Сертификация ИС и ее компонентов по требованиям информационной безопасности

В этой главе

- *Что такое сертификат безопасности*
- *Сертификат и экономические аспекты безопасности*
- *Риски применения средств защиты без сертификатов*
- *Критерии безопасности*
- *Процесс сертификации*
- *Сертификация программного обеспечения ИС*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Во всех секторах общественной жизни использование ИС постоянно растет. Такая тенденция повышает требования к безопасности применяемых информационных технологий.

В современных условиях уже не только функциональные возможности ИС, но и их защищенность стала для пользователя важным критерием выбора. Степень защищенности ИС определяется в процессе тестирования и оценки их компонентов по объективным критериям незаинтересованными организациями.

Цель сертификации — сделать защищенность информационных систем очевидной и сравнимой так, чтобы, с одной стороны, предоставить пользователям детализированную информацию и помощь при выборе системы, а с другой — дать заинтересованным изготовителям подтверждение качества их продукции.

Основные функции органа сертификации (700)

Орган сертификации наделен конкретными функциями, с которыми читатель может ознакомиться. Это:

- управление процессами сертификации закрепленной продукции;
- определение схемы и порядка проведения сертификации;
- разработка организационно-методических документов по сертификации;
- проведение по поручению Национального Центра аккредитации испытательных лабораторий по видам закрепленной продукции;
- технический надзор за сертифицированной продукцией;
- выдача сертификатов соответствия на продукцию.

Условием выдачи сертификата на продукцию служит ее соответствие требованиям установленных стандартов или нормативных документов.

В свою очередь основными функциями аккредитованных испытательных лабораторий являются:

- проведение испытаний сертифицируемой продукции и оформление протоколов испытаний;
- участие в проведении технического надзора и инспекционного контроля;
- участие в аттестации производства сертифицируемой продукции.

Орган сертификации и испытательные лаборатории выполняют свои функции в тесном взаимодействии

Изложенные положения являются основополагающими при определении структуры системы сертификации в интересах безопасности информации в компьютерных системах.

Кроме того, следует учитывать и полную независимость органа или лаборатории от заявителя (изготовителя, поставщика, продавца сертифицируемой продукции). То есть, должна быть исключена возможность административного, коммерческого и любого другого воздействия на них со стороны заявителей.

Наконец, проведение работ по сертификации продукции может быть доверено только организациям, имеющим необходимый уровень компетентности в данной области, что предполагает наличие в них высококвалифицированных специалистов.

Что такое сертификат безопасности (700)

Сертификат безопасности свидетельствует о качествах защищенной информационной техники. Они таковы:

Достоверность эффективности защиты. Достигается точным описанием защитных функций продукта в связи с характерными угрозами и наличием оценки степени устойчивости механизмов защиты против этих угроз.

Надежность. Достигается тестированием всех аспектов безопасности при разработке, производстве, поставке и применении продукта в соответствии с Европейскими критериями безопасности информационных технологий (ITSEC).

Корректность применения. Достигается точным описанием порядка и области применения продукта. Описываются также слабые места и указания по предупреждению негативных последствий.

А теперь, в знак доверия друг к другу, обменяйтесь сертификатами безопасности...

Примерный перечень продукции, процессов и услуг, подлежащих сертификации на соответствие требованиям обеспечения безопасности компонентов ИС:

Средства и процессы физической (объектовой) защиты информационных систем

- Технические средства контроля доступа на объект СВТ;
- Технические средства систем наблюдения (ТВ, ИК и др.);
- Процедура установления доступа на объект СВТ;
- Сертификация экранированных помещений специального назначения;
- Сертификация системы энергоснабжения компьютерных систем и объектов;
- Технические средства выявления на объектах активных источников электромагнитного излучения;
- Системы пространственного зашумления и их элементы;
- Системы линейного зашумления и их элементы;
- Помехоподавляющие фильтры в сетях питания, связи и сигнализации;
- Специальные фильтры и устройства защиты проводных линий связи;
- Технические средства обнаружения несанкционированного подключения к линиям связи компьютерных систем.

Технические средства ИС

- Средства вычислительной техники общего назначения;
- Защищенные средства вычислительной техники;
- Средства связи и периферийные устройства;
- Локальные вычислительные сети;
- Глобальные вычислительные сети;

Системы комплексной защиты информации в ИС

- Сертификация классификационного уровня защищенности существующих и проектируемых систем;
- Процедуры обеспечения достаточности систем защиты;
- Процедуры обеспечения непрерывности защиты информации.

Защита компьютерных систем от утечки информации по каналам ПЭМИН

- Защищенность СВТ общего назначения и периферийных устройств от утечки информации по ПЭМИН;
- Соответствие защищенных СВТ нормативным уровням ПЭМИН;
- Соответствие несущих конструкций и элементной базы СВТ требуемым уровням ПЭМИН;
- Соответствие уровней ПЭМИН СВТ требованиям ЭМС;
- Соответствие средств передачи информации в компьютерных системах требуемым уровням ПЭМИН;
- Соответствие СВТ требованиям отсутствия встроенных технических средств разведки и разрушений;

Защита от НСД

- Программные, аппаратные и программно-аппаратные средства защиты от НСД;
- Программные и аппаратные средства криптографической защиты информации в СВТ общего назначения;
- Программные средства антивирусной защиты в СВТ и вычислительных сетях;
- Процедуры установления разграничения и контроля доступа в СВТ и вычислительных сетях;
- Соответствие программного обеспечения компьютерных систем требованиям отсутствия программных средств разведки и разрушения информации.

