативные документы, на соответствие требованиям которых проводится сертификация средств защиты информации в системе, и методические документы по проведению сертификационных испытаний;

согласовывает с Межведомственной комиссией по защите государственной тайны положение о сертификации средств защиты информации по требованиям безопасности информации, перечень средств защиты информации, подлежащих обязательной сертификации, нормативные документы, на соответствие требованиям которых проводится сертификация средств защиты информации в системе;

представляет на государственную регистрацию в Госстандарт России и Минюст России систему сертификации и знак соответствия;

организует функционирование системы сертификации средств защиты информации по требованиям безопасности информации;

определяет центральный орган системы сертификации средств защиты информации (при его необходимости) или выполняет функции этого органа;

устанавливает правила аккредитации органов по сертификации, испытательных центров (лабораторий) и органов по аттестации объектов информатизации по требованиям безопасности информации;

аккредитует органы по сертификации, испытательные центры (лаборатории) и органы по аттестации объектов информатизации;

организует и финансирует разработку нормативных и методических документов системы сертификации средств защиты информации по требованиям безопасности информации;

рассматривает заявки на сертификацию, принимает по ним решения, определяет схему проведения сертификации средств защиты информации и испытательный центр (лабораторию) с учетом предложений заявителя и назначает орган по сертификации;

проводит экспертизу технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний, оформляет экспертные заключения при проведении сертификации средств защиты информации федеральным органом по сертификации;

выдает сертификаты и лицензии на применение знака соответствия;

ведет государственный реестр участников и объектов сертификации;

осуществляет государственный контроль и надзор, устанавливает порядок инспекционного контроля за соблюдением правил сертификации и за сертифицированными средствами защиты информации;

рассматривает апелляции по вопросам сертификации;

организует периодическую публикацию информации о сертификации;

организует подготовку и аттестацию экспертов-аудиторов;

осуществляет взаимодействие с соответствующими уполномоченными органами других стран и международных организаций по вопросам сертификации, принимает решение о признании международных и зарубежных сертификатов;

приостанавливает, продлевает либо отменяет действие выданных сертификатов.

Федеральный орган по сертификации может передавать некоторые из своих функций центральному органу системы сертификации или органам по сертификации.

2.3. Центральный орган системы сертификации средств защиты информации:

координирует деятельность органов по сертификации и испытательных центров (лабораторий), входящих в систему;

разрабатывает предложения по номенклатуре средств защиты информации, сертифицируемых в системе сертификации, и представляет их в федеральный орган по сертификации;

участвует в работах по совершенствованию фонда нормативных документов, на соответствие требованиям которых проводится сертификация средств защиты информации в системе, и методических документов по проведению сертификационных испытаний;

участвует в рассмотрении апелляций по поводу действий органов по сертификации и испытательных центров (лабораторий), входящих в систему;

участвует в аккредитации органов по сертификации, испытательных центров (лабораторий) по сертификации средств защиты информации и органов по аттестации объектов информатизации;

ведет учет входящих в систему органов по сертификации, испытательных центров (лабораторий), органов по аттестации объектов информатизации, выданных и аннулированных сертификатов и лицензий на применение знака соответствия, нормативных и методических документов, содержащих правила, требования, методики и рекомендации по сертификации;

обеспечивает участников сертификации информацией о деятельности системы и готовит необходимые материалы для опубликования.

