УДК 004

Особенности верификации средств защиты информации

Т. М. Каннер, Х. С. Султанахмедов
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрены особенности тестирования и верификации средств защиты информации (СЗИ). Предложен пример градации ошибок, полученных в результате тестирования СЗИ, а также предложен порядок действий при принятии решения о результатах верификации СЗИ на основе полученных данных.

Ключевые слова: тестирование СЗИ, верификация СЗИ, финализация, защитные функции, типы ошибок при верификации, уровень критичности ошибок.

Жизненный цикл разработки СЗИ, вне зависимости от его вида (программное или программно-аппаратное) состоит из следующих этапов:

- проектирование, включающее формирование требований;
- разработка, программирование;
- верификация, включающая тестирование;
- финализация и выпуск;
- исправление найденных при тестировании ошибок.

Все перечисленные этапы, кроме первого, как правило, приходится неоднократно повторять в процессе жизненного цикла любого продукта, в том числе и СЗИ.

Рассмотрим этап верификации, так как он является основополагающим при принятии решения о выпуске продукта на рынок.

В настоящее время существует достаточно большое количество разнообразных СЗИ. Некоторые обладают достаточно ограниченной функциональностью, некоторые реализуют целый комплекс инструментов, обеспечивающих защиту данных и гибкость в настройке способов защиты. В зависимости от перечня выполняемых задач СЗИ относятся к определенному классу, требования к которому определяют регулирующие органы нашей страны (ФСТЭК и ФСБ). На основании этих требований компанией-разработчиком формируются требования к конкретному СЗИ.

Вне зависимости от класса продукта до выпуска он должен быть проверен на соответствие предъявляемым к нему требованиям. Соответствие требованиям проверяется не только при первом выходе СЗИ на рынок, но и при выпуске последующих обновленных его версий. Для этого выполняется его тестирование, а затем, по результатам тестирования, верификация.

В общепринятом понимании верификация — это подтверждение соответствия выпускаемого продукта предъявляемым к нему требованиям. Верификация выполняется на основании проведения комплексного тестирования продукта, потому что именно тестирование приводит к выявлению всех ошибок и недочетов его работы, касающихся как удобства использования, так и нарушения работоспособности, а анализ полученных результатов позволяет сделать вывод о соответствии тестируемого продукта заявленным требованиям. Таким образом, получение результатов тестирования является основой для процесса верификации.

Верификация включает следующую последовательность действий:

- тестирование
  - выявление некорректного поведения продукта, указывающего на наличие в нем ошибок;
  - фиксация проявления ошибок;
  - локализация зафиксированных проявлений ошибок (поиск других проявлений и взаимосвязей);
  - анализ локализованных проявлений ошибок;
  - фиксация ошибок и особенностей;
- классификация ошибок и особенностей (определение типа, возможности компенсации, степени критичности);
- принятие решения об итогах верификации и о возможности финализации или возвращении на доработку.

В процессе тестирования используются специальные программы и методики тестирования (ПМИ), содержащие в себе определенные после-

Каннер Татьяна Михайловна, начальник отдела верификации и сопровождения продуктов.
E-mail: tatianash@okbsapr.ru
Султанахмедов Хизри Салихович, тестировщик.
E-mail: sultanahmedov@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

довательности действий и описания ожидаемых результатов. ПМИ составляются таким образом, чтобы охватить весь функционал продукта и получить наиболее полное представление о его работоспособности. При этом в случае СЗИ (в том числе содержащих аппаратную часть) тестируемый объект может находиться в различных стартовых условиях: разные операционные системы, разные аппаратные части и т. п. Эти условия являются входными данными для проведения тестирования. Для каждого такого набора условий тестирование по ПМИ выполняется отдельно. На основании каждого проведенного тестирования составляется таблица результатов, содержащая перечень всех выявленных проявлений ошибок. После этого тестировщик проводит локализацию ошибок путем исследования их выявленных проявлений и анализа возможных взаимосвязей с ранее встречавшимся неверным поведением продукта, если таковое было. На основании полученных от тестировщика данных программист устанавливает ошибку и сообщает тестировщику, какие функции может затрагивать обнаруженная ошибка. Тестировщик, в свою очередь, проверяет, оказывает ли данная ошибка влияние на указанный функционал продукта, а затем формирует окончательный список найденных ошибок и особенностей. Далее выполняется классификация зафиксированных ошибок и особенностей, которая включает определение типа ошибки, возможности ее компенсации, а также степени ее критичности.

Совокупность результатов всех тестирований на разных наборах входных данных является итоговой таблицей верификации, которая используется для анализа работоспособности продукта в целом и принятия решения об успешном завершении верификации. Важно помнить, что зачастую некоторые найденные в процессе тестирования ошибки могут быть исправлены достаточно быстро, еще до окончания верификации. Учитывая, что каждое внесенное исправление в один из модулей продукта может повлечь за собой изменение работы других модулей, необходимо провести повторное тестирование исправленного продукта по всей ПМИ. Таким образом, постоянное изменение верифицируемого объекта может привести к путанице в результатах и к так называемому, "бесконечному тестированию", что, в свою очередь, приведет к задержке выпуска продукта. Для предотвращения входа в бесконечный цикл тестирования необходимо либо принять решение о внесении исправлений в следующую версию и завершить верификацию текущей, с выносом вердикта относительно ее выпуска, либо остановить верификацию текущей версии и сразу приступить к верификации новой, максимально доработанной на текущий момент версии продукта.

