КОНСПЕКТ ЛЕКЦИЙ К РАЗДЕЛУ 3. Сертификация ИТ-продуктов

Содержание лекции:

1. Основные понятия и термины в области сертификации
2. Обязательная сертификация.
3. Добровольная сертификация.
3. Методология принятия решений о допустимости выдачи сертификата.

.

ОСНОВНЫЕ ПОНЯТИЯ И ТЕРМИНЫ В ОБЛАСТИ СЕРТИФИКАЦИИ

В первой главе было дано определение собственно понятию ***сертификация*** и понятию ***сертификат соответствия***. Ниже приводятся еще несколько терминов, знание которых необходимо для понимания сущности процедуры сертификации.

Система сертификации - система, располагающая собственными правилами процедуры и управления для проведения сертификации.

Орган по сертификации - орган, проводящий сертификацию соответствия. Орган по сертификации может сам проводить испытания или же осуществлять надзор за этой деятельностью, проводимой по его поручению другими органами.

Испытательная лаборатория - лаборатория (центр), который проводит испытания в процессе сертификации.

Аккредитация (испытательной лаборатории или органа по сертификации) - процедура, посредством которой уполномоченный в соответствии с законодательными актами Российской Федерации орган официально признает возможность выполнения испытательной лабораторией или органом по сертификации конкретных работ в заявленной области.

Знак соответствия (в области сертификации) - защищенный в установленном порядке знак, применяемый или выданный в соответствии с правилами системы сертификации, указывающий, что обеспечивается необходимая уверенность в том, что данная продукция, процесс или услуга соответствует конкретному стандарту или другому нормативному документу.

Технические условия (ТУ) - документ, устанавливающий технические требования, которым должна удовлетворять продукция, процесс или услуга. ТУ могут быть стандартом, частью стандарта или самостоятельным документом.

В Законе "О сертификации продукции и услуг" определены два вида сертификации: ***обязательная*** **и** ***добровольная.*** Обязательной сертификации подлежит продукция, включенная в перечни, определяемые соответствующими нормативными документами.

Организационная структура системы сертификации в России включает: государственный (национальный) орган по сертификации, ведомственные органы по управлению сертификацией продукции определенных классов, а также испытательные центры (лаборатории). Основными функциями государственного органа по сертификации являются организация, координация, научно-методическое, информационное и нормативно-техническое обеспечение работ по испытаниям и сертификации, а также аккредитация центров сертификационных испытаний в соответствии с полномочиями национального органа по сертификации. Ведомственные органы сертификации выполняют те же функции в ограниченном

объеме для конкретных видов продукции.

Национальным органом по сертификации продукции в Российской Федерации является Госстандарт России, который осуществляет следующие функции:

• организует ведение обязательной сертификации продукции по поручению органов законодательной или исполнительной власти;

• организует и финансирует разработку, а также утверждает основополагающие нормативно-технические и методические документы системы сертификации;

• утверждает документы, устанавливающие порядок сертификации конкретных видов продукции;

• проводит аккредитацию испытательных центров (лабораторий) совместно с ведомственными органами по сертификации и выдает аттестат аккредитации;

• признает иностранные сертификаты соответствия, осуществляет взаимодействие с соответствующими уполномоченными органами других стран и международных организаций по вопросам сертификации;

• регистрирует и аннулирует сертификаты соответствия и сертификационные лицензии, рассматривает спорные вопросы, возникающие в процессе сертификации;

• организует периодическую публикацию информации по сертификации.

Основой сертификации продукции в Российской Федерации является Система сертификации ГОСТ Р Госстандарта России. Этой системой, в частности, определяются правила создания и регистрации ведомственных систем сертификации для конкретных классов продукции.

ОРГАНИЗАЦИЯ РАБОТ ПО СЕРТИФИКАЦИИ СРЕДСТВ И СИСТЕМ ИНФОРМАТИЗАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В соответствии с действующими законодательными и нормативными документами сертификация средств информатизации проводится в Российской Федерации в следующих основных направлениях:

• ***обязательная сертификация*** средств информатизации на соответствие требованиям электромагнитной совместимости, а также требованиям, обеспечивающим безопасность жизни, здоровья, имущества потребителей и охрану среды обитания;

• ***обязательная сертификация*** средств защиты информации;

• ***добровольная сертификация*** функциональных параметров средств и систем информатизации, по номенклатуре и характеристикам, устанавливаемым отраслевыми (фирменными) стандартами, и учитывающим различные аспекты применения аппаратуры и программного обеспечения. Рассмотрим основные особенности выделенных направлений сертификации в сфере информатизации.