Данный перечень продукции при проведении аккредитации органа сертификации может быть уточнен в соответствии с возможностями организации и конкретными условиями. По мере развертывания работ по сертификации и накопления опыта перечень может быть расширен.

В распоряжении органа сертификации предусматриваются необходимые испытательные лаборатории.

Сертификат и экономические аспекты безопасности (700)

Применение защищенной информационной техники экономически эффективнее, чем последующее осуществление мер безопасности с целью компенсировать первоначальное отсутствие мер защиты. Требование пользователя к изготовителю продукта о наличии такого сертификата подразумевает, что могут быть рассчитаны необходимые затраты для осуществления комплекса мер защиты. При наличии сертификата безопасности защитные функции продукта могут быть реально оценены и оптимально использованы в рамках концепции безопасности.

Риски применения средств защиты без сертификатов (700)

Для информационной техники характерны следующие риски:

- потеря конфиденциальности (например, несанкционированное получение информации);
- потеря целостности (например, манипуляции с данными);
- потеря функциональности (например, потеря или разрушение данных).

В случае реального воздействия эти риски могут привести:

- к плохо просчитываемым расходам;
- к потере репутации фирмы;
- к последовательным искам.

Поэтому наличие сертификата безопасности является существенным фактором безопасного и эффективного использования информационной техники.

Короче говоря: ***защищенность — функция корректности и эффективности.***

Корректность (701)

Уверенность в корректности информационной техники зависит от глубины тестирования и качества методик тестирования. ITSEC предусматривает 6 ступеней оценки корректности — от E1 до E6:

Аспекты тестирования

Критерии безопасности устанавливают детализированные требования:

- к продукту,
- процессу его разработки,
- условиям разработки,
- документации на продукт,
- условиям функционирования продукта.

Не сертифицированные средства защиты могут привести к лишним расходам...

Эффективность (701)

Под эффективностью понимается способность механизмов защиты противостоять характерным угрозам. Эта способность называется стойкостью механизмов и может быть охарактеризована одной из трех ступеней: низкая, средняя, высокая.

Чем выше требования пользователя к безопасности, тем выше должна быть уверенность в корректном функционировании и стойкости против несанкционированных манипуляций.

Критерии безопасности (700)

Испытание и оценка информационных систем и их компонентов выполняется на основе критериев безопасности, в которых формулировка требований к уровням безопасности имеет иерархическую структуру.

“Критерии оценки безопасности информационных систем” (ITSEC), разработаны на основе национальных критериев некоторых европейских государств. Предпосылкой разработки этих европейских критериев была необходимость взаимного признания сертификатов в связи с развитием общеевропейского рынка. С этим же связана и необходимость разработки общих основ для оценки защищенности информационных систем.

Функции защиты (704)

Технические требования к информационным системам и компонентам в первую очередь предполагают наличие определенных функций защиты, таких, как идентификация и аутентификация пользователей, контроль доступа (предоставление и проверка прав), протоколирование (обнаружение нарушений или попыток), очистка памяти перед повторным использованием, защита передачи данных.

Детальные требования к этим функциям защиты могут значительно различаться для разных приложений. Для многих стандартных ситуаций в названных Критериях предусмотрены классы функциональности.

Требования к классам функциональности от F-C1 до F-B3 (соответственно от F1 до F5) в основном относятся к операционным системам. На первом плане здесь — вопрос конфиденциальности данных.

Класс функциональности F-IN содержит требования к целостности банков данных или программных систем разработки приложений.

В классе F-AV сформулированы требования к доступности данных и услуг. Функциональные классы F-DI, F-DC и F-DX относятся к системам и компонентам для передачи данных.

Ниже дается более подробная характеристика классов функциональности от F-C1 до F-B3 (соответственно от F1 до F5). Совокупность классов имеет иерархическую структуру, от класса к классу требования повышаются.

F-C1 (F1): Имеется определяемая пользователем система контроля доступа ("знает только тот, кому это необходимо").

F-C2 (F2): Имеется более детализированная система контроля доступа, чем в классе F-C1. Устанавливается ответственность пользователей за их действия благодаря идентификации, регистрации событий, разделению ресурсов.

F-B1 (F3): Дополнительно к системе контроля вводится функция управления атрибутами секретности. Она представляет собой совокупность правил доступа относительно всех контролируемых субъектов информационных отношений и носителей информации, обеспечивает правильное присвоение атрибутов поступающей извне информации.

F-B2 (F4): Расширяются обязательные требования по контролю доступа относительно всех субъектов и объектов, усиливаются требования по аутентификации в сравнении с классом F-B1.

F-B3 (F5): Дополнительно к функциям класса F-B2 вводятся функции поддержки определенных административных процедур безопасности, расширяется диапазон регистрируемых событий, имеющих отношение к безопасности.

Качество защиты (701)

Наряду с объемом функций защиты решающую роль играет качество защиты информационных систем. Необходимо рассматривать два аспекта:

- предпосылкой разумной оценки защитных свойств является корректное функционирование механизмов защиты;
- основываясь на корректности, необходимо охарактеризовать эффективность защитных функций.

В старых критериях ИТС оба аспекта в совокупности характеризовались уровнем от Q1 до Q7, причем Q1 был нижним уровнем, а Q7 — высшим. В новых критериях ITSEC эти аспекты разделены.

Корректность характеризуется уровнем от E1 до E6, а для характеристики эффективности имеется шкала оценки стойкости механизмов защиты (низкая, средняя, высокая). Уровень качества обозначается комбинацией, например E2, средняя.