Все перечисленные выше действия, выполняемые при тестировании и верификации любого продукта, выполняются и для средств защиты информации. Однако в случае СЗИ верификация проходит с учетом некоторых особенностей, касающихся анализа связи ошибок в функционировании с безопасностью защищаемой системы.

К ошибкам, выявленным при тестировании СЗИ, относятся как, например, опечатка в выдаваемом продуктом сообщении, так и ошибка, приводящая к неработоспособности самого СЗИ или даже всей защищаемой этим продуктом системы, а также нарушение безопасности защищаемой при помощи данного СЗИ системы. Очевидно, что эти ошибки неравнозначны с точки зрения работы продукта, поэтому необходима определенная градация всех найденных ошибок относительно их влияния на выполнение основной задачи СЗИ — защиты информационных ресурсов и обеспечения безопасности.

Шкала критичности ошибок индивидуальна и, как правило, предназначена для внутреннего использования компанией, производящей данное средство защиты. При этом важно понимать, что корректность оценки критичности ошибок является основополагающим фактором при принятии решения о возможности финализации.

Рассмотрим пример оценки критичности ошибок, найденных при тестировании СЗИ. Ошибки можно разделить на несколько типов:

1. *Ошибки интерфейса*.

К ним относятся недочеты в удобстве пользования интерфейсом, корректности отображения всех его элементов, опечатки в системных сообщениях и т. д. Эти ошибки не влияют на функциональность СЗИ и защищаемой им системы, а также на защищенность системы, их исправление необходимо для обеспечения комфортной работы пользователя с продуктом. Наличие таких недочетов не опасно для защищаемой системы, соответственно им присваивается минимальный уровень критичности.

2. *Ошибки, ограничивающие функциональность СЗИ, без нарушения его защитных функций*.

Этот тип ошибок накладывает некоторые ограничения на функциональность СЗИ, при этом не подвергая опасности защищаемую систему. То есть либо нефункционирующие опции СЗИ не отвечают непосредственно за безопасность защищаемой системы, либо отсутствие этих функций можно компенсировать за счет других средств без снижения уровня защищенности.

3. *Ошибки, связанные с нарушением защитных функций СЗИ.*

К этому типу относятся ошибки, способные повлиять на безопасность защищаемой системы из-за нарушения защитных функций СЗИ, которое создает предпосылки для успешной реализации атаки с использованием возникшей уязвимости. Очевидно, что они являются наиболее критичными и наличие даже одной ошибки этого типа может привести к завершению верификации запретом финализации и выпуска продукта, кроме тех случаев, когда это нарушение можно компенсировать дополнительными средствами, например, донастройкой политик ОС.

Следует отметить, что тестировщик не всегда может определить тип ошибки на основании ее проявлений без участия программиста. Поэтому привлечение программиста к анализу обнаруженных проявлений ошибок является обязательным условием, без которого нельзя точно зафиксировать ошибки, и если этого не сделать, то это может повлечь за собой неверную их классификацию. Например, если ошибка, найденная тестировщиком, проявляется в том, что при проверке электронной подписи (ЭП) файла, в который внесены изменения после ее простановки, выдается сообщении о корректности этой ЭП, то это может быть ошибка второго типа, когда неверно отрабатывает функция формирования сообщения о результатах проверки подписи. Однако к такому проявлению может приводить и ситуация, когда некорректно работает функция проверки ЭП. В данном случае это уже будет ошибка третьего типа, которая как раз может привести к нарушению безопасности системы и возможности реализации каких-либо атак со стороны злоумышленника. В описанном случае тестировщик самостоятельно не сможет разобраться, в чем именно суть возникшего проявления ошибки, и необходимо привлечение программиста для ее анализа и фиксации.

После классификации ошибок и особенностей, а также анализа полученных результатов остается подвести итог — выполняются ли все требования, предъявленные к данному СЗИ, или есть критические ошибки, приводящие к их нарушению (даже с учетом компенсационых мер) и не позволяющие принять решение о начале финализации. Если таких ошибок нет, то принимается решение о выпуске продукта на рынок, иначе — о задержке для последующей доработки и повторного тестирования и верификации.

Таким образом, для СЗИ справедливы все общепринятые нормы верификации, но при этом имеются свои особенности. Они касаются оценки критичности полученных при тестировании ошибок, так как необходимо провести подробный анализ всех возможных рисков, которым может подвергнуться защищаемая система в результате некорректного функционирования определенных модулей СЗИ.

Features of verification of Data Security Tools

T. M. Kanner, H. S. Sultanakhmedov
OKB SAPR JSC, Moscow, Russia

The article is devoted to the features of data security tools (DST) testing and verification. Author describes gradation of errors obtained in result of DST testing, as well as actions while making decisions about DST verification results, based on received information.

Keywords: DST testing, DST verification, finalization, protective functions, types of errors, errors' criticality level.

Received June 14, 2014