## СТАНДАРТЫ И ДРУГИЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ, РЕГЛАМЕНТИРУЮЩИЕ ЗАЩИЩЕННОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ

###### 4.1.1. Международные стандарты в области информационной безопасности

Общие вопросы

За рубежом разработка стандартов проводится непрерывно, последовательно публикуются проекты и версии стандартов на разных стадиях согласования и утверждения. Некоторые стандарты поэтапно углубляются и детализируются в виде совокупности взаимосвязанных по концепциям и структуре групп стандартов.

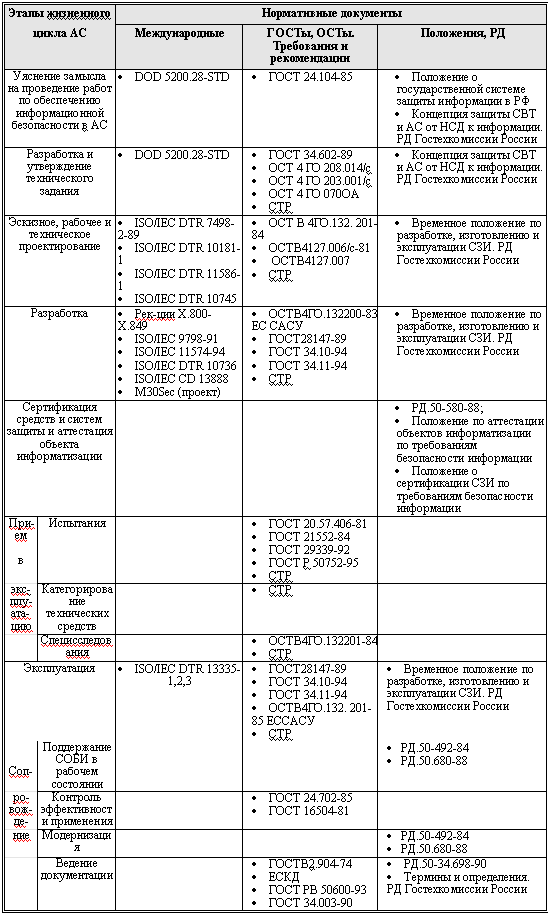
Принято считать, что неотъемлемой частью общего процесса стандартизации информационных технологий (ИТ) является разработка стандартов, связанных с проблемой безопасности ИТ, которая приобрела большую актуальность в связи с тенденциями все большей взаимной интеграции прикладных задач, построения их на базе распределенной обработки данных, систем телекоммуникаций, технологий обмена электронными данными.

Разработка стандартов для открытых систем, в том числе и стандартов в области безопасности ИТ, осуществляется рядом специализированных международных организаций и консорциумов таких, как, например, ISO, IЕС, ITU-T, IEEE, IАВ, WOS, ЕСМА, X/Open, OSF, OMG и др.

Значительная работа по стандартизации вопросов безопасности ИТ проводится специализированными организациями и на национальном уровне. Все это позволило к настоящему времени сформировать достаточно обширную методическую базу, в виде международных, национальных и отраслевых стандартов, а также нормативных и руководящих материалов, регламентирующих деятельность в области безопасности ИТ.

Основные нормативно-технические документы в области информационной безопасности приведены в таблице 4.1 (название некоторых документов приводятся в сокращенном виде, - их полное название можно найти в тексте данного раздела или списке литературы). При этом существующие нормативно-методические и нормативно-технические документы привязаны к этапам жизненного цикла автоматизированных систем.

Таблица 4.1



Архитектура безопасности Взаимосвязи открытых систем

Большинство современных сложных сетевых структур, лежащих в качестве телекоммуникационной основы существующих АС проектируются с учетом идеологии Эталонной модели (ЭМ) Взаимосвязи открытых систем (ВОС), которая позволяет оконечному пользователю сети (или его прикладным процессам) получить доступ к информационно-вычислительным ресурсам значительно легче, чем это было раньше. Вместе с тем концепция открытости систем создает ряд трудностей в организации защиты информации в ВС. Требование защиты ресурсов сети от НСД является обязательным при проектировании и реализации большинства современных ИВС, соответствующих ЭМ ВОС.

