УДК 004.056:004.75

А. Н. Давиденко, М. Р. Шабан, Киев

РАЗРАБОТКА МЕТОДИКИ ПРОВЕДЕНИЯ КОМПЛЕКСНИХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Abstract. Building a system of tests for safety analysis.

Государственная экспертиза КСЗИ в ИТС проводится согласно положению о государственной экспертизе в сфере технической защиты информации, утвержденным приказом Администрации Государственной службы специальной связи и защиты информации Украины от 16.05.2007 № 93, зарегистрированным в Министерстве юстиции Украины 16.07.2007 за № 820/14087 и НД ТЗИ 2.6-001-11 «Порядок проведения работ по государственной экспертизы средств технической защиты информации от несанкционированного доступа и комплексных систем защиты информации в информационно-телекоммуникационных системах».

Организатор экспертизы конкретной КСЗИ назначается Госспецсвязи после рассмотрения заявления на проведение государственной экспертизы, которую предоставляет владелец информационно-телекоммуникационной системы.

Проведение государственной экспертизы включает следующие основные этапы:

– анализ среды функционирования КСЗИ на соответствие требованиям НД ТЗИ;

– анализ технической, организационно-эксплуатационной документации на КСЗИ на соответствие требованиям НД ТЗИ;

– проведение экспертной оценки КСЗИ;

– оформление результатов экспертного оценивания - протокола экспертных испытаний в соответствии с требованиями НД ТЗИ.

Результатом проведения экспертизы является экспертое заключение содержащее в себе функциональный профиль услуг безопасности реализуемой системы и уровень гарантий определяющая степень доверия к ним. Рассмотрим особенности процедуры построения тестов в этом случае.

Обычно разлечают техническую диагностику и тестирование программного обеспечения. Первое рассматривает в основном аппаратную составляющую систем, вторая – программную. В большинстве случаев системы защиты являются комплексными, поэтому необходимо проводить комплексное тестирование совместно аппаратной и программной составляющей системы защиты информаций. Целью тестирование является проверка на соответствие требованием НД ТЗИ 2.5-004-99. Данный документ описывает требования к функциональным услугам безопасности (ФУБ)

поэтому тесты создаваемые в процессе подготовке должны, в первую очередь, носить характер функциональных.

Например, ISO 9126 – международный станадарт, определяющий оценочные характеристики качества программного обеспечения, рассматривает шесть структурных наборов характеристик. Из который нас интересует функциональность.

Функциональность – набор атрибутов характеризующий, соответствие функциональных возможностей программного обеспечения (ПО) набору требуемой пользователем функциональности. Особенностью [1] систем защиты является размытость понятия пользователь. В качестве пользователя может выступать как разработчик систем защиты, так и конечный пользователь для которого данная система разрабатовалось, так и эксперт выполняющий независимую оценку данной системы. При этом целью трех вышеперечисленных категорий пользователей между собой отличаются. Если целью разработчика является создание ситуаций при которой показывается максимальная эффективнсть системы защиты, целью конечного пользователя является определение минимально-гарантируемого уровня защиты. Целью эксперта является нахождение максимально-гарантируемого уровня защиты.

Тем немение все они заинтересованы в проверке функциональности как основного аспекта качества и основных его подхарактеристик. Это:

- пригодность к использованию (suitability);
- корректность (accuracy);
- совместимость (interoperability).

Кроме этого важным является проверка отсутствия деструктивных действий в процессе работы системы. Она не должна разрушать ваши данные, она не должна мешать работать другим программам, она не должна предоставлять доступ к данным тем, кому этот доступ не разрешен. Прочее аспекты рассматриваемые ISO 9126 такие как: надежность, практичность, эффективность, сопровождаемость, переносимость при тестировании не рассматриваются.

Наиболее частыми ошибками эксперта является восприятие процесса тестирование как части некой другой деятельности [2]. Тестирование на безопасность не является частью процесса разработки. Эксперт не имеет права на доработку и изменение тестируемой системы. Даже если тестировщики умеют программировать, в том числе и тесты (автоматизация тестирование = программирование), могут разрабатывать какие-то вспомогательные программы (для себя).