2.4. Органы по сертификации средств защиты информации в пределах установленной области аккредитации:

участвуют в определении схемы проведения сертификации средств защиты информации с учетом предложений заявителя;

уточняют требования, на соответствие которым проводятся сертификационные испытания;

рекомендуют заявителю испытательный центр (лабораторию);

утверждают программы и методики проведения сертификационных испытаний;

проводят экспертизу технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний;

оформляют экспертное заключение по сертификации средств защиты информации и представляют их в федеральный орган по сертификации;

организуют, при необходимости, предварительную проверку (аттестацию) производства сертифицируемых средств защиты информации;

участвуют в аккредитации испытательных центров (лабораторий) и органов по аттестации объектов информатизации;

организуют инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации и участвуют в инспекционном контроле за деятельностью испытательных центров (лабораторий);

хранят документацию (оригиналы), подтверждающую сертификацию средств защиты информации;

ходатайствуют перед федеральным органом по сертификации о приостановке или отмене действия выданных сертификатов;

формируют и актуализируют фонд нормативных и методических документов, необходимых для сертификации, участвуют в их разработке;

представляют заявителю необходимую информацию по сертификации.

2.5. Испытательные центры (лаборатории) в пределах установленной области аккредитации:

осуществляют отбор образцов средств защиты информации для проведения сертификационных испытаний;

разрабатывают программы и методики сертификационных испытаний, осуществляют сертификационные испытания средств защиты информации, оформляют протоколы сертификационных испытаний и технические заключения;

маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном правилами системы сертификации;

участвуют в аттестации производства сертифицируемых средств защиты информации.

Испытательные центры (лаборатории) несут ответственность за полноту испытаний средств защиты информации, достоверность, объективность и требуемую точность измерений, своевременную поверку средств измерений и аттестацию испытательного оборудования.

2.6. Заявители:

обеспечивают соответствие средств защиты информации требованиям нормативных документов в системе сертификации;

осуществляют подготовку производства и принимают меры для обеспечения стабильности характеристик сертифицируемых средств защиты информации, обеспечивающих (определяющих) выполнение требований по защите информации;

указывают в технической документации сведения о сертифицируемой технике защиты информации, нормативных документах, которым она

должна соответствовать, обеспечивают доведение этой информации до потребителя;

маркируют производимую сертифицированную технику защиты информации знаком соответствия в порядке, установленном правилами системы сертификации;

применяют сертификат, руководствуясь законодательными актами Российской Федерации и правилами системы сертификации;

извещают орган по сертификации и испытательный центр (лабораторию), проводившие сертификацию, о всех изменениях в технологии, конструкции (составе) сертифицированных средств защиты информации для принятия решения о необходимости проведения повторной сертификации;

обеспечивают доступ в организацию, к технической и технологической документации, технологическим процессам, местам хранения сертифицированной продукции должностных лиц органов, осуществляющих государственный контроль и надзор, инспекционный контроль за сертифицированными средствами защиты информации;

приостанавливают или прекращают реализацию средств защиты информации, если они не отвечают требованиям нормативных документов, а также по истечении срока действия сертификата, при приостановке его действия или отмены;

при обнаружении несоответствия сертифицированных средств защиты информации требованиям нормативных документов осуществляют доработку этих средств и представляют их на сертификацию.

Разработчики, изготовители и поставщики средств защиты информации должны иметь соответствующую лицензию Гостехкомиссии России.

2.7. Органы по сертификации, испытательные центры (лаборатории) и органы по аттестации объектов информатизации должны быть юридическими лицами, располагать подготовленными специалистами, необходимыми средствами измерений, испытательным оборудованием и методиками испытаний, нормативными документами для проведения испытаний средств защиты информации в соответствии с областью аккредитации.

Аккредитация производится только при наличии соответствующих лицензий.

3. Процедура сертификации и контроля

3.1. Процедура сертификации включает:

подачу и рассмотрение заявки на проведение сертификации (продление срока действия сертификата) средств защиты информации;

сертификационные испытания средств защиты информации и (при необходимости) аттестацию их производства;

экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия;

осуществление государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации;

информирование о результатах сертификации средств защиты информации;

рассмотрение апелляций.

3.2. Подача и рассмотрение заявки на проведение сертификации средств защиты информации.

3.2.1. Заявитель для получения сертификата направляет в федеральный орган по сертификации заявку (Приложение 2) на проведение сертификации. Заявка оформляется на бланке заявителя и заверяется печатью.

