УДК 004.415.5

ОСОБЕННОСТИ СЕРТИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Лебедь Оксана Олеговна, Масальская Елена Александровна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: Ksy4308@yandex.ru

Во всем мире сегодня практикуется тестирование кода информационных систем по требованиям безопасности информации, однако, несмотря на расширение практики сертификации, вокруг него сложился ряд заблуждений.

Ключевые слова – система сертификации; безопасность конфиденциальной информации.

ВВЕДЕНИЕ

В нашей стране традиционно преобладают директивные методы оценки соответствия, а программное обеспечение ряда информационных систем подлежит обязательной сертификации по требованиям безопасности информации.

Исторически система сертификации по требованиям безопасности информации в Украине возникла после распада СССР, когда появилась потребность в контроле безопасности зарубежного программного обеспечения, а также качества украинских программных систем, связанных с обработкой и защитой государственной тайны.

ОСНОВНЫЕ ЦЕЛИ СЕРТИФИКАЦИИ

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.

Оказывается, что сертификация программного обеспечения и аттестация объектов информатизации необходима большинству коммерческих компаний и всем государственным организациям, работающим в области медицины, образования, транспорта. В связи с этим возникло множество вопросов и, как правило, негативных суждений, связанных в большинстве случаев с недопониманием сути и процессов сертификации.

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 [1].

ОСОБЕННОСТИ ПРОВЕДЕНИЯ СЕРТИФИКАЦИИ

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 государсвенную службу специальной связи по сертификации заявку на проведение сертификационных испытаний некоторого продукта.
2. Государственный 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.
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. Государственный орган по сертификации на основании заключения органа по сертификации оформляет сертификат соответствия. Надо сказать, что в случае выявления каких-либо несоответствий государственный орган может провести дополнительную экспертизу с привлечением экспертов из различных аккредитованных лабораторий и органов.

В системах обязательной сертификации имеется практика отзыва и приостановления лицензий и аттестатов аккредитаций в случае выявления грубых нарушений в процессе сертификации [2].

СИСТЕМЫ СЕРТИФИКАЦИИ И ТРЕБОВАНИЯ К НИМ

Сертификация средств защиты информации может быть добровольной или обязательной. Добровольные системы сертификации средств защиты информации на сегодняшний день пока еще не получили широкого распространения. 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 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. 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.

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. 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 [3].

ВЫВОДЫ

Сертификация не является универсальным способом решения всех существующих проблем в области информационной безопасности, однако сегодня это единственный реально функционирующий механизм, который обеспечивает независимый контроль качества средств защиты информации, и пользы от него больше, чем вреда. При грамотном применении механизм сертификации позволяет вполне успешно решать задачу достижения гарантированного уровня защищенности автоматизированных систем.

Заглядывая вперед, можно предположить, что сертификация как инструмент регулятора будет изменяться в направлении совершенствования нормативных документов, отражающих разумные требования по защите от актуальных угроз, с одной стороны, и в направлении улучшения методов проверки критических компонентов по критерию «эффективность/время» – с другой.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Т. 2: Информационная безопасность. – К.: Арий, 2008, – 344 с.

2. Методы информационной защиты объектов и компьютерных сетей / А.В. Соколов, О.М. Степанюк. СПб.: ООО “Издательство Полигон”, 2000.

3. МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 27001 Первое издание 2005-10-15 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования