Задание подготовлено в рамках проекта АНО «Лаборатория модернизации образовательных ресурсов» «Кадровый и учебно-методический ресурс формирования общих компетенций обучающихся по программам СПО», который реализуется с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

**Разработчик**

Плюснина Елена Викторовна, ГБПОУ «Тольяттинский социально-экономический колледж»

**Назначение задания**

Обработка информации. Уровень I

09.02.07 Информационные системы и программирование (специалист по информационным системам)

МДК.07.02 Сертификация информационных систем

Тема: Сертификация информационных систем

**Комментарии**

После предъявления обратной связи имеет смысл продолжить обсуждение тезис с привлечением аргументации от обучающихся.

Внимательно изучите информацию о проведении сертификации и публикацию блогера, «разверчивающую мифы» вокруг сертификации программного обеспечения.

**Сформулируйте и запишите аргументы, основывающиеся на записи в блоге, в поддержку тезиса и в опровержение тезиса «Сертификация не является гарантом качества ПО».**

Не переписывайте фрагменты источников дословно.

Аргумент в поддержку тезиса:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Аргументы на опровержение тезиса:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Для справки:*

Тезис - суждение, требующее доказательств.

Аргумент - истинное суждение, независимое от тезиса, позволяющее обосновать или опровергнуть тезис.

***Источник 1***

**Что такое сертификация программного обеспечения**

Во всем мире сегодня практикуется тестирование кода информационных систем по требованиям безопасности информации. На Западе обязательные проверки предусмотрены для государственных и платежных программных систем, а банки, брокерские, инвестиционные, страховые и сервисные компании, предоставляющие услуги в индустрии недвижимости и в Интернете, проходят добровольный аудит. В нашей стране традиционно преобладают директивные методы оценки соответствия, в частности программное обеспечение ряда информационных систем подлежит обязательной сертификации по требованиям безопасности информации. Исторически система сертификации по требованиям безопасности информации в России возникла после распада СССР, когда появилась потребность в контроле безопасности зарубежного программного обеспечения, а также качества российских программных систем, связанных с обработкой и защитой государственной тайны. Активными участниками процесса сертификации стали Минобороны, ФСБ и ФСТЭК.

До недавнего времени сертификация главным образом касалась силовых министерств и предприятий промышленности, выполняющих государственные заказы, а основная масса специалистов в области информационных технологий мало интересовалась данной проблемой. Ситуация значительно изменилась с принятием ФЗ-152 «О персональных данных» и последовавших за ним нормативно-методических документов. Оказалось, что сертификация программного обеспечения (далее ПО) и аттестация объектов информатизации необходима большинству коммерческих компаний и всем государственным организациям, работающим в области медицины, образования, транспорта.

В общем случае под сертификацией принято понимать независимое подтверждение соответствия тех или иных характеристик товаров или услуг некоторым требованиям. В нашем случае речь идет о программных средствах защиты или программ в защищенном исполнении. Соответственно в качестве требований выступают нормативные документы и документация, касающаяся безопасности информации.

В Российской Федерации действует несколько ГОСТ и ГОСТ Р, согласно которым ПО проверяется по следующим параметрам:

* надежность - насколько ПО защищено от сбоев и насколько способно поддерживать работоспособность после сбоев и ошибок;
* защита информации;
* эффективность - соотношение функциональности и затрачиваемых ресурсов вычислительной техники;
* функциональные возможности - соответствует ли программный продукт потребностям;
* практичность - насколько удобно использовать ПО;
* мобильность - насколько ПО может быть интегрировано в различные операционные системы.

Добровольный сертификат на ПО позволяет вам занять более выгодные позиции на рынке, а вашим потребителям показывает, что продукции можно доверять. Таким образом, косвенно его оформление повышает продажи и укрепляет ваши позиции в конкурентной среде, увеличивает доверие со стороны партнеров и инвесторов.

Принципиальная особенность любых сертификационных испытаний - это независимость испытательной лаборатории, проводящей испытания, и сертифицирующей организации, осуществляющей независимый контроль результатов испытаний, проведенных лабораторией. В общем случае схема проведения сертификации выглядит следующим образом.