Условно качество защищенности можно охарактеризовать по четырем уровням):

- ***низкое***: грубо протестированная корректность, слабая защита от манипуляций или отсутствие таковой;
- ***удовлетворительное***: обстоятельно протестированная корректность, удовлетворительное действие защиты против манипуляций;
- ***хорошее или очень хорошее***: тщательно протестированная корректность, хорошая или очень хорошая защита от манипуляций;
- ***отличное***: максимальные требования к подтверждению корректности, практически не преодолимая защита от манипуляций.

При определении уровня качества защиты учитываются многие факторы. Назовем некоторые из них:

- корректность разработки продукта (требования к защищенности, архитектурный проект, подробный проект, реализация);
- эффективность конструкции продукта (пригодность, совместное проявление функций, оценка уязвимых мест, стойкость механизмов защиты);
- безопасность среды разработки (контроль конфигурации, язык программирования, компилятор, безопасность при разработке);
- рабочая документация (документация пользователя, администратора системы);
- область использования (поставка и конфигурирование, начало использования, техническое обслуживание).

Уровни корректности (701)

Приведем более подробные определения иерархических уровней корректности от E1 до E6:

E0: представляет недостаточную защищенность.

E1: предполагает наличие технического задания по защищенности продукта и неформальное описание архитектурного проекта. Функциональные тесты должны подтвердить, что требования ТЗ по защищенности выполняются.

E2: дополнительно к требованиям уровня E1 предполагается наличие неформального описания подробного проекта. Достаточность функциональных тестов должна быть оценена. Необходима система контроля конфигурации и согласованный вариант распределения полномочий.

E3: дополнительно к требованиям уровня E2 должен быть оценен исходный код программы или конструкторские чертежи изделия, отражающие механизмы защиты. Должна быть оценена полноценность тестов для оценки механизмов защиты.

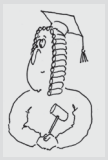
E4: дополнительно к требованиям уровня E3 предполагается наличие формальной модели безопасности как части технического задания по защищенности. Обязательны в полуформальном изложении описания

функций защиты, архитектурного и подробного проектов.

E5: дополнительно к требованиям уровня E4 должна быть представлена взаимозависимость между подробным проектом и исходным кодом программы или, соответственно, конструкторскими чертежами изделия.

E6: дополнительно к требованиям уровня E5 предполагается наличие формального описания функций защиты и архитектурного проекта, согласованного с моделью безопасности.

Сертификация продукции (700)



Определение

Под сертификацией продукции по требованиям безопасности информации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — сертификата и знака соответствия с определенной степенью достоверности подтверждается, что продукция соответствует требованиям стандартов по безопасности информации или иных нормативно-технических документов.

При сертификации могут подтверждаться как отдельные характеристики, так и весь комплекс характеристик продукции, связанных с обеспечением безопасности информации, а именно технических, программно-технических, программных средств, систем, сетей вычислительной техники и связи, средств защиты и средств контроля эффективности защиты по требованиям безопасности информации.

При сертификации продукции подтверждаются требования по защите информации:

от несанкционированного доступа (действия), в том числе от компьютерных вирусов;

посредством криптографических преобразований;

от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) или от воздействия на нее специальных устройств, встроенных в технические средства.

Обязательной сертификации по требованиям безопасности информации подлежат средства и системы вычислительной техники и связи, предназначенные для обработки (передачи) секретной (конфиденциальной) информации, для использования в управлении экологически опасными объектами, вооружением и военной техникой, а также средства защиты и контроля эффективности защиты такой информации.

Сертификация продукции по требованиям безопасности информации базируется на системах:

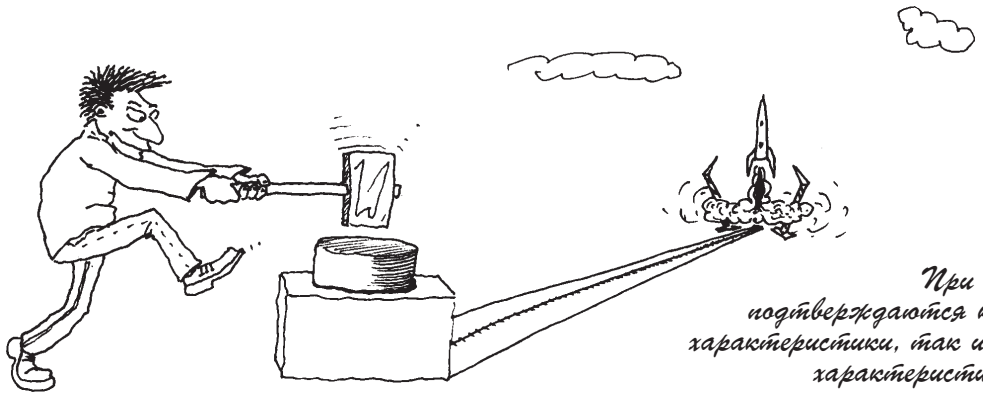
- стандартизации и фонде нормативно-технической документации по безопасности информации;
- аккредитации органов по сертификации продукции, органов надзора и испытательных центров (лабораторий).

Основными схемами сертификации продукции по требованиям безопасности информации являются:

а) для единичных образцов продукции — испытания на соответствие требованиям по безопасности информации;

б) для серийного производства продукции — типовые испытания образцов продукции на соответствие требованиям по безопасности информации и последующий надзор за стабильностью характеристик сертифицированной продукции, обеспечивающих (определяющих) выполнение этих требований. Кроме того, решением органа по сертификации допускается предварительная проверка производства по утвержденной программе.

По согласованию с органом сертификации по требованиям безопасности информации могут быть ис-



При сертификации подтверждаются как отдельные характеристики, так и весь комплекс характеристик продукции...

