5. Спосіб діагностування типу і ступеня тяжкості дихальної недостатності [Текст]: Пат. 23019 Україна: МПК7А61В 5/09 / Воронко А.А.; заявник та патентовласник Воронко А.А. - u200608338, заявл. 25.07.2006; опуб. 10.05.2007, Бюл. №6.
6. Способ оценки резервных возможностей организма человека [Текст]: Патент 2195858 Рос. Федерация: МПК7 А61В5/02 / Воронков Д.В., Соколов А.В., Баландин Ю.П., Лабутин Г.И.; заявитель и патентообладатель ООО "Центр медицинской профилактики "Валеомед". - №99108795/14; заявл. 06.05.1999; опуб. 10.01.2003.
7. Шмерлинг Д.С. Методы экспертных оценок [Электронный документ]. Режим доступа: http://www.intuit.ru/department/economics/expertmeth/ Проверено 21.04.2011.
8. Do maximum flow-volume loops collected during maximum exercise test alter the main cardiopulmonary parameters? / M. Bussotti, P. Agostoni, A. Durigato, C. Santoriello, S. Farina, V. Brusasco, R. Pellegrino // Chest – 2009. - V.135, №2. – P.425-433.
9. Expiratory flow limitation during exercise in competition cyclists / S. Mota, P. Casan, F. Drobnic, J. Giner, O. Ruiz, J. Sanchis, J. Milic- Emili// J Appl Physiol. – 1999. – V.86, №2. – P.611-616.
10. Ghosh A.K. Pulmonary capacities of different groups of sportsmen in India / A.K. Ghosh, A.Ahuja, G.L.Khanna // Br J Sports Med. – 1985. – V.19, №4. – P.232-234.
11. Milic Emili J. Mechanical work of breathing during maximal voluntary ventilation / J. Milic-Emili, M.M. Orzalesi // J Appl Physiol.– 1998.–V.85, №1.–P.254-258.
12. Noninvasive measurement of respiratory muscle performance after exhaustive endurance exercise / C. Perret, R. Pfeiffer, U. Boutellier, H.M. Wey, C.M. Spengler // Eur Respir J. – 1999. – V.14, №2. – P.264-269.
13. The effect of moderate altitude on some respiratory parameters of physical education and sports' students / O. Orhan, U. Bilgin, E. Cetin, E. Oz, B.E. Dolek // J Asthma. – 2010. – V.47, №6. – P.609-613.
14. The effects of learning on the ventilatory responses to inspiratory threshold loading / P.R. Eastwood, D.R. Hillman, A.R. Morton, K.E. Finucane// Am J Respir Crit Care Med. – 1998. – V.158, №4. – P.1190-1196.

УДК 681.324

ОРГАНІЗАЦІЯ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРИ ОЦІНЮВАННІ ЙОГО БЕЗПЕКИ

О.А. Авраменко
Кандидат технічних наук, доцент
Кафедра інженерії програмного забезпечення
Національний авіаційний університет
пр. Комарова, 1, м. Київ, Україна
Контактний тел.: 096-435-40-76
E-mail: alena.avramenko@livenau.net

Пропонується методика організації тестування при оцінюванні безпеки програмного забезпечення за національними критеріями НД ТЗІ 2.5-004-99
Ключові слова: програмне забезпечення, критерії оцінки безпеки

Предлагается методика организации тестирования при оценивании безопасности программного обеспечения по национальным критериям НД ТЗИ 2.5-004-99
Ключевые слова: программное обеспечение, критерии оценки безопасности

The organization method of testing at safety evaluation of software by the national criteria НД ТЗІ 2.5-004-99 is suggested.
Keywords: software, criteria of security evaluation

Вступ

Споживачі сучасних комп'ютерних систем стурбовані поширенням загроз безпеки інформації та потребують забезпечення певного рівня її захищеності. Слід зазначити, що рівень захищеності інформації в комп'ютерних системах оцінюється за національною нормативною базою, яка визначає відповідні критерії та методологію оцінки. В Україні використовуються так звані "національні критерії" (НК) [1].

Як відомо, одним з ключових компонентів системи захисту комп'ютерних систем є програмне забезпечення (ПЗ). У статті розглядаються деякі аспекти методики оцінки безпеки ПЗ за національними критеріями [1].