В 1986 г. рядом международных организаций была принята Архитектура безопасности ВОС (АБ ВОС). В архитектуре ВОС выделяют семь уровней иерархии: физический, канальный, сетевой, транспортный, сеансовый, представительный и прикладной. Однако в АБ ВОС предусмотрена реализация механизмов защиты в основном на пяти уровнях. Для защиты информации на физическом и канальном уровне обычно вводится такой механизм защиты, как линейное шифрование. Канальное шифрование обеспечивает закрытие физических каналов связи с помощью специальных шифраторов. Однако применение только канального шифрования не обеспечивает полного закрытия информации при ее передаче по ИВС, так как на узлах коммутации пакетов информация будет находиться в открытом виде. Поэтому НСД нарушителя к аппаратуре одного узла ведет к раскрытию всего потока сообщений, проходящих через этот узел. В том случае, когда устанавливается виртуальное соединение между двумя абонентами сети и коммуникации, в данном случае, проходят по незащищенным элементам ИВС, необходимо сквозное шифрование, когда закрывается информационная часть сообщения, а заголовки сообщений не шифруются. Это позволяет свободно управлять потоками зашифрованных сообщений. Сквозное шифрование организуется на сетевом и/или транспортном уровнях согласно ЭМ ВОС. На прикладном уровне реализуется большинство механизмов защиты, необходимых для полного решения проблем обеспечения безопасности данных в ИВС.

АБ ВОС устанавливает следующие службы безопасности (см. табл.4.2.).

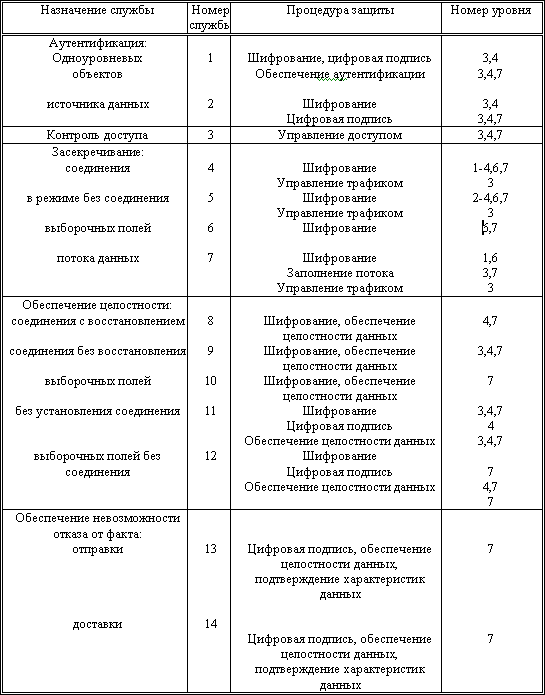
* обеспечения целостности данных (с установлением соединения, без установления соединения и для выборочных полей сообщений);
* обеспечения конфиденциальности данных (с установлением соединения, без установления соединения и для выборочных полей сообщений);
* контроля доступа;
* аутентификации (одноуровневых объектов и источника данных);
* обеспечения конфиденциальности трафика;
* обеспечения невозможности отказа от факта отправки сообщения абонентом - передатчиком и приема сообщения абонентом - приемником.

Состояние международной нормативно-методической базы

С целью систематизации анализа текущего состояния международной нормативно-методической базы в области безопасности ИТ необходимо использовать некоторую классификацию направлений стандартизации. В общем случае, можно выделить следующие направления.

1. Общие принципы управления информационной безопасностью.
2. Модели безопасности ИТ.
3. Методы и механизмы безопасности ИТ (такие, как, например: методы аутентификации, управления ключами и т.п.).
4. Криптографические алгоритмы.
5. Методы оценки безопасности информационных систем.
6. Безопасность EDI-технологий.
7. Безопасность межсетевых взаимодействий (межсетевые экраны).
8. Сертификация и аттестация объектов стандартизации.

Таблица 4.2



Стандартизация вопросов управления информационной безопасностью

Анализ проблемы защиты информации в информационных системах требует, как правило, комплексного подхода, использующего общеметодологические концептуальные решения, которые позволяют определить необходимый системообразующей контекст для редуцирования общей задачи управления безопасностью ИТ к решению частных задач. Поэтому в настоящее время возрастает роль стандартов и регламентирующих материалов общеметодологического назначения.

На роль такого документа претендует, находящийся в стадии утверждения проект международного стандарта ISO/IEC DTR 13335-1,2,3 - "Информационная технология. Руководство по управлению безопасностью информационных технологий". Данный документ содержит:

* определения важнейших понятий, непосредственно связанных с проблемой управления безопасностью ИТ; - определение важных архитектурных решений по созданию систем управления безопасностью ИТ (СУБ ИТ), в том числе, определение состава элементов, задач, механизмов и методов СУБ ИТ;
* описание типового жизненного цикла и принципов функционирования СУБ ИТ;
* описание принципов формирования политики (методики) управления безопасностью ИТ;
* методику анализа исходных данных для построения СУБ ИТ, в частности методику идентификации и анализа состава объектов защиты, уязвимых мест информационной системы, угроз безопасности и рисков и др.;
* методику выбора соответствующих мер защиты и оценки остаточного риска;
* принципы построения организационного обеспечения управления в СУБ ИТ и пр.

Стандартизация моделей безопасности ИТ

С целью обеспечения большей обоснованности программно-технических решений при построении СУБ ИТ, а также определения ее степени гарантированности, необходимо использование возможно более точных описательных моделей как на общесистемном (архитектурном) уровне, так и на уровне отдельных аспектов и средств СУБ ИТ.

Построение моделей позволяет структурировать и конкретизировать исследуемые объекты, устранить неоднозначности в их понимании, разбить решаемую задачу на подзадачи, и, в конечном итоге, выработать необходимые решения.

Можно выделить следующие международные стандарты и другие документы, в которых определяются основные модели безопасности ИТ:

* ISO/IEC 7498-2-89 - "Информационные технологии. Взаимосвязь открытых системы. Базовая эталонная модель. Часть 2. Архитектура информационной безопасности";
* ISO/IEC DTR 10181-1 - "Информационные технологии. Взаимосвязь открытых систем. Основы защиты информации для открытых систем. Часть 1. Общее описание основ защиты информации ВОС";
* ISO/IEC DTR 10745 - "Информационные технологии. Взаимосвязь открытых систем. Модель защиты информации верхних уровней";
* ISO/IEC DTR 11586-1 - "Информационные технологии. Взаимосвязь открытых систем. Общие функции защиты верхних уровней. Часть 1. Общее описание, модели и нотация";
* ISO/IEC DTR 13335-1 - "Информационные технологии. Руководство по управлению безопасностью информационных технологий. Часть 1. Концепции и модели безопасности информационных технологий".<

Стандартизация методов и механизмов безопасности ИТ

На определенном этапе задача защиты информационных технологий разбивается на частные подзадачи, такие как обеспечение, конфиденциальности, целостности и доступности. Для этих подзадач должны вырабатываться конкретные решения по организации взаимодействия объектов и субъектов информационных систем. К таким решениям относятся методы:

* аутентификации субъектов и объектов информационного взаимодействия, предназначенные для предоставления взаимодействующим сторонам возможности удостовериться, что противоположная сторона действительно является тем, за кого себя выдает;
* шифрования информации, предназначенные для защиты информации в случае перехвата ее третьими лицами;
* контроля целостности, предназначенные для обеспечения того, чтобы информация не была искажена или подменена;
* управления доступом, предназначенные для разграничения доступа к информации различных пользователей; - повышения надежности и отказоустойчивости функционирования системы, предназначенные для обеспечения гарантий выполнения информационной системой целевых функций;
* управления ключами, предназначенные для организации создания, распространения и использования ключей субъектов и объектов информационной системы, с целью создания необходимого базиса для процедур аутентификации, шифрования, контроля подлинности и управления доступом.

Организации по стандартизации уделяют большое внимание разработке типовых решений для указанных выше аспектов безопасности. К ним, в первую очередь отнесем следующие международные стандарты:

* ISO/IEC 9798-91 - "Информационные технологии. Защита информации. Аутентификация объекта".

Часть 1. Модель.  
Часть 2. Механизмы, использующие симметричные криптографические алгоритмы.  
Часть 3. Аутентификация на базе алгоритмов с открытыми ключами.  
Часть 4. Механизмы, использующие криптографическую контрольную функцию.  
Часть 5. Механизмы, использующие алгоритмы с нулевым разглашением.

* ISO/IEC 09594-8-88 - "Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации";
* ISO/IEC 11577-94 - "Информационные технологии. Передача данных и обмен информацией между системами. Взаимосвязь открытых систем. Протокол защиты информации на сетевом уровне";
* ISO/IEC DTR 10736 - "Информационные технологии. Передача данных и обмен информацией между системами. Протокол защиты информации на транспортном уровне";
* ISO/IEC CD 13888 - "Механизмы предотвращения отрицания".

Часть 1. Общая модель.  
Часть 2. Использование симметричных методов.  
Часть 3. Использование асимметричных методов;

* ISO/IEC 8732-88 - "Банковское дело. Управление ключами";
* ISO/IEC 11568-94 - "Банковское дело. Управление ключами".

Часть 1. Введение. Управление ключами.  
Часть 2. Методы управления ключами для симметричных шифров.  
Часть 3. Жизненный цикл ключа для симметричных шифров;

* ISO/IEC 11166-94 - "Банковское дело. Управление ключами посредством асимметричного алгоритма".

Часть 1. Принципы процедуры и форматы.  
Часть 2. Принятые алгоритмы, использующие криптосистему RSA;

* ISO/IEC DIS 13492 - "Банковское дело. Управление ключами, относящимися к элементам данных";
* ISO/IEC CD 11770 - "Информационные технологии. Защита информации. Управление ключами".

Часть 1. Общие положения.  
Часть 2. Механизмы, использующие симметричные методы.  
Часть 3. Механизмы, использующие асимметричные методы;

* ISO/IEC DTR 10181- "Информационные технологии. Взаимосвязь открытых систем. Основы защиты информации для открытых систем".

Часть 1. Общее описание основ защиты информации в ВОС.  
Часть 2. Основы аутентификации.  
Часть 3. Управление доступом.  
Часть 4. Безотказность получения.  
Часть 5. Конфиденциальность.  
Часть 6. Целостность.  
Часть 7. Основы проверки защиты.

К этому же уровню следует отнести стандарты, описывающие интерфейсы механизмов безопасности ИТ:

* ISO/IEC 10164-7-92. "Информационные технологии. Взаимосвязь открытых систем. Административное управление системы. Часть 7. Функции уведомления о нарушениях информационной безопасности".
* ISO/IEC DTR 11586. "Информационные технологии. Взаимосвязь открытых систем. Общие функции защиты верхних уровней".

Часть 1. Общее описание, модели и нотация.  
Часть 2. Определение услуг сервисного элемента обмена информацией защиты.  
Часть 3. Спецификация протокола сервисного элемента обмена информацией защиты.  
Часть 4. Спецификация синтаксиса защищенной передачи.

В стандартах этого уровня, как правило, не указываются конкретные криптографические алгоритмы, а декларируется, что может быть использован любой криптоалгоритм, при этом подразумевалось использование определенных зарубежных криптографических алгоритмов. Поэтому в ряде случаев при использовании некоторых стандартов может потребоваться их адаптация к отечественным криптоалгоритмам.