3.2.2. Федеральный орган по сертификации в месячный срок после получения заявки направляет заявителю, в назначенные для проведения сертификации орган по сертификации и испытательный центр (лабораторию) решения по заявке на проведение сертификации (Приложение 3). Орган по сертификации и испытательный центр (лаборатория) могут быть изменены по согласованию с заявителем.

После получения решения заявитель обязан представить в испытательный центр (лабораторию) средства защиты информации в комплектации, согласно техническим условиям, или формуляру на средство защиты, а также комплект необходимой технической и эксплуатационной документации на это средство в соответствии с ЕСКД или ЕСПД.

3.3. Сертификационные испытания средств защиты информации и аттестация их производства.

3.3.1. Сертификационные испытания средств защиты информации проводятся в испытательных центрах (лабораториях) на образцах, конструкция, состав и технология изготовления которых должны быть аналогичны образцам средств защиты информации, поставляемым потребителю, по программам и методикам испытаний, утвержденным органом по сертификации.

Количество образцов, порядок их отбора и идентификации должен соответствовать требованиям нормативных и методических документов.

В случае отсутствия на момент сертификации испытательных центров (лабораторий) с соответствующей областью аккредитации федеральный орган по сертификации определяет возможность, место и условия проведения испытаний, обеспечивающих объективность их результатов.

3.3.2. Сроки проведения испытаний устанавливаются договором между заявителем и испытательным центром (лабораторией).

3.3.3. По просьбе заявителя его представителям должна быть предоставлена возможность ознакомиться с условиями хранения и испытаний средств защиты информации и предоставленной документации на эти средства в испытательном центре (лаборатории).

3.3.4. По результатам испытаний оформляются протоколы и технические заключения, которые направляются испытательным центром (лабораторией) в орган по сертификации, а копия технического заключения - заявителю.

3.3.5. При внесении изменений в конструкцию (состав) средств защиты информации или технологию их производства заявитель (разработчик, изготовитель) извещает об этом орган по сертификации. Последний принимает решение о необходимости проведения новых сертификационных испытаний этих средств.

3.3.6. Сертификация средств защиты информации зарубежного производства проводится по тем же правилам, что и отечественной.

3.4. Экспертиза результатов сертификационных испытаний, оформление, регистрация и выдача сертификата и лицензии на право использования знака соответствия.

3.4.1. Орган по сертификации проводит экспертизу результатов испытаний и оформляет экспертное заключение, которое вместе с техническим заключением, материалами сертификационных испытаний, комплектом необходимой технической и эксплуатационной документации на средство защиты информации направляет в федеральный орган по сертификации.

3.4.2. Сроки проведения экспертизы результатов сертификационных испытаний устанавливаются договором между заявителем и органом по сертификации.

3.4.3. После согласования технических условий или формуляра на средства защиты информации и присвоения сертификату регистрационного номера федеральный орган по сертификации оформляет сертификат (Приложение 4) и выдает его заявителю. Срок действия сертификата - три года.

При несоответствии результатов испытаний требованиям нормативных документов федеральный орган по сертификации принимает решение об отказе в выдаче сертификата и направляет заявителю мотивированное заключение. В случае несогласия с отказом в выдаче сертификата заявитель имеет право обратиться в апелляционный совет федерального органа по сертификации для дополнительного рассмотрения материалов сертификации.

КонсультантПлюс: примечание.

Нумерация подпунктов дана в соответствии с официальным текстом документа.

3.4.5. Получение изготовителем средств защиты информации сертификата дает ему право получить в федеральном органе по сертификации лицензию (Приложение 5) на применение знака соответствия.

В случае сертификации единичных образцов или партии средств защиты информации лицензия на применение знака соответствия заявителю не выдается. Маркирование знаками соответствия средств защиты информации

в этом случае производится испытательной лабораторией, проводившей сертификационные испытания.

Владелец лицензии на применение знака соответствия несет ответственность за поставку маркированных средств защиты информации.