пользованы и другие схемы сертификации, применяемые в международной практике.

В отдельных случаях по согласованию с органом по сертификации допускается проведение испытаний на базе разработчика (изготовителя) продукции. При этом орган по сертификации определяет условия, необходимые для обеспечения объективности результатов испытаний.

Органы по сертификации и испытательные центры (лаборатории) несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав заявителя при испытаниях его продукции.

Процесс сертификации (700)

Для проведения сертификации изготовитель или продавец продукта представляют необходимую конструкторскую документацию.

Оценка продукта выполняется испытательными лабораториями.

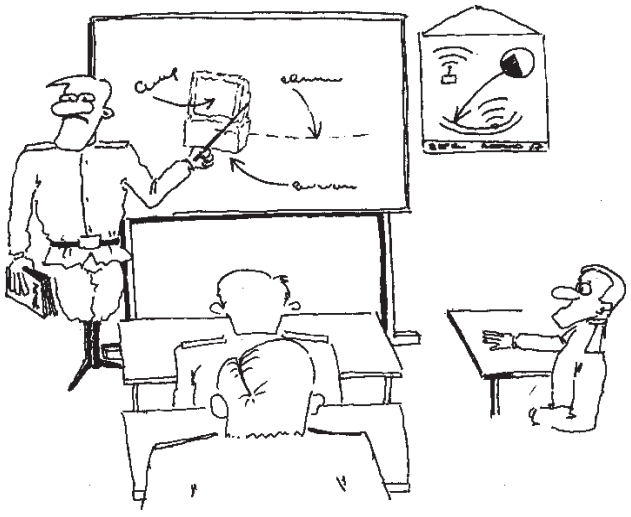
Перед обращением по поводу сертификации часто возникает вопрос, какие продукты могут быть сертифицированы, и какие ограничения могут влиять на законную силу сертификата. Поэтому критериями ITSEC предусматривается возможность тестирования и, при выполнении необходимых требований, сертификации любого информационного продукта: изделия, программы, апаратно-программного комплекса или группы продуктов (операционная система, банк данных, пакет электронной почты).

Существует три вида сертификации:

- сертификация готового продукта;
- сертификация в процессе разработки;
- повторная сертификация уже сертифицированного продукта.

При сертификации в процессе разработки сертификационная оценка и разработка идут параллельно, бок о бок. При этом обеспечивается не только то преимущество, что новая версия продукта и сертификат появляются одновременно, но и то, что ошибки и уязвимые места своевременно выявляются и корректируются на стадии разработки.

Необходимо подчеркнуть, что ***сертификат выдается не на определенный тип продукта, а на определенную версию продукта и имеет силу только для этой версии.*** Это значит, что если после сертификации готового продукта через короткий промежуток времени, обусловленный жизненным циклом данного продукта, на рынке появляется его новая версия, для нее сертификат не действителен. Это обстоятельство вынуждает проводить повторную сертификацию, что позволяет изготовителю в значительно сокращенные сроки получить повторный сертификат на новую версию уже сертифицированного продукта, и тогда тестируются только изменения в продукте, имеющие отношение к его защищенности. Эта возможность в настоящее время широко используется.



Сертификация в процессе разработки...

Процесс сертификации делится на три фазы:

- подготовка к сертификации;
- сертификационная оценка;
- сертификация.

Процесс подготовки к сертификации начинается, как правило, с переговоров между изготовителем и соответствующим уполномоченным органом о процессе сертификации конкретного продукта. На переговорах обсуждают детали методики, оплату, временной график, конструкторскую документацию. Рассматриваются функции защиты продукта, при возможности происходит соотнесение с одним из классов функциональности, устанавливается, на какой уровень защищенности претендует продукт. После этого изготовитель подает заявление на сертификацию.

Выбор испытательной лаборатории предоставляется изготовителю. Если он останавливает выбор на аккредитованной испытательной лаборатории, с этой лабораторией заключается отдельный договор. Фаза подготовки к сертификации заканчивается с проведением первого совместного совещания, на котором вырабатываются план работ и временной график.

Сертификационная оценка выполняется персоналом испытательной лаборатории. В процессе оценки требуется тесное взаимодействие между изготовителем и испытательной лабораторией. Описания отдельных этапов тестирования и результаты тестирования как у изготовителя (должны быть представлены акты), так и в испытательной лаборатории включаются в отчеты.

Должны быть учтены такие существенные моменты:

- выявление совокупности условий (образ действий, комплект документации, и т.д.)
- интерпретация лежащих в основе Критериев безопасности (отдельно и в совокупности);
- сопровождение тестирования — для каждой сертификационной оценки должны быть определены цель, характерный подход и методика.

В последней фазе процесса сертификации составляется ***Заключение о сертификации*** с использованием итогового отчета, отчетов по отдельным тестам и информации, полученной в процессе сертификационной оценки. Кроме предварительных замечаний и пояснений, Заключение содержит сертификат и отчет о сертификации. В отчет о сертификации входит описание оцененных защитных свойств продукта, указания и ограничения для пользователя. Выводы Заключения о сертификации действительны только при соблюдении этих указаний и ограничений. Заключение о сертификации, как правило, публикуется и может быть получено у изготовителя.

Результат процесса сертификации направляется изготовителю в виде Решения. После этого сертифицированный продукт включается в соответствующий список, который регулярно обновляется и публикуется. Он содержит, кроме общей информации по сертификации и аккредитации, короткое описание сертифицированных продуктов.