Тем не менее, тестирование — это не деятельность по разработке программного обеспечения. Тестирование на безопасность не является частью процесса анализа.Тестирование не анализ и не деятельность по сбору и анализу требований. Хотя, в процессе тестирования иногда приходится уточнять требования, а иногда приходится их анализировать. Но эта деятельность не основная, скорее, это приходится делать просто по

необходимости. В процессе тестирования появляются только определенные НД ТЗИ 2.6-001-11 документы. В процессе тестирования документация на систему не должна изменяться, однако тестировщикам приходится документировать свои тесты и свою работу.

Данные ошибки возникают так как тестировщику приходиться заниматься данными работами однако они делаются для обеспечения проведения тестирования, а не развития или модификации тетстируемой системы.

Одним из принятых подходов к классификации видов тестирования является разбиение на три уровня:

- модульное тестирование,
- интеграционное тестирование,
- системное тестирование.

Под модульным тестированием обычно подразумевается тестирование на достаточно низком уровне, то есть тестирование отдельных операций, методов, функций.

Под системным тестированием подразумевается тестирование на уровне пользовательского интерфейса.

При интеграционном тестировании мы проверяем, если в рамках какой-то системы модули взаимодействуют друг с другом корректно. То есть, мы фактически выполняем те же самые тесты, что и при системном тестировании, только еще дополнительно обращаем внимание на то, как именно модули взаимодействуют между собой. Выполняем некоторые дополнительные проверки.

Разница между системным и модульным тестированием проявляется при классификации по целям тестирования. Наиболее хорошо это видно при использовании «магического квадрата», который был изначально придуман Брайаном Мариком и потом улучшен Эри Тенненом. [Рис. 1]

В этом магическом квадрате все виды тестирования располагаются по четырем квадрантам в зависимости от того, чему в этих тестах больше уделяется внимания.

По вертикали — чем выше располагается вид тестирования, тем больше внимания уделяется некоторым внешним проявлениям поведения программы, чем ниже он находится, тем больше мы внимания уделяем ее внутреннему технологическому устройству программы.

По горизонтали — чем левее находятся наши тесты, тем больше внимания мы уделяем их программированию, чем правее они находятся, тем больше внимания мы уделяем ручному тестированию и исследованию программы человеком.

В частности, в этот квадрат можно легко вписать такие термины как приемочное тестирование, Acceptance Testing, модульное тестирование именно в том понимании, в котором оно чаще всего употребляется в литературе. Это низкоуровневое тестирование с большой, с подавляющей

долей программирования. То есть это все тесты программируются, полностью автоматически выполняются и внимание уделяется в первую очередь именно внутреннему устройству программы, именно ее технологическим особенностям.

В правом верхнем углу у нас окажутся ручные тесты, нацеленные на внешнее какое-то поведение программы, в частности, тестирование удобства использования, а в правом нижнем углу у нас, скорее всего, окажутся проверки разных нефункциональных свойств: производительности, защищенности и так далее.

Рис.1 Магический квадрат

Так вот, исходя из классификации по целям, модульное тестирование у нас оказывается в левом нижнем квадранте, а все остальные квадранты — это системное тестирование.

По методам тестирования можно классифицировать, например, как тестирование чёрного ящика или поведенческое тестирование — стратегия (метод) тестирования функционального поведения объекта (программы, системы) с точки зрения внешнего мира, при котором не используется знание о внутреннем устройстве тестируемого объекта. Под стратегией понимаются систематические методы отбора и создания тестов для тестового набора. Стратегия поведенческого теста исходит из технических требований и их спецификаций [3].

Под «чёрным ящиком» понимается объект исследования, внутреннее устройство которого неизвестно. Понятие «чёрный ящик» предложено У. Р. Эшби. В кибернетике оно позволяет изучать поведение систем, то есть их реакций на разнообразные внешние воздействия и в то же время абстрагироваться от их внутреннего устройства.

Манипулируя только лишь со входами и выходами, можно проводить определенные исследования. На практике всегда возникает вопрос, насколько гомоморфизм «чёрного» ящика отражает адекватность его изучаемой модели,

то есть как полно в модели отражаются основные свойства оригинала.

Описание любой системы управления во времени характеризуется картиной последовательности её состояний в процессе движения к стоящей перед нею цели. Преобразование в системе управления может быть либо взаимно-однозначным и тогда оно называется изоморфным, либо только однозначным, в одну сторону. В таком случае преобразование называют гомоморфным.