3.5. Государственный контроль и надзор, инспекционный контроль за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации.

3.5.1. Государственный контроль и надзор за соблюдением заявителями, испытательными центрами (лабораториями), органами по сертификации правил обязательной сертификации и за сертифицированными средствами защиты информации осуществляет федеральный орган по сертификации. Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации, действующей в системе сертификации.

3.5.2. Инспекционный контроль за сертифицированными средствами защиты информации осуществляют федеральный орган по сертификации, органы по сертификации, проводившие их сертификацию, с привлечением испытательных центров (лабораторий), проводивших сертификационные испытания. Общие правила инспекционного контроля за сертифицированными средствами защиты информации устанавливаются в нормативных и методических документах системы сертификации средств защиты информации по требованиям безопасности информации. Периодичность и объемы испытаний в рамках инспекционного контроля сертифицированных средств защиты информации в испытательных центрах (лабораториях) должны предусматриваться в нормативных и методических документах по их сертификации.

3.5.3. По результатам контроля федеральный орган может приостановить или аннулировать действие сертификата и аттестата аккредитации, а орган по сертификации - ходатайствовать об этом. Решение об аннулировании действия сертификата принимается только в том случае, если в результате принятых незамедлительных мер не может быть восстановлено соответствие средств защиты информации установленным требованиям. Причинами, которые могут заставить принять такое решение, являются:

изменение нормативных и методических документов по защите информации в части 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.

3.5.4. Информация о приостановлении (аннулировании) действия сертификата или аттестата аккредитации доводится федеральным органом по сертификации до сведения изготовителей, потребителей средств защиты информации, органов по сертификации и испытательных центров (лабораторий).

3.6. Информирование о сертификации средств защиты информации.

3.6.1. Федеральный орган по сертификации обеспечивает участников сертификации необходимой информацией о деятельности системы сертификации, включающей:

перечень средств защиты информации (их сертифицированных параметров), на которые выданы сертификаты;

перечень средств защиты информации (их сертифицированных параметров), на которые действие сертификатов аннулировано;

перечень органов по сертификации;

перечень испытательных центров (лабораторий);

перечень органов по аттестации объектов информатизации;

перечень нормативных документов, на соответствие требованиям которых проводится сертификация средств защиты информации, и методических документов по проведению сертификационных испытаний.

3.7. Порядок продления срока действия сертификата.

Продление срока действия сертификата может проводиться по упрощенной схеме, включающей проверку конструкторской, технологической, эксплуатационной документации и условий производства сертифицированных средств защиты информации.

Заявитель для продления срока действия сертификата соответствия не позднее чем за три месяца до окончания срока его действия направляет в федеральный орган по сертификации заявку (Приложение 2А).

Федеральный орган по сертификации в месячный срок после получения заявки направляет заявителю, в назначенные для проведения сертификации орган по сертификации и испытательный центр (лабораторию) решение по заявке на проведение сертификации. Орган по сертификации и испытательная лаборатория выбираются, как правило, с учетом проведения предыдущих сертификационных испытаний.

3.8. При изменении требований к сертифицированным средствам защиты информации, их конструкции или условий производства проводится повторная сертификация, включающая действия, предусмотренные п. п. 3.1 - 3.4 настоящего Положения. При этом сертификация может проводиться по упрощенной схеме, а сертификационные испытания - по сокращенной программе. При этом могут осуществляться:

проверка основных характеристик сертифицированных средств защиты информации, обеспечивающих (определяющих) выполнение требований по защите информации;

сертификационные испытания характеристик сертифицированных средств защиты информации, обеспечивающих (определяющих) выполнение изменившихся или вновь предъявляемых требований по защите информации;

контроль технологии производства средств защиты информации.

Орган по сертификации и испытательная лаборатория выбираются, как правило, с учетом проведения предыдущих сертификационных испытаний.