Длительность процесса сертификационной оценки зависит от сложности продукта и от заявленного уровня защищенности. Для средства защиты персонального компьютера длительность процесса сертификации, как правило, составляет 3 месяца, а для операционной системы большой ЭВМ — составить около 2 лет.

Пропорционально длительности процесса сертификации, естественно, растут расходы изготовителя продукта на сертификацию. Опыт показывает, что эти расходы колеблются в пределах 5% от стоимости разработки.

Порядок подготовки и проведения сертификации (700)

Порядок подготовки и проведения сертификации предусматривает следующие действия:

- подачу и рассмотрение заявки на сертификацию;
- предварительную проверку производства сертифицируемой продукции;
- испытания сертифицируемой продукции;
- оформление, регистрацию и выдачу сертификата соответствия и сертификационной лицензии на право использования знака соответствия;
- признание зарубежных сертификатов соответствия;
- осуществление надзора за сертификацией и производством сертифицированной продукции;
- информацию о результатах сертификации;
- рассмотрение апелляций.

Подача и рассмотрение заявки на сертификацию

Заявитель для получения сертификата соответствия направляет в орган по сертификации продукции заявку на проведение испытаний с указанием схемы проведения сертификации, наименованием стандартов и иных нормативно-технических документов, на соответствие требованиям которых должна проводиться сертификация.

Предварительная проверка состояния производства сертифицируемой продукции

Проводится органом по сертификации в соответствии с выбранной схемой сертификации и представляет со-

бой комплекс мероприятий, направленных на подтверждение наличия условий для обеспечения стабильного уровня требований, характеристик и показателей, которые контролируются при сертификации.

Испытания сертифицируемой продукции

Испытания сертифицируемой продукции в аккредитованных испытательных центрах (лабораториях) проводятся на образцах, конструкция, состав и технология изготовления которых должны быть такими же, как и у образцов, поставляемых потребителю (заказчику). Количество образцов, порядок их отбора и идентификации устанавливается организационно-методическими документами по сертификации конкретного вида продукции.

Признание зарубежных сертификатов соответствия

Решение о признании и регистрации сертификатов, выданных органами по сертификации других стран на отечественную и импортируемую продукцию, используемую в стране, по требованиям безопасности информации, принимает соответствующий орган. Признаются сертификаты или аналогичные по назначению документы (лицензии, официальные утверждения и т.п.), выданные в рамках международных систем. Порядок такого признания устанавливается правилами этих систем или соглашений.

Осуществление надзора за сертификацией

Надзор за проведением сертификации предусматривает проверки правильности и полноты проводимых испытаний центрами (лабораториями), оформление и рассмотрение отчетных документов и протоколов испытаний. Осуществляется контроль за своевременным внесением изменений в нормативно-техническую документацию по требованиям безопасности информации.

Надзор за производством сертифицированной продукции включает в себя испытания продукции и контроль производства сертифицированной продукции.

По результатам надзора составляется заключение, направляемое в орган по сертификации для принятия решения.

Сертификация представляет собой действия, доказывающие, что должным образом идентифицированная продукция (процесс или услуга) соответствует требованиям конкретного стандарта или другого нормативного документа. Таким образом, по отношению к компьютерным системам сертификация является неотъемлемой частью процесса обеспечения безопасности информации. Для выполнения работ по сертификации определенных видов продукции назначаются и аккредитуются органы и испытательные лаборатории.

Сертификация программного обеспечения на соответствие требованиям безопасности (720)

Существует значительное число производственных и коммерческих ИС, в которых нарушения функционирования программного обеспечения могут привести к катастрофическим последствиям — порче ценного оборудования, финансовым потерям или даже к угрозе здоровью и жизни людей (экология, финансы, транспорт, связь и т.п.).

В мировой практике принято, что испытания программного обеспечения (ПО) для таких (критичных) вычислительных систем следует специально организовывать и документировать. Эти испытания объединяются понятиями аттестации и сертификации ПО.

Процессы аттестации и сертификации отличаются от обычных испытаний ПО более высоким уровнем формализации условий и результатов испытаний, проводимых специальной испытательной лабораторией.

Аттестация — специальный процесс испытаний ПО с использованием упорядоченной совокупности тестов, в результате которого специальный коллектив гарантирует полное выполнение предписанных функций и безопасность ПО в пределах документированных требований. В результате аттестации ПО присваиваются различные уровни безопасности.

Сертификация также является испытанием ПО, но в более жестких условиях тестирования, особо выделенным (третейским) коллективом специалистов, имеющим право на официальный государственный или ведомственный контроль функций ПО. В результате

Надзор за проведением сертификации...

сертификации выдается свидетельство о соответствии ПО стандартам и другим нормативным фактам

Существует три ситуации, когда Вы задумаетесь об аттестации и/или сертификации ПО на соответствие требованиям безопасности.

1. Вы — пользователь. Ваша служба безопасности требует гарантий, что приобретенное ПО не будет содержать каких-либо угроз деятельности объекта.

2. Вы — разработчик. Ваш заказчик требует гарантий, что разработанное вами ПО не содержит дефектов (случайных или злоумышленных), которые нанесут ему материальный ущерб.

3. ПО относится к классу программ, который по существующим нормативным актам требует обязательной сертификации (например, программное обеспечение защиты информации).

Во всех подобных случаях вам предстоит искать испытательную лабораторию, которая аккредитована (имеет лицензию) на право проведения таких работ. Прежде чем заключать с ней договор, неплохо получить представление об общем порядке и особенностях проведения подобных испытаний.