ОБЯЗАТЕЛЬНАЯ СЕРТИФИКАЦИЯ ПО ТРЕБОВАНИЯМ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ И ПАРАМЕТРАМ БЕЗОПАСНОСТИ

В соответствии с действующими законодательными и нормативными документами выполнение работ по сертификации средств информатизации в данном направлении возложено на Госстандарт России. В 1994 году Госстандарт России ввел в действие нормативный документ "Номенклатура продукции и услуг, подлежащих обязательной сертификации в Российской Федерации". Этот документ ежегодно пересматривается и уточняется с учетом практики, условий торговли, производства и тенденций научно-технического развития.

Указанным документом к продукции, подлежащей обязательной сертификации в рассматриваемом направлении, отнесены следующие средства информатизации:

- вычислительные машины и комплексы;
- персональные ЭВМ;
- устройства внешней памяти, ввода-вывода и отображения информации;
- устройства подготовки и телеобработки данных.

Поскольку основу сертификации по параметрам безопасности составляют общие требования к оборудованию, остановимся подробнее на специфической для средств информатизации характеристике - электромагнитной совместимости.

Обеспечение электромагнитной совместимости заключается в выполнении требований по допустимым уровням электромагнитных помех, создаваемых функционирующими средствами, и требований к помехоустойчивости технических средств при воздействии внешних электромагнитных помех**.**

Невыполнение требований электромагнитной совместимости приводит к неэффективному использованию радиочастотного спектра, являющегося хотя и не расходуемым, но ограниченным ресурсом, к различным нарушениям в работе технических средств, а в ряде случаев и к аварийным ситуациям.

Сертификация средств информатизации по требованиям электромагнитной совместимости и параметрам безопасности возложена на Госстандарт России и проводится органами (центрами) сертификации, аккредитованными Госстандартом в рамках Системы сертификации ГОСТ Р.

Вы, вероятно, не раз встречали в рекламных объявлениях по продаже компьютеров фразу "Товар сертифицирован". Иногда в рекламе указывается и регистрационный номер сертификата соответствия, например, "Сертификат соответствия № РОСС RU.ME67.B00373". Речь в этих случаях идет именно о сертификации по требованиям электромагнитной совместимости и параметрам безопасности.

Для получения подобного сертификата изготовитель или поставщик технических средств информатизации должен обратиться в аккредитованный Госстандартом России орган сертификации, представив комплект документов, определяемый правилами сертификации. Орган сертификации организует

проведение соответствующих испытаний (проверок) и при положительном результате испытаний выдает сертификат соответствия. В тексте сертификата указываются конкретные виды требований, по которым проведены испытания, и соответствующие им нормативные документы.

Необходимо иметь в виду, что сертификат соответствия по требованиям электромагнитной совместимости и параметрам безопасности является необходимым, но в ряде случаев недостаточным условием полноты сертификации средств информатизации.

Это объясняется тем, что данный сертификат соответствия практически не затрагивает функциональных характеристик объекта и соответствия их современным требованиям. Такой сертификат дает вам только определенную уверенность в том, что предлагаемое оборудование не создает недопустимого уровня помех и безопасно в эксплуатации. Упрощенно говоря, объект может не

выполнять ряда возложенных на него, согласно имеющейся документации, функций или выполнять их некачественно, но, в полном соответствии с установленными правилами, может получить сертификат по электромагнитной совместимости и безопасности.

Сертификация средств информатизации по функциональным характеристикам будет рассмотрена нами в следующих разделах.

ОБЯЗАТЕЛЬНАЯ СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Законом "Об информации, информатизации и защите информации" определено, что информационные ресурсы, то есть отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учету и защите, как всякое материальное имущество собственника. При этом собственнику предоставляется право самостоятельно, в пределах своей компетенции, устанавливать режим защиты информационных ресурсов и доступа к ним.

Российская Федерация и ее субъекты являются собственниками информационных ресурсов, создаваемых за счет средств федерального бюджета и бюджетов субъектов Российской Федерации.

Законом "Об информации, информатизации и защите информации" введено также понятие документированной информации с ограниченным доступом, которая подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (то есть представляющую коммерческую, личную, служебную и другие тайны).

В соответствии с положениями этого закона собственник информационных ресурсов, содержащих государственную тайну, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

Таким образом, законодательно определяется некоторая категория информации, которая требует определенных ограничений в ее использовании, а сама информация требует защиты.

