X[1]

Особенности верификации средств защиты информации

В век стремительного развития технологий и их внедрения во все сферы жизни человека особую роль начинает играть необходимость защиты информационных ресурсов.

Часто в организациях, заинтересованных в сохранении конфиденциальности обрабатываемыхданных, применяется организационный метод защиты информации, регулирующий физический доступ сотрудников к рабочим станциям. Однако, практически всегда одного организационного метода недостаточно для обеспечения безопасности от попыток получения несанкционированного доступа, и необходимо применениесредств защиты информации (СЗИ).

СЗИ, в зависимости от исполнения, бывают программными и программно-аппаратными. Независимо от вида, главной задачей этих продуктов является защита данных пользователей. Выполнение этой задачи может достигатьсяразличными методами, в числе которых, например, разграничение доступа к информационным ресурсам, криптографическая защита данных, контроль целостности программной и аппаратной частей рабочих станций.

Жизненный цикл СЗИ, вне зависимости от его вида, состоит из следующих этапов:

- проектирование, включающее формирование требований к продукту;
- разработка, программирование;
- тестирование, необходимое для проверки работоспособности и фиксации ошибок;
- верификация на основании проведенного тестирования;
- финализация и выпуск.

В данной статье рассмотрим предпоследний этап, так как он является основополагающим при принятии решения о выходе продукта на рынок.

В настоящее время существует достаточно большое количестворазнообразных СЗИ. Некоторые обладают достаточно ограниченной функциональностью, некоторые реализуют целый комплекс инструментов, обеспечивающих защиту данных и гибкость в настройке способов защиты. Разнообразие СЗИ на рынке закономерно приводит к необходимости определенной их классификации на основе выполняемых ими задач.На основании проведенной классификации,вырабатывается список требований, предъявляемых к СЗИ.

Вне зависимости от класса продукта, до выпуска он должен быть проверен на соответствие предъявляемым к нему требованиям. Соответствие требованиям проверяетсяне 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, его верификация.

В общепринятом понимании, верификация – это подтверждение соответствия выпускаемого продукта предъявляемым к нему требованиям. Верификация выполняется на основании проведенного комплексного тестирования функционала продукта,так как тестирование приводит к выявлению всех недочетов его работы системы, касающихся как удобства использования, так и нарушения работоспособности.

Верификацию можно разделить на несколько этапов, первый из которых является переходным этапом между тестированием и верификацией:

- формирование таблицы результатов тестирования, содержащей перечень ошибок и особенностей;
- оценка критичности выявленных ошибок;

[1] Текст является черновиком статьи, которая в дальнейшем была отредактивана и опубликована.

- анализ оценки критичности ошибок и особенностей, вывод о соответствии требованиям;
- принятие решения об окончании верификации и о возможности финализации.

В процессе тестирования используются специальные программы и методики тестирования (ПМИ), содержащие в себе определенные последовательности действий с отслеживанием полученного результата. 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 весь перечень найденных ошибок. Совокупность результатов всех тестирований на разных наборах входных данных является итоговой таблицей результатов тестирования, которая используется для анализа работоспособности продукта в целом.

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 вышеописанные принципы верификации справедливы и для средств защиты информации. Однако, в случае СЗИ, верификация проходит с учетом некоторых особенностей, касающихся анализа связи ошибок в функционировании с безопасностью данных в защищаемой системе.

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. 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. Именно этот этап является основополагающим 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 нарушают целостность СЗИ, не влияют на его функциональность, их исправление необходимо для обеспечения комфортной работы пользователя с продуктом. Наличие таких недочетов не опасно для защищаемой системы, соответственно присваивается минимальный уровень критичности.

2. Ошибки, ограничивающие функциональность СЗИ, без нарушения 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 защиту обрабатываемых данных, либо отсутствие этих функций можно скомпенсировать за счет других средствбез потери уровня защищенности.

3. Ошибки, нарушающие целостность системы защиты.

К этому типу относятся ошибки, приводящие к образованию «дыр» в защите, либо к полной неработоспособности СЗИ. Очевидно, что они являются наиболее критичными и наличие даже одной ошибки этого типа приводит к завершению верификации запретом выпуска продукта.

Следует отметить, что разделение полученных ошибок на второй и третий тип не всегда является тривиальной задачей, так как не всегда очевидно к чему впоследствии может привести нарушение в функционировании той или иной функции СЗИ. Например, если ошибка, найденная тестировщиком, проявляется в том, что в журнал СЗИ записывается информация с неправильным именем пользователя, то, это может быть ошибка второго типа, когда, например, некорректно работает функция записи в журнал (записывается не то, что происходит в действительности). Однако, если разобраться, то к такому проявлению может приводить и ситуация, когда, например, некорректно работает функция разграничения прав доступа (один пользователь имеет права доступа совершенно другого пользователя). . 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 описанной ситуации, тестировщик самостоятельно не сможет разобраться в чем именно суть проблемы, и необходимо привлечение программиста. Именно поэтому необходимо проведение анализа оценки критичности ошибок. Только на основании такого анализа можно принимать решение об итоге верификации.

После оценки полученных результатов остается вынести вердикт – выполняются ли все требования, предъявленные к данному СЗИ, или есть нарушения. На основании этого вердикта принимается решение о выпуске продукта на рынок, или 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.