В первую очередь выясните, какую информацию об испытуемом ПО необходимо представить. Как правило, от вас потребуют весь объем программной документации (причем не только эксплуатационной, но и конструкторской), исходные тексты программ, подробные данные о разработчике ПО и источнике его приобретения, подробные данные о системе, в которой это ПО предлагается использовать и другие данные, а также попросят детально сформулировать выдвигаемые вами требования по безопасности (например, отсутствие компьютерных вирусов и программной закладки, невозможность хищения или модификации информации и т.д.).

Эффективность информационной системы определяется качеством применяемых информационных технологий, которые в свою очередь существенным образом зависят от качества программного обеспечения (ПО).

Существующие информационные технологии не позволяют создавать ПО, полностью свободное от недостатков, однако существует реальная угроза воздействия на ПО различных негативных факторов (вирусы, программные закладки).

Как показывает анализ, программная закладка может быть легко и незаметно внедрена разработчиком в тело программы. Ситуация осложняется тем, что зачастую невозможно однозначно определить, является ли выявленный программный дефект случайным или преднамеренным. Кроме того, актуальной остается проблема защиты ПО от злоумышленного несанкционированного доступа и воздействия на содержание выполняемых операций и, соответственно, на качество выполняемых функций. ***Решение проблемы обеспечения безопасности ПО требует комплексного подхода, соответствующего в рассмотрении всей совокупности факторов:***

- технология производства ПО;
- стандартизация;
- сертификация.

Качество ПО определяется совокупностью свойств, обуславливающих его способность удовлетворять определенные потребности в соответствии с назначением. При этом свойства ПО проявляются на всех уровнях жизненного цикла — от ТЗ до сопровождения и эксплуатации.

Проблема разработки ПО высокого качества включает три задачи:

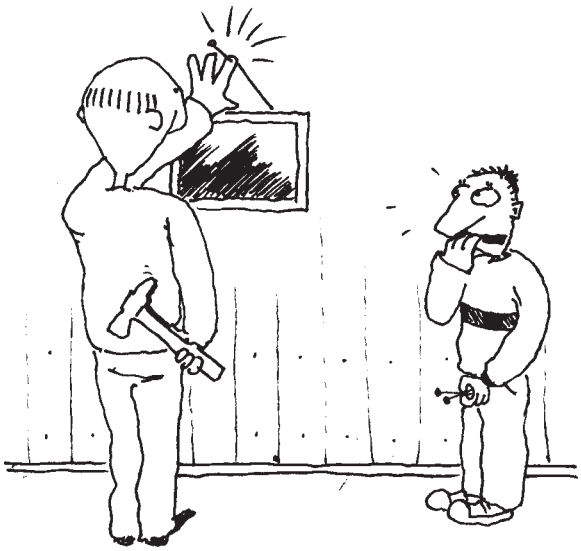
- оценка качества;
- гарантия качества;
- управление качеством.

Гарантия качества, как правило, обеспечивается поддержкой надлежащим образом функционирующей и документально оформленной системой качества. Тем самым гарантируется, что качество будет закладываться по мере проведения разработки, а не определяться в конце данного процесса.

Управление качеством заключается в надлежащей корректуре проекта после оценки качества на каждом этапе с целью достижения необходимого (гарантированного) уровня защищенности конечного продукта.

В условиях существующего рынка ПО наиболее дешевым и быстро реализуемым способом оградить пользователя от низкокачественной продукции может стать введение сертификации качества ПО.

Сертификация является процедурой и инструментом установления соответствия ПО конкретным требованиям и проводится в целях охраны прав пользователя. В соответствии с поставленной целью, в процессе сертификации ПО решаются задачи, связанные с анализом и оценкой программного продукта. Завершающим этапом сертификации является выдача официального заключения (сертификата). ***Сертификат дает право*** разработчику на распространение продукции и обязывает его выпускать ПО не ниже качества, установленного сертификатом.



Качество закладывается по мере проведения разработки...

Типовой алгоритм испытаний ПО на соответствие требованиям безопасности (720)

Рассмотрим основные процедуры испытаний, при этом любые программы, процедуры, данные, влияющие на ход вычислительного процесса, будем называть программными помехами (ПП).

Анализ требований заказчика к ПО на соответствие требованиям безопасности (720)

Этот анализ заключается в их уяснении, конкретизации, формализации, установлении взаимной корреляции требований, приведении их, по возможности, к количественной мере. ***Среди требований по безопасности использования ПО в ИС можно выделить типовые***. К ним относятся:

- допустимый ущерб (выраженный количественно), который может быть нанесен ИС за заданное время при использовании ПО с программными помехами;
- допустимые функции для ПО по управлению ресурсами ИС;
- отсутствие процедур самовоспроизведения;
- отсутствие процедур преодоления защиты ИС;
- отсутствие процедур, имитирующих решение истинных задач;
- отсутствие процедур, разрушающих систему;
- отсутствие технологических ошибок и др.

Помимо типовых требований к ПО в конкретных условиях могут быть выдвинуты индивидуальные с учетом специфики объекта, на котором предполагается использовать программное обеспечение.

Анализ источника получения ПО (720)

Программное обеспечение может попасть к заказчику одним из следующих путей:

- закуплено у разработчика или официального дистрибьютора;
- получено от законного пользователя в составе программного комплекса его разработки;
- скопировано у законного или незаконного пользователя. ПО, полученные по последнему каналу (т.н. “серые” и “черные” копии), не могут быть аттестованы как безопасные и использоваться в критичных ИС по ряду причин:
- опыт длительной безопасной эксплуатации некоторых ПО не может быть распространен на незаконные копии;
- незаконные копии являются основным источником проникновения компьютерных вирусов в ИС во всех зарегистрированных случаях;
- многие ПО имеют различные виды защиты от незаконного копирования, что может привести к непредсказуемым последствиям при эксплуатации таких копий в ИС.