Целями защиты информации упомянутый Закон определяет:

• предотвращение утечки, хищения, утраты, искажения, подделки информации;

• предотвращение угроз безопасности личности, общества, государства;

• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

• предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

• защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

• сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

• обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Государство, владея информацией, представляющей национальное достояние или содержащей сведения ограниченного доступа, неправомерное обращение с которой может нанести ущерб ее собственнику, изыскивает специальные меры, обеспечивающие контроль ее использования и качества защиты. Одной из таких мер является сертификация средств защиты информации**.**

Необходимость сертификации средств защиты, применяемых при обработке информации, составляющей государственную тайну, закреплены в Законе Российской Федерации "О государственной тайне". Сертификации подлежат защищенные технические, программно-технические, программные средства, системы, сети вычислительной техники и связи, средства защиты и средства контроля эффективности защиты. Обязательной сертификации подлежат средства, в том числе и иностранного производства, предназначенные для обработки информации с ограниченным доступом, и прежде всего составляющей государственную тайну, а также использующиеся в управлении экологически опасными объектами, вооружением и военной техникой и средства их защиты. Наличие у владельца информационной системы сертифицированных средств обработки информации является гарантией надежности ее защиты и дает ему преимущества при осуществлении страхования.

Порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом установлен Положением "О сертификации средств защиты информации", утвержденным Постановлением Правительства Российской Федерации от 26 июня 1995 года № 608 (текст этого Положения приводится во второй части книги). Это Положение определяет области деятельности и сферу

компетенции различных государственных органов при сертификации средств защиты информации. Основной объем работ по сертификации средств защиты информации в пределах Российской Федерации возлагается на Гостехкомиссию России и Федеральное агентство правительственной связи и информации (ФАПСИ). Координация работ по организации сертификации этой продукции возложена на Межведомственную комиссию по защите государственной тайны.

Мы думаем, что на роли и общих задачах ФАПСИ здесь нет необходимости останавливаться подробно, поскольку они, в допустимых пределах, достаточно широко освещаются в печати. А вот название такого государственного органа, как Гостехкомиссия России, некоторым из наших читателей, возможно, незнакомо.

Государственнаятехническаякомиссияпри Президенте Российской Федерации (Гостехкомиссия России) является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации некриптографическими методами.

Непосредственное подчинение Президенту Российской Федерации обеспечивает независимость Гостехкомиссии России от региональных, ведомственных и корпоративных влияний, гарантирует соответствие ее деятельности высшим государственным интересам. Гостехкомиссия России - коллегиальный орган. В ее состав входят министры, председатели государственных комитетов, первые заместители (заместители) этих руководителей. Решения Гостехкомиссии России являются обязательными для исполнения всеми органами государственного управления, предприятиями, организациями и учреждениями независимо от их организационно-правовой формы и формы собственности, которые по роду своей деятельности обладают информацией, составляющей государственную или служебную тайну.

Директивными документами, в частности уже упоминавшимся Положением "О сертификации средств защиты информации" установлено, что:

В ведении Гостехкомиссии России находится сертификация программных и технических средств защиты информации, не использующих методы криптографии (шифрования), а в ведении ФАПСИ - сертификация средств защиты информации, использующих эти методы.

В соответствии с установленным распределением сфер деятельности Гостехкомиссии России и ФАПСИ в Российской Федерации созданы и функционируют две системы сертификации средств защиты информации:

- "Система сертификации средств защиты информации по требованиям безопасности информации", разработанная Гостехкомиссией России и зарегистрированная Госстандартом за № РОСС RU.OOOI.OIBHOO;
- "Система сертификации средств криптографической защиты информации (СКЗИ)", разработанная ФАПСИ и зарегистрированная Госстандартом за № РОСС RU.OOO 1.030001.

Эти системы сертификации технических и программных средств направлены на защиту интересов государства и государственного информационного ресурса, а также

интересов и прав собственников и владельцев информации — предпринимателей и граждан России, потребителей продукции и услуг от недобросовестной работы исполнителей.

ДОБРОВОЛЬНАЯ СЕРТИФИКАЦИЯ ПО ФУНКЦИОНАЛЬНЫМ ПАРАМЕТРАМ

Добровольная сертификация применяется для средств информатизации, не подлежащих в соответствии с законодательными актами Российской Федерации обязательной сертификации, и проводится по требованиям, на соответствие которым законодательными актами Российской Федерации не предусмотрено проведение обязательной сертификации.

Добровольная сертификация проводится для удостоверения качества средств и систем информатизации с целью повышения их конкурентоспособности, расширения сферы использования и получения дополнительных экономических преимуществ.