Загальна характеристика НК

Під час оцінки безпеки ПЗ експерт формує сукупність вимог до об'єкта оцінки (ОО). НК розрізняють вимоги двох видів:

1) функціональні, що містять вимоги до рівня реалізації захисту в ОО;

2) гарантій, що містять вимоги до коректності реалізації захисту.

Оцінка полягає у дослідженні ОО, яке спрямоване на виявлення його відповідності визначеним вимогам безпеки, і дозволяє експертам зробити висновок щодо захищеності ОО (рис. 1).

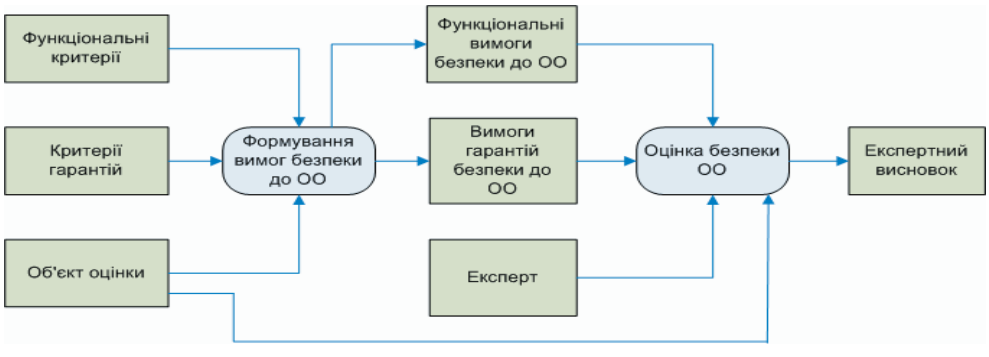

Рис. 1. Схема формування експертного висновку щодо безпеки ПЗ

Функціональні критерії розділяються на чотири групи в залежності від типа загроз інформації. Кожна з груп представлена у вигляді сукупності функціональних послуг безпеки, які є відображенням функціональних можливостей ОО, що дозволяють протистояти певній множині загроз. Кожна функціональна послуга безпеки містить множину вимог, яка структурована за рівнями, що відображають повноту захисту.

Відповідно до документу [2] функціональність ОО, що забезпечує захист, специфікується як функціональний профіль захищеності, який є переліком функціональних послуг безпеки та рівнів їх реалізації в ОО. Експерт здійснює оцінку ОО спираючись на визначений функціональний профіль захищеності.

Довіра до результатів оцінки реалізації функціональних послуг безпеки характеризується вимогами гарантій НК[1] , які визначають ступінь повноти та глибини дослідження ОО експертами.

Проблеми організації тестування при оцінці безпеки ПЗ за НК

Критерії гарантій включають вимоги до випробувань комплексу засобів захисту (КЗЗ) ОО, виконання яких дозволяє експерту оцінити ефективність і повноту випробувань, проведених розробником ПЗ. Для цього розробник надає експерту документацію щодо випробувань, яка включає план випробувань, програму, методику і результати випробувань [1]. Випробування можуть реалізовуватися шляхом виконання множини тестів, кожен з яких є технічною операцією, що виконується відповідно до специфікованої процедури для визначення однієї або кількох характеристик ОО [3].

При оцінці безпеки розрізняють тестування розробником та незалежне тестування. Розробник повинен надавати результати власного тестування ПЗ у вигляді, достатньому для його повторення. Незалежне тестування виконується незалежними експертами та верифікує результати тестів, наданих розробником. Незалежне тестування може проводися як повторення тестів розробника та доповнюватися тестами, створюваними незалежними експертами (рис. 2).

Основними характеристиками тестування є покриття та глибина. Тестове покриття є мірою, що характеризує здатність тестових даних випробовувати вимоги до ОО [4]. При оцінці безпеки ОО покриття визначає повноту охоплення тестами функціональності безпеки. Глибина тестування характеризує рівень деталізації тестів. Зростання рівня гарантій оцінки обумовлює підвищення деталізації процедур тестування. Для невисоких рівнів гарантій оцінки, як правило, застосовують функціональне тестування, що розглядає ОО як сукупність функціональних компонентів, кожен з яких тестується методом „чорного ящика"[5].