1. Заявитель (разработчик либо другая компания, заинтересованная в проведении сертификации) подает в федеральный орган по сертификации заявку на проведение сертификационных испытаний некоторого продукта.
2. Федеральный орган определяет аккредитованную испытательную лабораторию и орган по сертификации.
3. Испытательная лаборатория совместно с заявителем проводит сертификационные испытания. Если в процессе испытаний выявляются те или иные несоответствия заявленным требованиям, то они могут быть устранены заявителем в рабочем порядке (что и происходит в большинстве случаев), либо может быть принято решение об изменении требований к продукту, например о снижении класса защищенности. Возможен вариант, когда сертификационные испытания завершаются с отрицательным результатом. Наиболее нашумевшим в прессе примером можно назвать случай, когда испытательная лаборатория НИИ ВМФ после года проверок выдала отрицательное сертификационное заключение на программные изделия специального назначения. Известны как минимум пять случаев, когда определенные версии ОС и СУБД не смогли получить сертификат на отсутствие недекларированных возможностей по причине потери части исходного кода старых модулей. Если посмотреть реестр ФСТЭК, то можно заметить, что ряд программных систем защиты (например, СУБД Oracle и система безопасности приложений IBM Guardium) получили сертификаты лишь на соответствие техническим условиям, а не на соответствие руководящему документу Гостехкомиссии. Это значит, что орган по сертификации посчитал, что не все требования руководящего документа подтверждены при испытаниях.
4. Материалы испытаний передаются в орган по сертификации, который проводит их независимую экспертизу. Как правило, в экспертизе участвуют не менее двух экспертов, которые независимо друг от друга подтверждают корректность и полноту проведения испытаний.
5. Федеральный орган по сертификации на основании заключения органа по сертификации оформляет сертификат соответствия. В случае выявления каких-либо несоответствий федеральный орган может провести дополнительную экспертизу с привлечением экспертов из различных аккредитованных лабораторий.

В системах обязательной сертификации имеется практика отзыва и приостановления лицензий и аттестатов аккредитаций в случае выявления грубых нарушений в процессе сертификации.

**Системы сертификации и требования**

Деятельность российских систем сертификации в РФ регламентируется Федеральным законом № 184 «О техническом регулировании». Сертификация средств защиты информации может быть добровольной или обязательной, проводимой главным образом в рамках Минобороны, ФСБ и ФСТЭК. Для большинства коммерческих компаний термин «сертификация» является синонимом понятий «сертификация в системе ФСБ» для криптографических средств защиты и «сертификация в системе ФСТЭК» для всех остальных продуктов. Однако необходимо иметь в виду, что, помимо криптографии, к компетенции ФСБ относятся средства защиты информации, применяемые в высших органах государственной власти. Система сертификации средств защиты информации Минобороны, в свою очередь, ориентирована на программные изделия, применяемые на объектах военного назначения.

Добровольные системы сертификации средств защиты информации на сегодняшний день не получили широкого распространения. Единственной сколько-нибудь было заметной из такого рода систем является «АйТи-Сертифика». К сожалению, несмотря на то что в добровольных системах можно получить сертификат на соответствие любому нормативному документу по защите конфиденциальной информации, при аттестации объектов информатизации такие сертификаты ФСТЭК России не признаются.

Что касается документов, на соответствие которым проводятся сертификационные испытания, то они практически идентичны во всех системах сертификации. Существуют два основных подхода к сертификации и соответственно два типа нормативных документов.

1. Функциональное тестирование средств защиты информации, позволяющее убедиться в том, что продукт действительно реализует заявленные функции. Это тестирование чаще всего проводится на соответствие конкретному нормативному документу - например, одному из руководящих документов Гостехкомиссии России. Такие документы установлены, например, для межсетевых экранов и средств защиты от несанкционированного доступа. Если же не существует документа, которому сертифицируемый продукт соответствовал бы в полной мере, то функциональные требования могут быть сформулированы в явном виде, например, в технических условиях, или в виде задания по безопасности (в соответствии с положениями стандарта ГОСТ Р 15408).
2. Структурное тестирование программного кода на отсутствие недекларированных возможностей. Классическим примером недекларированных возможностей являются программные закладки, которые при возникновении определенных условий инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию (по ГОСТ Р 51275-99). Выявление недекларированных возможностей предполагает проведение серии тестов исходных текстов программ, предоставление которых является необходимым условием для возможности проведения сертификационных испытаний.