В общем случае упрощенную схему добровольной сертификации можно представить следующим образом. Необходимость добровольной сертификации обычно определяет разработчик или поставщик средств информатизации, руководствуясь при этом указанными выше соображениями. Разработчик или поставщик обращается в аккредитованный в установленном порядке сертификационный центр и финансирует проведение работ по сертификации. Совокупность и значения показателей качества, по которым проводится сертификация, формируются совместно заявителем и сертификационным центром. При положительных результатах испытаний средств информатизации, представленных для сертификации, заявитель получает сертификат соответствия, который используется, например, для рекламы при взаимодействии с потенциальным пользователем или потребителем. Последние не имеют непосредственных контактов с сертификационным центром. В случае выявления недостатков в сертифицированном изделии они обращаются непосредственно к поставщику, который обязан обеспечить доработку и повторные сертификационные испытания.

В соответствии с действующим законодательством добровольная сертификация средств информатизации может проводиться как в уже упоминавшейся нами Системе сертификации ГОСТ Р, так и в других системах сертификации, зарегистрированных Госстандартом России в установленном порядке.

Основные принципы организации систем сертификации средств информатизации и ведения процедуры сертификации мы рассмотрим в следующем разделе на примере Системы добровольной сертификации средств и систем в сфере информатизации "Росинфосерт", являющейся одним из важнейших инструментов проведения единой государственной научно-технической политики в сфере информатизации России.

Методология принятия решений о допустимости выдачи сертификата

Подтверждение соответствия осуществляется на основе следующих принципов:

- доступности информации о порядке осуществления подтверждения соответствия заинтересованным лицам;
- недопустимости применения обязательного подтверждения соответствия к объектам, в отношении которых не установлены требования технических регламентов;
- установления перечня форм и схем обязательного подтверждения соответствия в отношении определенных видов продукции в соответствующем техническом регламенте;
- уменьшения сроков осуществления обязательного подтверждения соответствия и затрат заявителя;
- недопустимости принуждения к осуществлению добровольного подтверждения соответствия, в том числе в определенной системе добровольной сертификации;
- защиты имущественных интересов заявителей, соблюдения коммерческой тайны в отношении сведений, полученных при осуществлении подтверждения соответствия;
- недопустимости подмены обязательного подтверждения соответствия добровольной сертификацией.

Кроме того, к основным принципам подтверждения соответствия следует отнести:

- открытость, прозрачность и одинаковое толкование требований и процедур оценки соответствия, стоимости и времени проведения работ для всех заинтересованных сторон;
- недопустимость ограничения конкуренции на рынке или создания необоснованных барьеров в торговле, связанных с оплатой работ;
- базирование в основном намеждународных руководствах и стандартах.

Для характеристики принципов подтверждения соответствия следует указать прежде всего на четкое разделение подтверждения соответствия на обязательное и добровольное, а также на осуществление обязательного подтверждения только в отношении объектов, требования к которым установлены в технических документах.

Важнейшим принципом обязательного подтверждения соответствия является установление перечня форм и схем подтверждения для определенных

видов продукции в технических регламентах, а не в документах, утверждаемых федеральным органом исполнительной власти Законом устанавливается обязанность лиц, осуществляющих подтверждение соответствия, обеспечивать доступность информации о действующем порядке подтверждения соответствия для всех заинтересованных лиц, принимать меры по сокращению сроков осуществления обязательного подтверждения соответствия и затрат заявителя.

Для тех видов продукции, на которые распространяется конкретный технический регламент, формы и схемы обязательного подтверждения соответствия должны содержаться в этом техническом регламенте.

Форма подтверждения соответствия — определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки,

реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров, выбор форм и схем для подтверждения соответствия конкретной продукции путем определения рисков ее использования и учета специфики отрасли

Формы подтверждения соответствия классифицируются по различным признакам. Согласно ст. 20 закона «О техническом регулировании» подтверждение соответствия на территории РФ может носить добровольный или обязательный характер.

Характер подтверждения соответствия может быть добровольным или обязательным.

При обязательной форме используют либо обязательную сертификацию, либо декларирование соответствия.

Обязательное подтверждение соответствия осуществляется в случаях, установленных техническим регламентом, в формах:

- принятия декларации о соответствии (декларирование соответствия);
- обязательной сертификации.

Декларирование соответствия может проводиться по одной из следующих схем:

- принятие декларации на основе только собственных доказательств;
- принятие декларации на основе собственных доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра) (третьей стороны).

Вопросы для самопроверки

1. Согласно Федеральному закону «О техническом регулировании» от 27.12.2002 № 184-ФЗ [21] с какой целью принимаются технические регламенты?

2. Какие группы документов входят в нормативную базу сертификации средств и систем информатизации?

3. В каких основных направлениях проводится сертификация средств информатизации?

4. Перечислите средства информатизации, которые подлежат обязательной сертификации согласно «Номенклатуре продукции и услуг, подлежащих обязательной сертификации в Российской Федерации».

5. Ознакомьтесь с текстом Федерального закона «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ. Какие цели защиты информации определяет данный закон?