Стандартизация международных криптографических алгоритмов

ISO стандартизировала ряд криптографических алгоритмов в таких международных стандартах, как, например:

* ISO/IEC 10126-2-91 - "Банковское дело. Процедуры шифрования сообщения. Часть 2. Алгоритм DEA";
* ISO/IEC 8732-87 - "Информационные технологии. Защита информации. Режимы использования 64-битного блочного алгоритма";
* ISO/IEC 10116-91- "Банковское дело. Режимы работы n-бит блочного алгоритма шифрования";
* ISO/IEC 10118-1,2-88 - "Информационные технологии. Шифрование данных. Хэш-функция для цифровой подписи";
* ISO/IEC CD 10118-3,4 - "Информационные технологии. Защита информации. Функции хэширования";
* ISO/IEC 9796-91 - "Информационные технологии. Схема электронной подписи, при которой производится восстановление сообщения";
* ISO/IEC CD 14888 - "Информационные технологии. Защита информации. Цифровая подпись с добавлением". Однако широкое внедрение этих алгоритмов представляется малореальным, поскольку политика крупных государств направлена, как правило, на использование собственных криптоалгоритмов.

###### 4.1.2. Отечественная нормативно-правовая база, под действие которой подпадают АС различного назначения

Стандартизация в области защиты информации

К основным стандартам и нормативным техническим документам по безопасности информации, в первую очередь, относятся:

* в области защиты информации от несанкционированного доступа
* комплект руководящих документов Гостехкомиссии России (1998 г), которые в соответствии с Законом "О стандартизации" можно отнести к отраслевым стандартам, в том числе "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности средств вычислительной техники"", "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", "Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники", "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации",
* ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования";
* в области защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)
* "Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки за счет ПЭМИН" (СТР),
* ГОСТ 29339-92 "Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Общие технические требования",
* ГОСТ Р 50752-95 "Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний",
* методики контроля защищенности объектов ЭВТ и другие.

Особенности защиты программ нашли свое отражение в следующих документах Гостехкомиссии России: "Программное обеспечение автоматизированных систем и средств вычислительной техники. Классификация по уровню гарантированности отсутствия недекларированных возможностей" и "Антивирусные средства. Показатели защищенности и требования по защите от вирусов". В первом документе устанавливается классификация программного обеспечения автоматизированных систем и средств вычислительной техники по уровню гарантированности отсутствия в нем недекларированных возможностей, где уровень гарантированности определяется набором требований, предъявляемых к составу, объему и содержанию документации представляемой заявителем для проведения испытаний программ и к содержанию испытаний.

Во втором документе устанавливается классификация средств антивирусной защиты по уровню обеспечения защиты от воздействия программ-вирусов на базе перечня показателей защищенности и совокупности описывающих их требований. Кроме того, следующие нормативные документы так или иначе косвенно регламентируют отдельные вопросы обеспечения безопасности ПО:

* ГОСТ 28195-89. Оценка качества программных средств. Общие положения;
* ГОСТ 21552-84. Средства вычислительной техники. ОТТ, приемка методы испытаний, маркировка, упаковка, транспортировка и хранение;
* ГОСТ ВД 21552-84. Средства вычислительной техники. ОТТ, приемка методы испытаний, маркировка, упаковка, транспортировка и хранение;
* ТУ на конкретный вид продукции (ПО).

Стандартизация отечественных криптографических алгоритмов

Отечественные стандарты ГОСТ 28147-89, ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94 описывают криптографические алгоритмы, достаточные для решения большинства прикладных задач:

* ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования" описывает три алгоритма шифрования данных (из них один - так называемый "режим простой замены" - является служебным, два других - "режим гаммирования" и "режим гаммирования с обратной связью" - предназначены для шифрования целевых данных) и алгоритм выработки криптографической контрольной суммы (имитовставки), предназначенной для контроля целостности информации;
* ГОСТ Р 34.10-94 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма";
* ГОСТ Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хэширования".

Последние два алгоритма связаны друг с другом и описывают алгоритмы выработки и проверки электронной цифровой подписи, служащей для удостоверения авторства и подлинности информации.