В большинстве случаев средство защиты информации должно быть сертифицировано как в части основного функционала, так и на предмет отсутствия недекларированных возможностей. Делается исключение для систем обработки персональных данных второго и третьего класса с целью снижения затрат на защиту информации для небольших частных организаций. Если программное средство не имеет каких-либо механизмов защиты информации, оно может быть сертифицировано только на предмет отсутствия недекларированных возможностей.

***Источник 2***

**Мифология вокруг сертификации**

Процесс организации и проведения испытаний в любой системе сертификации жестко формализован, однако отсутствие у большинства ИТ-специалистов опыта участия в таких испытаниях, а также взаимодействия с регуляторами рождает ряд мифов и заблуждений, касающихся вопросов сертификации.

Миф №1: сертификация - это торговля.

К сожалению, часть потребителей искренне считает любую сертификацию формальной процедурой получения разрешительной документации, естественно, коррумпированной и абсолютно бесполезной. Поэтому для многих заявителей становится шоком тот факт, что предъявляемые для сертификации средства защиты действительно серьезно проверяются, причем результат проверки может быть отрицательным. Независимый контроль органов по сертификации над испытательными лабораториями гарантирует отсутствие сговора между заявителем и лабораторией.

Миф №2: сертификацию проводят государственные органы.

Безусловно, федеральные органы всех обязательных систем сертификации являются государственными, однако испытательные лаборатории и органы по сертификации могут иметь любую форму собственности, и на практике большинство из них - коммерческие организации.

Миф № 3: сертификация нужна только госструктурам.

На самом деле любого конечного заказчика интересует аттестация объекта информатизации - формальное подтверждение того, что автоматизированная система является защищенной. В большинстве случаев для успешного прохождения аттестации система должна строиться с использованием исключительно сертифицированных средств защиты. Это справедливо не только для систем, относящихся к государственному информационному ресурсу, но и для систем, связанных с обработкой персональных данных. Можно встретить требования по обязательной сертификации программной продукции даже независимо от вида защищаемых тайн; например, такие требования имеются для систем, работающих с кредитными историями граждан, игровых систем в случаях предоставлении доступа к ресурсам из сетей международного обмена и др.

Миф № 4: зарубежный продукт нельзя сертифицировать.

В действительности продукты таких разработчиков, как Microsoft, IBM, SAP, Symantec, Trend Micro и т.д., успешно проходят сертификационные испытания, в том числе и на отсутствие недекларированных возможностей. Как правило, зарубежные компании не передают исходные тексты в Россию, поэтому испытания проводятся с выездом к разработчику. Число зарубежных продуктов, проходящих сертификацию в России, с каждым годом увеличивается. Сегодня около 20 зарубежных компаний, в том числе Microsoft, IBM, Oracle и SAP, предоставили исходные коды своих продуктов для сертификационных испытаний. За последние пять лет почти 40 зарубежных продуктов получили сертификаты на отсутствие недекларированных возможностей.

Миф № 5: сертифицирован - значит защищен.

Это не совсем так. Правильной была бы формулировка: продукт сертифицирован, значит, соответствует тем или иным требованиям. При этом потребитель должен четко понимать, на соответствие чему именно сертифицировано средство защиты, чтобы убедиться, действительно ли в ходе проведения испытаний проверялись характеристики продукта, которые его интересуют. Если испытания продукта проводились на соответствие техническим условиям, то в сертификате это соответствие будет зафиксировано, но при этом потребитель, не прочитав технические условия на продукт, в принципе не может определить, какие характеристики проверялись, что создает предпосылки для обмана неквалифицированного потребителя. Аналогичным образом наличие сертификата на отсутствие недекларированных возможностей ничего не говорит о функциональных возможностях продукта.

Очень важно ознакомиться с ограничениями на использование продукта, которые указаны в технических условиях: конкретные операционные среды и платформы, режимы работы, конфигурации, применение дополнительных средств защиты и др. Например, сертификат на некоторые версии операционных систем Windows и МСВС действителен только с модулем доверенной загрузки. Почти все сертификаты на внешние средства защиты действительны только для конкретных версий операционной системы, а в ограничениях на использование ряда средств доверенной загрузки указывается, что должна быть обеспечена физическая защита компьютера.