«Чёрный» ящик представляет собой сложную гомоморфную модель кибернетической системы, в которой соблюдается разнообразие. Он только тогда является удовлетворительной моделью системы, когда содержит такое количество информации, которое отражает разнообразие системы. Можно предположить, что чем большее число возмущений действует на входы модели системы, тем большее разнообразие должен иметь регулятор.

В настоящее время известны два вида «чёрных» ящиков. К первому виду относят любой «чёрный» ящик, который может рассматриваться как автомат, называемый конечным или бесконечным. Поведение таких «чёрных» ящиков известно. Ко второму виду относятся такие «чёрные» ящики, поведение которых может быть наблюдаемо только в эксперименте. В таком случае в явной или неявной форме высказывается гипотеза о предсказуемости поведения «чёрного» ящика в вероятностном смысле. Без предварительной гипотезы невозможно любое обобщение, или, как говорят, невозможно сделать индуктивное заключение на основе экспериментов с «чёрным» ящиком. Для обозначения модели «чёрного» ящика Н. Винером предложено понятие «белого» ящика. «Белый» ящик состоит из известных компонентов, то есть известных X, Y, δ, λ. Его содержимое специально подбирается для реализации той же зависимости выхода от входа, что и у соответствующего «чёрного» ящика. В процессе проводимых исследований и при обобщениях, выдвижении гипотез и установления закономерностей возникает необходимость корректировки организации «белого» ящика и смены моделей. В связи с этим при моделировании исследователь должен обязательно многократно обращаться к схеме отношений «чёрный» — «белый» ящик. Создание математического описания «черного» ящика является своего рода искусством. В некоторых случаях удается сформировать алгоритм, в соответствии с которым «черный» ящик реагирует на произвольный входной сигнал.

Основными приёмами тестирования чёрного ящика являются:

- эквивалентное разбиение;
- анализ граничных значений;
- анализ причинно-следственных связей;
- предположение об ошибке.

Тестировщик с большим опытом выискивает ошибки без всяких методов, но при этом он подсознательно использует метод предположения об ошибке. Данный метод в значительной степени основан на интуиции.

Основная идея метода состоит в том, чтобы составить список, который перечисляет возможные ошибки и ситуации, в которых эти ошибки могли проявиться. Потом на основе списка составляются тесты.

Возможно что, правильнее говорить о разных степенях прозрачности, а может быть даже вообще о разных цветах ящика, а не о тестировании методом черного и методом белого ящика. Важно только то, какую информацию мы принимаем во внимание когда проектируем тесты. Либо мы используем информацию о внутреннем устройстве программы, либо не используем.

На основе рассмотренного подхода были произведены испытания КСЗИ грид-сайта Украинского академического грид-узла ИТФ НАНУ. Испытания КСЗИ грид-сайта Украинского академического грид-узла ИТФ НАНУ предусматривало проведение таких видов испытаний:

- государственные испытания;
- опытная эксплуатация;
- государственная экспертиза.

Государственные испытания организовал собственник грид-узла Институт теоретической физики НАН Украины, а проводил разработчик КСЗИ Институт программных систем НАН Украины. Опытная эксплуатация проводилась разработчиком КСЗИ Институт программных систем НАН Украины. Государственную экспертизу организовал и провел Институт проблем моделирования в энергетике НАН Украины.

Объектом экспертизы является КСЗИ грид-сайта Украинского академического грид-узла Института теоретической физики НАН Украины, создана в соответствии к требованиям утвержденного с Администрацией Госспецсвязи Украины ТЗ на создание комплексной системы защиты информации, которая циркулирует в Украинском академическом грид-узле Института теоретической физики НАН Украины.

Испытаниям подлежали такие составляющие КСЗИ:

1) средства защиты и администрирования ОС;
2) средства защиты (сервисы безопасности) промежуточного ПО;
3) средства повышения доступности;
4) организационные мероприятия защиты информации, ПО и технический средств;
5) документация на КСЗИ согласно перечню, определенным требованиям ТЗ.

Целью испытаний КСЗИ являются:

- проверка реализации и достаточности приведенных в документации организационных мер защиты;
- проверка выполнения требований раздела 10 «Критерии гарантий» НД ТЗИ 2.5-004-99 для уровня гарантий корректности реализации функций безопасности Г2 в отношении архитектуры КСЗ, среды

разработки КСЗ, последовательности разработки КСЗ, среды функционирования КСЗ, документации и испытаний КСЗ.