3.9. Для признания зарубежного сертификата заявитель направляет его копию и заявку на признание сертификата в федеральный орган по сертификации, который в срок не позднее двух месяцев после получения заявки извещает заявителя о признании сертификата или необходимости проведения сертификационных испытаний. В случае признания зарубежного сертификата заявителю выдается сертификат установленного образца.

3.10. Рассмотрение апелляций.

Апелляция подается в апелляционный совет федерального органа по сертификации по вопросам, связанным с деятельностью испытательных центров (лабораторий) или органов по сертификации. Апелляция рассматривается в месячный срок с привлечением заинтересованных сторон и независимых экспертов. О принятом решении извещается податель апелляции.

4. Требования к нормативным и методическим документам по сертификации средств защиты информации

4.1. Сертификация средств защиты информации отечественного и зарубежного производства проводится на соответствие требованиям нормативных документов, действующих в системе сертификации средств защиты информации по требованиям безопасности информации, и в соответствии с утвержденными органом по сертификации программами и методиками сертификационных испытаний.

4.2. Тексты нормативных и методических документов, используемых при сертификации средств защиты информации, должны быть сформулированы ясно и четко, обеспечивая их точное и единообразное толкование. В разделе "Область применения" должно содержаться указание о возможности использования документа в целях сертификации.

4.3. В специальном разделе или путем ссылки на другой нормативный или методический документ должны быть установлены методы, условия, объем и порядок испытаний для определения показателей, характеристик и требований, проверяемых при сертификации. Содержание и изложение этих сведений должны быть таковы, чтобы свести к минимуму погрешности результатов испытаний и позволить квалифицированному персоналу любого испытательного центра (лаборатории) получать сопоставимые результаты.

Должна быть указана последовательность проведения испытаний, если эта последовательность влияет на результаты испытаний.

4.4. В разделе "Маркировка" должны содержаться требования, которые обеспечивают однозначную идентификацию сертифицированных средств защиты информации, а также указания о месте и способе нанесения знака соответствия.

4.5. Официальным языком системы сертификации средств защиты информации по требованиям безопасности информации является русский. Все нормативные и методические документы системы сертификации оформляются на русском языке.

Приложение 1

ПЕРЕЧЕНЬ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ПОДЛЕЖАЩИХ СЕРТИФИКАЦИИ В СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ГОСТЕХКОМИССИИ РОССИИ (N РОСС RU.0001.01БИ00)

Средства защиты информации	Код средств защиты информации по ОК 005-93(ОКП)	Код средств защиты информации по ТН ВЭД	Область применения средств защиты информации
1. Технические средства защиты информации от утечки по техническим каналам, доступа, представленных	66 5000 0	847100000	Защита информационных ресурсов ограниченного
	66 6000 0	847210000	

включая средства контроля			в виде носителей на
эффективности принятых мер	66 7000 0	847300000	магнитной или оптической
защиты информации, основные			основе, информативных
и вспомогательные	66 8000 0	851700000	физических полей,
технические средства и			информационных массивов и
системы в защищенном	67 0000 0	851800000	баз данных.
исполнении.		
Средства и системы|	|69 0000 0 |851900000 |информатизации (средства|	
вычислительной техники,|	|70 3000 0 |852000000 |информационно-		
вычислительные комплексы,|	|852100000 |сети и системы),|	
автоматизированные		|854000000 |системы управления,|	
системы связи, приема,|	|854100000 |передачи, обработки и|	
хранения информации|	|854200000 |(звукозаписи,		
звукоусиления,		
звуковоспроизведения,		
переговорных и		
телевизионных устройств,

средства изготовления, тиражирования документов и других технических средств обработки графической, смысловой и буквенно-цифровой информации), используемых для обработки информации ограниченного доступа. Технические средства и системы, не обрабатывающие информацию, размещенные в помещениях, где обрабатывается (циркулирует) информация, отнесенная к категории ограниченного доступа, а также сами помещения (выделенные помещения).		
1.1. Средства защиты Средства телевидения		