Миф № 6: при сертификации ничего не находят.

В рамках сертификационных испытаний эксперты тщательно инспектируют исходный код (в случае его предоставления), а также проводят различные варианты нагрузочного тестирования. Кроме того, они изучают различные бюллетени по безопасности продуктов и сред их функционирования. В результате этого опытная лаборатория получает список критических уязвимостей, которые заявитель должен исправить или описать в документации. Например, при сертификации выявляются такие уязвимости, как встроенные пароли и алгоритмы их генерации, архитектурные ошибки (некорректная реализация дискретного и мандатного принципов доступа и т. п.), некорректности программирования (уязвимости к переполнению буфера, ошибки операторов логики и времени, гонки, возможность загрузки недоверенных файлов и др.), а также ошибки обработки данных приложений (SQL-инъекции, кросс-сайтовый скриптинг), реализация которых может существенно снизить уровень безопасности системы. Согласно нашей практике, в 70% проверенного коммуникационного оборудования обнаруживались встроенные мастер-пароли, а почти в 30% проверяемых операционных систем были выявлены ошибки реализации системы разграничения доступом. Зафиксированы также случаи, когда в продуктах присутствовали даже логические временные бомбы.

Миф № 7: продукт сертифицирован на отсутствие недекларированных возможностей - значит в нем нет уязвимостей.

На сегодняшний день нет методов гарантированного выявления всех возможных уязвимостей программного обеспечения. Успешное прохождение сертификации на отсутствие недекларированных возможностей гарантирует обнаружение лишь определенного класса уязвимостей, выявляемых с использованием конкретных методов. С другой стороны, прохождение сертификации на отсутствие недекларированных возможностей гарантирует наличие у разработчика системы качества производства программ, то есть найдены и зафиксированы все реальные исходные тексты и компиляционная среда, компиляция и сборка могут быть гарантировано повторены, а также имеется русскоязычная документация.

Миф № 8: требования по анализу исходного кода существуют только в нашей стране.

Часто можно столкнуться с критикой строгости отечественной сертификации, связанной с предоставлением исходных текстов программ. Действительно, в международной системе сертификации Common Criteria допускается проведение испытаний продукции, обрабатывающей информацию, не отнесенную к гостайне, без предоставления исходных кодов, однако в этом случае должны быть обоснованы проверки на отсутствие скрытых каналов и уязвимостей. Для систем обработки гостайны и платежных систем предусмотрен структурный анализ безопасности исходного кода. Требования по аудиту безопасности исходного кода коммерческих программных продуктов можно найти в международных стандартах PCI DSS, PA DSS и NISTIR 4909.

Инструмент проверки

Внимание!

* Следует оценивать соответствие суждений модельному ответу по смыслу. Обучающийся может использовать другую вербализацию.
* Аргументы на опровержение могут следовать в любом порядке.

В поддержку тезиса:

1. Сертификация гарантирует

качество программного обеспечения только в том аспекте, по которому оно проходило сертификацию (1) \\

только соответствие выносимых на сертификацию характеристик программы исключительно требованиям того документа, на соответствие которому проводилась сертификация (1)

другие важные покупателю характеристики программы могут не соответствовать его ожиданиям \ заявленным характеристикам (2) \\

программное обеспечение может содержать уязвимости в той части, которая не выносилась на сертификацию \ в которой оно не проходило сертификацию.

На опровержение тезиса:

1. Статистика решений по сертификации свидетельствует (3), что в процессе сертификации выявляются (и исправляются разработчиком) (все \ многие) несоответствия ПО требованиям, на соответствие которым проводилась сертификация.
2. Успешное прохождение сертификации программным обеспечением свидетельствует о том, что у разработчика имеется система качества (4), что существенно повышает вероятность качества ПО и в отношении тех характеристик, по которым оно не проходило сертификацию (5).

*Подсчет баллов*

|  |  |
| --- | --- |
| За каждый верный элемент аргумента | 1 балл |
| ***Максимальный балл*** | ***5 баллов*** |