Если ПО официально закуплено у фирмы-разработчика, анализу подлежат следующие вопросы:

- государственная принадлежность фирмы;
- репутация фирмы-разработчика (известность, независимость, степень взаимодействия с государственными и особенно силовыми структурами, используемая при производстве систем управления качеством и т.п.);
- способ распространения продукции (ведется ли учет пользователей, имеет ли ПО учетный номер, может ли изготовитель знать конечного пользователя ПО).

При этом факторами, повышающими опасность от ПП, являются:

- фирма-разработчик малоизвестна;
- фирма работает по заказам спецслужб;
- продукция фирмы не имеет международного сертификата;
- каждый дистрибутив ПО имеет учетный номер, пользователь которого известен фирме-разработчику;

- нет сведений об использовании данного ПО в критических областях применения.

Если ПО приобретено у официального дистрибьютора фирмы-разработчика, тот же круг вопросов подлежит анализу как в отношении разработчика, так и дистрибьютора.

Анализ условий предполагаемого применения ПО (720)

Для анализа необходимы следующие исходные данные:

- о типе и категории объекта, на котором предполагается использовать ПО;
- об используемой на объекте аппаратной и программной среде;
- о предполагаемой к использованию на объекте системе защиты информации;
- роль и место испытуемого ПО в системе управления объектом.

Программное обеспечение может планироваться для использования в различных информационных системах. Оно может быть использовано при решении задач по управлению ресурсами самой ИС или внешними объектами. В зависимости от важности задач, в которых используется ПО, определяется ущерб, наносимый программными помехами, присутствующими в ПО.

При анализе ПО следует учитывать, является ли рассматриваемая ИС сосредоточенной или распределенной, структуру системы, возможные каналы утечки информации и ввода управляющих воздействий, например по активизации программных помех в ИС. Необходимо принимать во внимание удаленность предполагаемых злоумышленников от ИС, степень информированности фирм-разработчиков ПО об особенностях рассматриваемой ИС и решаемых ею задач, используемых аппаратных и программных средствах защиты, ее физической и логической организации.

Важное значение при анализе ПО на соответствие требованиям безопасности имеет учет характеристик вычислительной среды, уровня изолированности ПО в ИС, условий перехода к уровню с более высокими привилегиями (по управлению ресурсами системы), уязвимости элементов ИС.

Необходимо оценивать возможные угрозы ИС со стороны ПО. Среди таких угроз могут быть:

- непредусмотренное прерывание вычислительного процесса;
- стирание или искажение полезной информации в памяти ИС;
- внедрение в чистые программы мешающих процедур, создающих побочные эффекты;
- перегрузка памяти ИС;
- считывание или перехват ценной информации;
- выдача ошибочных (ложных) результатов решения задач;
- увеличение времени решения системных и прикладных задач и др.

С учетом всех этих обстоятельств должен быть составлен план проведения стендовых испытаний.

Требования к обеспечению испытаний (720)

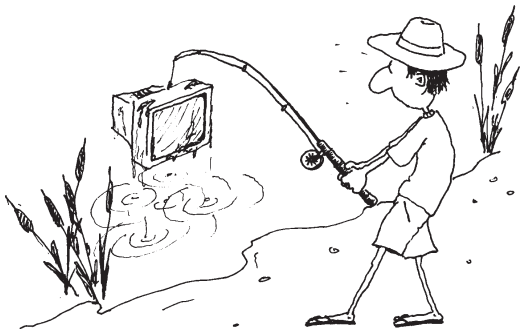
Научно-методическое обеспечение процесса испытаний ПО на соответствие требованиям безопасности представляет собой комплекс базовых методик, охватывающий процесс от анализа требований по показателям безопасности до принятия решения о соответствии требованиям и, при необходимости, расчета рисков. При проведении испытаний конкретной реализации программного обеспечения (ПО) на основе базовых методик создается частная методика испытаний данного конкретного ПО.

Базовые методики, как правило, являются плодом многолетнего труда серьезных научных подразделений. В ходе практических сертификационных испытаний они постоянно модифицируются и совершенствуются. Базовые методики должны быть согласованы с органом по сертификации при выдаче испытательной лаборатории лицензии на право проведения сертификационных испытаний.

Требования к техническому и инструментальному обеспечению испытательной лаборатории, вообще говоря, определяются испытываемым программным обеспечением. При разработке частной методики испытаний создается испытательный стенд с требуемой конфигурацией технических средств и соответствующим программным обеспечением.

Круг задач испытательной лаборатории предъявляет крайне высокие требования к квалификации ее сотрудников. В ее состав должны входить с***пециалисты, хорошо подготовленные по вопросам:***

- действующих отечественных и международных законов в области информатики и авторского права;
- состояния отечественного и международного рынка ПО, деятельности на нем основных производителей и поставщиков ПО, их репутации;
- теории и практики методов воздействия на целостность ПО;
- системного программирования и работы с исполняемыми кодами программ;



Так создается испытательный стенд...

- распространенных языков программирования;
- методов верификации;
- устройства и работы технических средств.

Короче говоря, сотрудник испытательной лаборатории должен иметь подготовку и опыт работы не ниже уровня высококвалифицированного хакера. Кроме того, испытательная лаборатория должна иметь возможность привлечения при необходимости к работе экспертов “со стороны”.

Особенности стендовых испытаний (720)

При проведении испытаний особое внимание следует уделять формированию рабочей группы для выполнения конкретного заказа (специалисты лаборатории и приглашенные эксперты), должен быть выделен ответственный исполнитель, наделенный особыми полномочиями по руководству ходом испытаний, взаимодействию с заказчиком и ответственный за результаты.