## СЕРТИФИКАЦИОННЫЕ ИСПЫТАНИЯ ПРОГРАММНЫХ СРЕДСТВ

До получения готового программного изделия оценить его показатели качества можно лишь вероятностным образом на макроуровне рассмотрения структуры программного комплекса. Поэтому возникает насущная потребность в организации специального этапа в процессе создания ПО необходимого для подтверждения соответствия показателям качества реального программного изделия заданным к нему требованиям. Причем контроль выполнения этих требований должен осуществляться с учетом предполагаемых условий применения при форсированных нагрузках и тестировании всех установленных режимов. В рамках создания современных информационных технологий решение задач испытания ПО и получения документального подтверждения требуемых показателей качества программ объединяется в рамках процесса сертификации.

Сертификация программного обеспечения представляет собой процесс испытаний программ в нагруженных режимах применения, подтверждающий соответствие показателей качества программного изделия требованиям установленным в нормативно-технических документах на него и обеспечивающий документальную гарантию использования программного средства при соблюдении заданных ограничений.

Сертификация программного обеспечения КС возможна при выполнении следующих условий:

* разработке шкалы показателей качества с учетом специфики целевого использования программных средств и набора их функциональных характеристик;
* каталогизации программ, как объекта сертификации на основе опыта их эксплуатации;
* создании специализированного центра сертификации, выполняющего роль "третейской" организации контроля качества;
* разработке нормативно-технической базы, регламентирующей сертификацию программного обеспечения;
* разработке эталонов программных средств, которые удовлетворяют требованиям технических заданий на разработку разнотипных программных комплексов;
* разработке специальной технологии испытаний, определяющей объем и содержание сертификационных испытаний;
* реализации комплекса тестового программного обеспечения для широкого спектра программных изделий.

В процессе сертификации сложного ПО следует выделить два аспекта: методический и технологический. Методический аспект связан с разработкой комплекса методик сертификации программного обеспечения с учетом специфики его применения, а технологический с автоматизацией процесса применения методического аппарата.

Следует отметить, что по некоторым оценкам до 70% общих затрат на создание и внедрение сложных программных комплексов приходится на реализацию процесса их сертификации. Причем значительная доля этих затрат относится к организации аппаратно-программной платформы, моделирующих средств и тестового обеспечения стенда сертификации.

Кроме того, важнейшим вопросом создания качественных программных изделий является обеспечение технологической безопасности ПО на этапе сертификационных стендовых испытаний. Недостаточный уровень развития современных информационных технологий разработки ПО, доминирующее использование зарубежных инструментальных средств и применение разработчиками программ лишь средств защиты от непреднамеренных дефектов обуславливают существенные, принципиально новые изменения технологии создания программ в этих условиях. Поэтому, одной из задач сертификации на современном уровне развития информационных технологий становится выявление преднамеренных программных дефектов.

Технологическая безопасность на этапе сертификационных испытаний характеризуется усилением мер контроля, так как в настоящее время предполагается, что вероятность внедрения закладок на окончательных фазах разработки программ выше, чем на начальных фазах в связи со снижением вероятности их обнаружения при последовательном технологическом контроле. В связи с этим завершающей процедурой тестового контроля и испытаний программ должна стать сертификация ПО по требованиям безопасности с выпуском сертификата на соответствие этого изделия требованиям технического задания. В условиях существующих технологий создания ПО сертификация программ является наиболее дешевым и быстро реализуемым способом "фильтрации" компьютерных систем от низкокачественных, не отвечающих условиям безопасности программных средств. Сертификационные испытания программных средств, в том числе защищенных программных средств и программных средств контроля защищенности проводятся в государственных и отраслевых сертификационных центрах.

Право на проведение сертификационных испытаний защищенных средств вычислительной техники, в том числе программных средств предоставляется Гостехкомиссией России по согласованию с Госстандартом России предприятиям-разработчикам защищенных СВТ, специализированным организациям ведомств, разрабатывающих защищенные СВТ, в том числе программные средства.

В соответствии с "Положением о сертификации..." по результатам сертификационных испытаний оформляется акт, а разработчику выдается сертификат, заверенный в Гостехкомиссии России и дающий право на использование и распространение этих средств как защищенных.

Средства, получившие сертификат, включаются в номенклатуру защищенных СВТ, в том числе программных средств. Разработанные программные средства после их приемки представляются для регистрации в специализированный фонд Государственного фонда алгоритмов и программ.