информации от перехвата		
(телевизионные системы и оптических сигналов		
аппаратура, системы и		
(изображений) в видимом,		
аппаратура видеозаписи		
инфракрасном и		
воспроизведения). Системы		
ультрафиолетовом диапазонах		
телевизионной охранной		
волн, осуществляемого		
сигнализации. Компоненты		
оптическими, оптико-		
вычислительной техники		
электронными,		
(терминалы ЭВМ и		
телевизионными,		
оконечных устройств		
тепловизионными		
автоматизированных		
(инфракрасными), лазерными,		
систем, печатающие		
фото и другими визуальными		
устройства ЭВМ и		
средствами съема		
оконечных устройств		
информации.		
автоматизированных		
систем). Промышленные		
объекты.		
1.2. Средства защиты		
Средства радио- и		
информации от перехвата		
кабельной связи,		
акустических сигналов,		
радиовещания и		
распространяющихся в		
телевидения видео- и		
воздушной, водной, твердой		
звукозаписывающей и		

средах, воспроизводящей техники и акустическими, гидроакустическими, (радиовещательная и виброакустическими, телевизионная аппаратура, лазерными и сейсмическими телефонная и телеграфная средствами.	осуществляемого		их компоненты
аппаратура, микрофоны, громкоговорители, аппаратура видеозаписи	телефоны,		и воспроизведения,
аппаратура звукозаписи и воспроизведения). Промышленные объекты.			
1.3. Электронно-вычислительная информации техника и ее компоненты (ЭВМ), вычислительные сети, системы и комплексы, устройства защиты, в т.ч. от перехвата телеобработки информации). Автоматизированные	Средства защиты от перехвата электромагнитных сигналов, возникающих при функционировании объектов побочных электромагнитных излучений и наводок		

(ПЭМИН), возникающих при		
системы. Программно-		
работе технических средств		
технические комплексы для		
обработки информации,		
автоматизации различных		
осуществляемого		
процессов. Средства		
магнитометрическими,		
радио- и кабельной связи,		
радио-, радиотехническими		
радиовещания и		
и радиолокационными		
телевидения, включая		
средствами.		
спутниковые системы и		
волоконно-оптические		
линии связи и их		
компоненты, а также		
средства видео-,		
звукозаписывающей и		
воспроизводящей техники и		
		ее
компоненты. Приборы и		
оборудование охранной и		
пожарной сигнализации.		
Промышленные объекты,		
образцы вооружения и		
военной техники.		
Программно-технические		
комплексы для		

автоматизации контроля и производственных испытаний средств вычислительной техники, связи и средств защиты информации, изделий радиоэлектроники и приборостроения. Средства автоматизации труда (электрические и автоматические пишущие машинки, копировально-множительная техника, в том числе ризографы).		
1.4. Средства защиты информации от перехвата электрических сигналов, распространяющихся в токопроводящих коммуникациях и являющихся причиной электромагнитной		

наводки за счет побочных электромагнитных излучений технических средств обработки информации или следствием эффекта электроакустического преобразования сигналов вспомогательными техническими средствами и системами.			
1.5. Средства защиты информации от деятельности радиационной разведки по добыванию сведений за счет изменения естественного радиационного фона окружающей среды, возникающего при функционировании объекта защиты.			

1.6. Средства защиты информации от деятельности химической разведки по получению сведений за счет изменения химического состава окружающей среды, возникающего при функционировании объекта защиты.			
1.7. Средства защиты информации от возможности получения сведений магнитометрической разведкой за счет изменения локальной структуры магнитного поля Земли, возникающего вследствие деятельности объекта защиты.			
2. Средства защиты			

информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности.		
2.1. Средства пассивной защиты, в том числе: замки (с управлением от микропроцессора, радиоуправляемые и т.п.); электрические датчики разных типов; телевизионные системы охраны и контроля; СВЧ и радиолокационные системы; лазерные системы; оптические и инфракрасные системы; акустические системы; кабельные системы; устройства идентификации; ограждения;		

