# Тема. СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

## 9.1. Основные понятия и термины в области сертификации

Рынок средств и систем информатизации в России сейчас настолько разнообразен, что в подавляющем большинстве случаев потребитель не в состоянии самостоятельно убедиться в соответствии приобретаемой им продукции установленным на государственном уровне нормам и правилам. Положение усугубляется тем обстоятельством, что российский рынок заполнен импортными изделиями. Для этих изделий производители и поставщики в лучшем случае декларируют соответствие отдельным зарубежным стандартам, о содержании которых у вас, как правило, нет никакой информации. В результате вы, например, можете приобрести оборудование, являющееся опасным для обслуживающего персонала по поражению электрическим током или создающее большие электромагнитные помехи, нарушающие работу соседних устройств.

На бытовом уровне логичным путем решения этой проблемы является обращение к некоторому третьему лицу, являющемуся специалистом в данной области и заведомо независимому от поставщика продукции, которое может дать заключение о соответствии продукции установленным требованиям. На государственном уровне аналогичная процедура называется ***сертификацией.***

**Сертификация** — процедура, выполняемая третьей стороной, независимой от изготовителя (продавца) и потребителя продукции или услуг, по подтверждению соответствия этих продукции или услуг установленным требованиям.

Результатом выполнения процедуры сертификации является так называемый **сертификат соответствия*.***

**Сертификат соответствия** — документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Общие правовые основы сертификации продукции и услуг в Российской Федерации установлены Законом "О сертификации продукции и услуг", где определены права и ответственность в области сертификации органов государственного управления, а также изготовителей (продавцов, исполнителей) и других участников сертификации. В этом Законе, в частности, указано, что **сертификация проводится в целях*:***

1. создания условий для деятельности предприятий, учреждений, организаций и предпринимателей на едином товарном рынке Российской Федерации, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле;
2. содействия потребителям в компетентном выборе продукции;
3. защиты потребителя от недобросовестности изготовителя (продавца, исполнителя);
4. контроля безопасности продукции для окружающей среды, жизни, здоровья и имущества;
5. подтверждения показателей качества продукции, заявленных изготовителем.

Сертификация средств и систем информатизации является элементом общей системы сертификации продукции в Российской Федерации.

**Основные цели**сертификации средств информатизации, информационных технологий и услуг***:***

1. защита пользователей средств и систем информатизации от приобретения средств и систем, в том числе импортных, которые представляют опасность для жизни, здоровья, имущества, а также для окружающей среды;
2. обеспечение разработчиков систем, а также широкого круга пользователей этих систем достоверной информацией о состоянии отечественного и зарубежного рынков средств информатизации, телекоммуникаций, информационных технологий и услуг;
3. обеспечение информационного обмена между государственными системами информатизации (налоговая служба, правоохранительные органы, службы управления трудом и занятостью, образование, здравоохранение и др.);
4. обеспечение условий для информационного взаимодействия субъектов негосударственной принадлежности с субъектами государственной принадлежности;
5. содействие повышению научно-технического уровня и конкурентоспособности отечественных систем информатизации, информационных технологий и услуг;
6. содействие созданию условий для вхождения России в мировое информационное пространство.

Необходимо отметить, чтосертификация средств информатизации не только обеспечивает удовлетворение интересов потребителя, но приносит определенные выгоды и изготовителю (поставщику) продукции***.*** Так, в частности, сертификация способствует расширению рынка сбыта (распространению продукции в тех районах, где потребителю неизвестна репутация фирмы) и обеспечивает подтверждение качества продукции фирмы по сравнению с продукцией конкурентов. С точки зрения организации торговых взаимосвязей сертификация способствует созданию доверительных отношений между производителями (поставщиками) и потребителями продукции. Необходимо иметь в виду, что только имеющее место и объективно подтвержденное качество конкретных видов отечественной информационной продукции и средств информатизации может сделать их конкурентоспособными и реально обеспечить спрос на них.

**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:

1. государственный (национальный) орган по сертификации,
2. ведомственные органы по управлению сертификацией продукции определенных классов,
3. 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:

1. организует ведение обязательной сертификации продукции по поручению органов законодательной или исполнительной власти;
2. организует и финансирует разработку, а также утверждает основополагающие нормативно-технические и методические документы системы сертификации;
3. утверждает документы, устанавливающие порядок сертификации конкретных видов продукции;
4. проводит аккредитацию испытательных центров (лабораторий) совместно с ведомственными органами по сертификации и выдает аттестат аккредитации;
5. признает иностранные сертификаты соответствия, осуществляет взаимодействие с соответствующими уполномоченными органами других стран и международных организаций по вопросам сертификации;
6. регистрирует и аннулирует сертификаты соответствия и сертификационные лицензии, рассматривает спорные вопросы, возникающие в процессе сертификации;
7. организует периодическую публикацию информации по сертификации.