Таблица 1 – Услуги функционального профиля защищенности, реализации которых проверяется

Критерии	Услуга	ФП-3	Уровень услуги для ФПЗ	Необходимые условия
Конфиден-циальность	Доверительная конфиденциаль-ность	КД-2	Базовая доверительная конфиденциальность	НИ-1
	Административная конфиденциаль-ность	КА-2	Базовая административная конфиденциаль-ность	НО-1, НИ-1
	Конфиденциаль-ность при обмене	КВ-1	Минимальная конфиденциаль-ность при обмене	--
Целостность	Доверительная целостность	ЦД-1	Минимальная доверительная целостность	НИ-1
	Административная целостность	ЦА-1	Минимальная административная целостность	НО-1, НИ-1
	Целостность при обмене	ЦВ-1	Минимальная целостность при обмене	--
Доступность	Устойчивость к отказам	ДС-1	Устойчивость при ограниченных отказах	НО-1
	Горячая замена	ДЗ-1	Модернизация	НО-1
	Восстановление после сбоев	ДВ-1	Ручное восстановление	НО-1
Наблюдае-мость	Регистрация (аудит)	НР-2	Защищенный журнал	НИ-1 НО-1
	Идентификация и аутентификация	НИ-2	Одиночная идентификация и аутентификация	НК-1
	Достоверный канал	НК-1	Однонаправленный достоверный канал	--
	Распределение обязанностей	НО-2	Распределение обязанностей администраторов	НИ-1
	Целостность КСЗ	НЦ-2	КСЗ с гарантированной целостностью	--
	Самотестирование	НТ-2	Самотестирования при старте	НО-1
	Идентификация и аутентификация при обмене	НВ-1	Аутентификация узла	--

Проведение государственных экспертизы КСЗИ с учетом требований ТЗ предусматривает в соответствии с программой и методикой государственных испытаний:

– проверку определенности и достаточности организационных мероприятий;
– проверку исполнения условий реализации услуг безопасности информации определенного в ТЗ функционального профиля защищенности (ФПЗ).

Проверка исполнения условий реализации услуг безопасности информации осуществляется в соответствии с ФПЗ:

З.КЦД = {КА-2, КД-2, КВ-1,
ЦА-1 , ЦД-1, ЦВ-1,
ДС-1, ДЗ-2, ДВ-1,
НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-2, НВ-1}

Описание услуг функционального профиля защищенности, реализация которых проверяется, приведена в таблице 1.

Таким образом на основе рассмотренных в статье положений была разработана методика проведения комплексной системы защиты информации Института теоретической физики подтвердившая соответствие к требованием НД ТЗИ в рамках указанного профиля ФУБ. Получен сертификат соответствия № 9434 от 13.12.2013 г.

1. *Зегжда Д.П, Ивашко А.М*. Основы безопасности информационных систем. Учеб. пособие для вузов, 2000,с.451
2. *Лупан А*., 2010. — http://testitquickly.com/2010/03/09/testing-basics-by-barancev/
3. *Бейзер Б.* Тестирование черного ящика. Технологии функционального тестирования программного обеспечения и систем. — Питер, 2004. — 320 с. — ISBN 5-94723-698-2.

Поступила 18.08.2014р.

УДК 004.051

О.С. Панова, К.М. Обельовська, НУ “Львівська політехніка”, Львів
Р.І. Ліскевич, ТзОВ “Українські промислові телекомунікації”, Львів

ДОСЛІДЖЕННЯ ВПЛИВУ С ПІВВІДНОШЕННЯ ТИПІВ ТРАФІКІВ НА ПРОДУКТИВНІСТЬ РОБОТИ БЕЗПРОВІДНОЇ МЕРЕЖІ

Abstract. Performance analysis of the wireless networks with different ratio of high-/low-priority traffic has been performed. Using a developed simulation model it was shown that for small and medium-sized wireless network its performance for the high-priority traffic does not depends on the amount of low-priority traffic in the network. And for the large wireless network its total performance decreases considerably depending on the ratio of high-/low-priority traffic in the network.