средства обнаружения нарушителя или нарушающего воздействия; специальные средства для транспортировки и хранения физических носителей информации (кассет стриммеров, магнитных и оптических дисков и т.п.).			
2.2. Средства защиты от подделки документов на основе оптико-химических технологий.			
2.3. Программы, обеспечивающие разграничение доступа к информации.			
2.4. Программы идентификации и			

аутентификации терминалов и пользователей.		
2.5. Программы контроля целостности информационных массивов.		
2.6. Антивирусные программы.		
2.7. Программы уничтожения остаточной информации в запоминающих устройствах.		
2.8. Программы контроля и восстановления файловой структуры на внешних запоминающих устройствах.		
2.9. Программы имитации работы системы или ее блокировки при обнаружении		

фактов НСД.			
2.10. Средства защиты, встроенные в операционные системы, системы управления базами данных и пакеты прикладных программ.			
2.11. Программы предотвращения несанкционированного копирования информации.			

КонсультантПлюс: примечание.
Нумерация пунктов в таблице дана в соответствии с официальным текстом документа.

2.15. Межсетевые экраны.			
2.16. Средства стирания данных.			
2.17. Средства локализации			

электронных закладок.			
2.18. Средства предотвращения несанкционированного копирования информации.			
2.19. Средства автоматизированного анализа защищенности, обнаружения атак и уязвимостей АС и СВТ.			
2.20. Средства управления доступом в локальные вычислительные сети на основе виртуальных локальных сетей.			
2.21. Средства, реализующие виртуальные частные сети поверх глобальных и			

локальных вычислительных сетей.		
2.22. Базовая система ввода/вывода (BIOS).		
2.23. Система управления потоками информации в цифровых АТС.		
2.24. Программные средства идентификации изготовителя программного (информационного) продукта, средства идентификации авторского права.		
3. Средства контроля эффективности применения средств защиты информации.		
4. Защищенные программные		

средства обработки информации.			
4.1. Пакеты прикладных программ.			
4.2. Программные средства, входящие в состав автоматизированных систем управления.			
5. Программные средства общего назначения.			
5.1. Операционные системы.			
5.2. Системы управления базами данных.			
5.3. Компиляторы.			
5.4. Средства разработки			

программного обеспечения.			
5.5. Редакторы текстовые и графические.			
6. Контрольно-кассовые машины (ККМ).			

Приложение 2

Кому (наименование федерального органа по сертификации, адрес)

ЗАЯВКА
на проведение сертификации средств защиты
информации в системе сертификации средств защиты
информации по требованиям безопасности
информации N РОСС RU.0001.01БИ00
(наименование заявителя, адрес)

просит провести сертификацию следующей продукции:
(наименование продукции, код ОКП, шифр) на соответствие требованиям (наименование нормативных и методических документов)

Заявитель предлагает провести испытания продукции по схеме (указывается схема сертификации) в (наименование испытательного центра (лаборатории))

Заявитель обязуется:

выполнять все условия сертификации;

обеспечивать стабильность сертифицированных характеристик средств защиты информации, маркированных знаком соответствия;

оплатить все расходы по проведению сертификации.

Дополнительные условия или сведения для договора:

а) предварительную проверку производства предлагаем провести в период

_____

место печати дата, подпись Фамилия И.О.

Приложение 2А

Кому (наименование федерального органа по сертификации, адрес)

ЗАЯВКА
на продление срока действия сертификата на средство
защиты информации в системе сертификации средств защиты
информации по требованиям безопасности информации
N РОСС RU.0001.01БИ00

(наименование заявителя, адрес) просит продлить срок действия сертификата:

(номер сертификата, дата выдачи) на (наименование сертифицированного СЗИ, код ОКП, шифр) на соответствие требованиям (наименование нормативных и методических документов)

Заявитель предлагает провести сертификацию в (наименование органа по сертификации) и (наименование испытательного центра (лаборатории))

Заявитель обязуется:

выполнять все условия сертификации;

обеспечивать стабильность сертифицированных характеристик средств защиты информации, маркированных знаком соответствия;

оплатить все расходы по проведению сертификации.