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

Говоря о сертификации, нельзя не отметить ее тесную взаимосвязь со стандартизацией в сфере информатизации.

**Во-первых,** как уже говорилось выше, суть процедуры сертификации заключается в подтверждении соответствия средств информатизации установленным требованиям. Документами, содержащими эти требования, являются стандарты, разрабатываемые в процессе стандартизации.

**Во-вторых*,*** собственно процедура сертификации регламентируется действующими нормативными документами (стандартами).

Таким образом, основой сертификации являются результаты стандартизации. В **нормативную базу сертификации** средств и систем информатизации, информационных технологий и услуг включаются три группы документов:

1. нормативные документы на объекты сертификации, где устанавливаются характеристики объектов, подтверждаемые при сертификации;
2. нормативные документы на методы испытаний для оценки характеристик объектов сертификации;
3. нормативные документы, регламентирующие процедуры сертификации.

В целом стандартизация вместе с сертификацией образуют единый процесс управления качеством средств, систем и технологий в области информатизации, одной из основных целей которого является защита интересов потребителя.

**Лицензирование**. Основным отличием процесса лицензирования от процесса сертификации является состав категорий, по отношению к которым они применяются. В процессе лицензирования фигурируют такие категории, как "деятельность" (подразумеваются виды или направления деятельности) и "субъект" (физическое лицо, предприятие, организация или иное юридическое лицо).

В соответствии с действующим законодательством в Российской Федерации отдельные виды деятельности осуществляются предприятиями, организациями и учреждениями независимо от организационно-правовой формы, а также физическими лицами, осуществляющими предпринимательскую деятельность без образования юридического лица, на основании лицензии — специального разрешения органов, уполномоченных на ведение лицензирования***.***

**Лицензия**является официальным документом, который разрешает осуществление указанного в нем вида деятельности в течение установленного срока, а также определяет условия его осуществления.

Основу нормативно-правовой базы лицензирования в сфере информатизации составляют Законы "О лицензировании отдельных видов деятельности", "Об информации, информатизации и защите информации" и "Об участии в международном информационном обмене".

Общие принципы лицензирования видов деятельности в сфере информатизации России можно сформулировать следующим образом:

Целью лицензирования является защита интересов государства и граждан от неумышленного или сознательного некачественного выполнения работ, соответствующих определенным видам деятельности в сфере информатизации.

Виды деятельности в сфере информатизации, подлежащие лицензированию, а также органы, осуществляющие лицензирование конкретных видов деятельности в различных областях информатизации, определены рядом нормативных документов.

Право на осуществление деятельности, подлежащей лицензированию, может получить субъект, отвечающий определенным критериям, которые заранее определяются правилами проведения лицензирования и являющимися их неотъемлемой частью требованиями к предприятию-заявителю. Таким образом, субъектом лицензирования становится лишь то физическое или юридическое лицо, которое представляет все необходимые и правильно оформленные документы и удовлетворяет соответствующим требованиям.

За органом, уполномоченным на проведение лицензионной деятельности, закрепляется право на осуществление контроля за деятельностью лицензиата.

## 9.2. Сертификация средств 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. а Рассмотрим основные особенности выделенных направлений сертификации в сфере информатизации.

### 9.2.1. 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:

1. вычислительные машины и комплексы;
2. персональные ЭВМ;
3. устройства внешней памяти, ввода-вывода и отображения информации;
4. 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 нерасходуемым, 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.

### 9.2.2. 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:**

1. предотвращение утечки, хищения, утраты, искажения, подделки информации;
2. предотвращение угроз безопасности личности, общества, государства;
3. предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
4. предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
5. защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
6. сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
7. и 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 ис-" пользующиеся 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.

**Государственная техническая комиссия при 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", текст которого приводится во второй части книги, 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.

С основными принципами построения и организационной структурой этих систем, а также правилами и конкретным порядком сертификации в их рамках средств защиты информации вы можете ознакомиться по документам, приведенным во второй части книги.

### 9.2.3. 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 Рос-. сии 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.