Крайне важно для репутации лаборатории, чтобы любая информация об испытуемом ПО не вышла за ее стены и не могла быть использована в самой лаборатории для работ, не связанных с заказом (в этом смысле предпочтительнее, чтобы организация-испытатель не имела функций разработчика ПО, дабы не было соблазна использования чужих алгоритмов и программ, ставших известными в ходе испытаний).

При обнаружении в ходе испытаний несоответствия требованиям оно должно быть зафиксировано, но программа испытаний должна быть выполнена до конца, поскольку заказчика может устроить класс защиты более низкий, чем заявленный первоначально. При обнаружении несоответствия на каком-либо этапе испытатель не имеет права поддаваться на уговоры заказчика подправить что-либо в ходе испытаний, сколь бы соблазнительными ни были предложения, т.к. внесенные изменения могут исказить результаты, полученные на более ранних этапах испытаний, что сведет к нулю всю работу.

После выполнения всей программы работ, получив отчет об испытаниях, заказчик может внести свои изменения и вновь отдать ПО на испытания как новую реализацию по новому договору. Цикл испытаний должен быть повторен сначала и в полном объеме.

Заказчик и испытатель должны представлять себе юридические особенности испытаний по требованиям безопасности ПО, разработчиком которого не является заказчик (например, импортного). С одной стороны, обнаружение в ПО недокументированных функций (например, программной закладки) влечет за собой юридические санкции к разработчику. С другой — методы, используемые испытателем для обнаружения непротоколированных функций (восстановление структуры и исходного текста ПО, обход защиты от дисассемблирования и т.п.), находятся на грани нарушения авторских прав разработчика, что может повлечь юридические санкции с его стороны. Поэтому перед началом испытаний эти вопросы должны быть юридически грамотно решены (например, получено разрешение разработчика на проведение испытаний).

Обработка результатов стендовых испытаний (720)

Чаще всего обработка результатов испытаний сводится к вычислению оценок статистических характеристик случайных величин с применением методов теории вероятностей. При предварительной обработке результатов устраняются искажения и погрешности в ходе испытаний, проверяется соответствие ранее высказанным гипотезам и выбираются исходные параметры для дальнейших расчетов.

В ходе первичной обработки испытаний может быть явно обнаружено несоответствие требованиям по безопасности. В ряде случаев программные помехи в ПО могут быть при испытаниях и не выявлены. Однако это не означает, что их нет. В этом случае можно лишь утверждать, что ПП отсутствует в ПО с какой-то степенью вероятности. Для определения вероятных оценок проводится полная обработка результатов испытаний. В ходе ее могут быть определены средние значения случайных величин, среднеквадратические отклонения их значений от математических ожиданий и др. Результаты обработки должны быть учтены при последующих испытаниях ПО.

Принятие решения по удовлетворению ПО заданным требованиям (720)

Решение по использованию испытуемого программного обеспечения в ИС должно приниматься на основании результатов стендовых испытаний и заданных требований по безопасности.

Принятие решения представляет собой выбор одного из двух вариантов; ПО подлежит использованию или ПО не подлежит использованию, пока не будут устранены преднамеренные и непреднамеренные программные помехи.

Протокол проведения испытаний (720)

Результатом испытаний является Протокол, в котором, не раскрывая методов и средств испытаний, перечисляются заявленные требования и результаты, полученные в ходе испытаний. В случае фиксации несоответствия требованиям подробно описывается методика обнаружения этого несоответствия с тем, чтобы этот этап испытаний мог быть повторен самим заказчиком или третьей стороной. К протоколу прилагается заключение о проведении испытаний, в котором делается вывод о степени соответствия требований, а в случае заявки на сертификационные испытания — рекомендации органу по сертификации о целесообразности выдачи сертификата. Особо следует отметить важность перечисления в Заключении эксплуатационных ограничений — испытатель должен перечислить аппаратно-программное окружение ПО, в котором оно фактически испытано. Протокол испытаний и Заключение составляют Отчет об испытаниях, который предоставляется заказчику.

Резюме

Цель сертификации — сделать защищенность информационных систем очевидной и сравнимой, так, чтобы с одной стороны, предоставить пользователям детализированную информацию и помощь при выборе системы, а с другой — дать заинтересованным изготовителям подтверждение качества их продукции.

Проведение работ по сертификации продукции может быть доверено только организациям, имеющим необходимый уровень компетентности в данной области, что предполагает наличие в них высококвалифицированных специалистов в области безопасности информации.

Применение защищенной информационной техники экономически эффективнее, чем последующее осуществление мер безопасности с целью компенсировать первоначальное отсутствие мер защиты. При наличии сертификата безопасности защитные функции продукта могут быть реально оценены и оптимально использованы в рамках концепции безопасности.

Сертификат выдается не на определенный тип продукта, а на определенную версию продукта и имеет силу только для этой версии. Это значит, что если после сертификации готового продукта через короткий промежуток времени, обусловленный жизненным циклом данного продукта, на рынке появляется его новая версия, для нее сертификат не действителен.

Гарантия качества обеспечивается поддержкой надлежащим образом функционирующей и документально оформленной системой качества. Тем самым гарантируется, что качество будет закладываться по мере проведения разработки, а не определяться в конце данного процесса.

Научно-методическое обеспечение процесса испытаний средств защиты на соответствие требованиям безопасности представляет собой комплекс базовых методик, охватывающий процесс от анализа требований по показателям безопасности до принятия решения о соответствии требованиям и, при необходимости, расчета рисков.