Дополнительные условия или сведения для договора:

а) проверку аттестованного производства предлагаем провести в период

_____

место печати дата, подпись Фамилия И.О.

Приложение 3

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ

ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
N РОСС RU.0001.01БИ00

РЕШЕНИЕ

от "__" _____ 20__ г.

по заявке на проведение сертификации

По заявке (наименование заявителя) на сертификацию (наименование продукции, код ОКП, ТУ) принято решение:

1. Сертификацию провести по схеме (указывается схема сертификации)
2. Испытания сертифицируемой продукции провести в (наименование испытательного центра (лаборатории), адрес)
3. Сертификацию провести на соответствие требованиям (наименование нормативных и методических документов)
4. Инспекционный контроль осуществлять (наименование организации, адрес) с периодичностью, установленной руководящими документами
5. Работы провести на основе (хозяйственный договор, тариф, другие варианты оплаты)
6. Экспертизу результатов сертификационных испытаний провести в (наименование органа по сертификации, адрес)

дата, подпись Фамилия И.О.

Приложение 3А

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
N РОСС RU.0001.01БИ00

РЕШЕНИЕ

от "__" _____ 20__ г.

по заявке на продление срока действия сертификата

По заявке (наименование заявителя) на продление срока действия сертификата N _____ от _____ на (наименование сертифицированной продукции, код ОКП, ТУ) принято решение:

1. Сертификацию провести по схеме (указывается схема сертификации (испытания единичного образца, партии образцов))

2. Испытания сертифицируемой продукции провести в (наименование испытательного центра (лаборатории), адрес)

3. Сертификацию провести на соответствие требованиям (наименование нормативных и методических документов)

4. Инспекционный контроль осуществлять (наименование организации, адрес) с периодичностью, установленной руководящими документами

5. Работы провести на основе (хозяйственный договор, тариф, другие варианты оплаты)

6. Экспертизу результатов сертификационных испытаний провести в (наименование органа по сертификации, адрес)

7. Проверку аттестованного производства провести (наименование органа по сертификации (испытательного центра (лаборатории)), адрес)

дата, подпись Фамилия И.О.

Приложение 4

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

место знака соответствия N РОСС RU.0001.01БИ00

СЕРТИФИКАТ

N _____

Выдан "__" _____ 20__ г.

Действителен до "__" _____ 20__ г.

Настоящий сертификат удостоверяет, что:

(наименование средств защиты информации, код, N ТУ) является (наименование по перечню средств защиты информации)

соответствует требованиям (наименование нормативных документов, на соответствие которым проведены сертификационные испытания)

Сертификат выдан на основании результатов сертификационных испытаний, проведенных (наименование испытательного центра (лаборатории)) и экспертного заключения (наименование органа по сертификации)

Заявитель (наименование организации-заявителя, адрес, телефон)

Маркирование (контроль маркирования) знаками соответствия и инспекционный контроль соответствия сертифицированной продукции требованиям руководящих документов Гостехкомиссии России осуществляется (наименование испытательного центра (лаборатории))

место гербовой печати дата, подпись Фамилия И.О.

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 21 февраля 2000 г.

Приложение 5

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

место знака соответствия N РОСС RU.0001.01БИ00

ЛИЦЕНЗИЯ

на применение знака соответствия

N _____

Выдана "__" _____ 20__ г.

Действительна до "__" _____ 20__ г.

Настоящая сертификационная лицензия выдана (наименование предприятия-изготовителя, адрес) на применение знака соответствия для маркирования (наименование вида продукции)

место гербовой печати дата, подпись Фамилия И.О.