Практика тестування при проведенні оцінки безпеки ПЗ за НК виявила наступні проблеми, з якими зіштовхуються експерти:

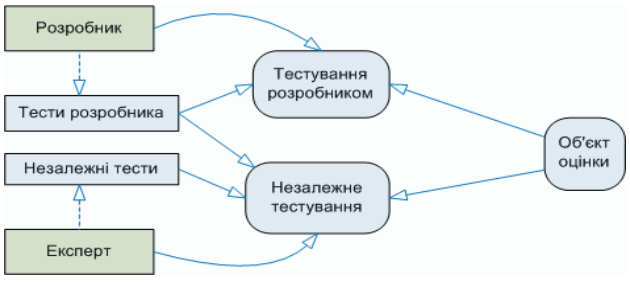

Рис. 2. Тестування при оцінці безпеки ОО

1) недостатня регламентація організації тестування та відсутність в контексті НК відповідної методології тестування, внаслідок чого організація тестування залежить від досвіду і кваліфікації експертів, які самостійно визначають порядок і методологію проведення тестування, рівень формалізації процедур тестування та порядок оформлення результатів. НК [1] при формулюванні вимог до організації випробувань посилаються на ДСТУ 2853-94 [6] та ДСТУ 2851-94 [7], які мають загальний характер;

2) відсутність чітких вимог до підтвердження достатності тестового покриття. НК не надають конкретних рекомендацій щодо методів, способів визначення та демонстрації повноти тестування;

3) відсутність вимог до глибини тестування залежно від рівня гарантій, що призводить до невизначених ситуацій, коли в процесі різних оцінок для одного рівня гарантій створюються тести з різним рівнем деталізації;

4) невизначеність методів та способів зіставлення результатів тестів з функціональністю ОО;

5) недостатня регламентація організації незалежного тестування третьою стороною.

Наявні елементи невизначеності при організації та оцінці результатів тестування найчастіше призводять до зниження рівня формалізації процедур і результатів тестування та до зростання фактора суб'єктивності роботи експертної комісії при аналізі, оцінці ОО і формуванні зваженого висновку.

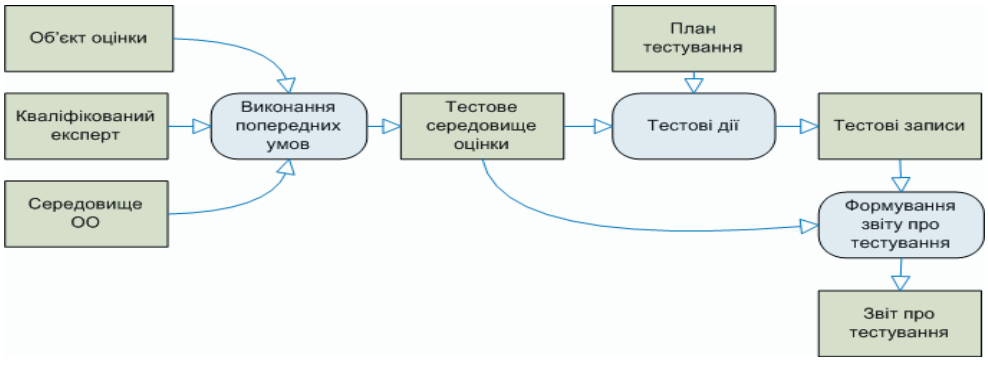

Рис. 3. Процес тестування згідно з ДСТУ ISO/IEC 12119:2003

Нормативна база методики з тестування безпеки ПЗ

Пропонується нормативну базу методики з тестування безпеки ПЗ базувати на положеннях наступних стандартів:

1) ДСТУ ISO/IEC 12119:2003 [3];

2) ГОСТ Р ИСО/МЭК 15408-1-02 [8].

Перший стандарт [3] містить рекомендації щодо тестування властивостей продуктів та пакетів програм на відповідність вимогам якості. Основними факторами, які обумовили вибір цього документу для організації тестування при проведенні оцінки безпеки ПЗ, є наступне:

1) документ структурує вимоги до якості ПЗ та містить інструкції щодо організації тестування цих вимог;

2) інструкції для тестування, розглянуті в документі, описують функціональне тестування (тестування методом „чорного ящика");

3) рекомендації щодо тестування спрямовані на тестування продукту, в першу чергу, третьою стороною.

Згідно з цим стандартом [3] мінімальним базовим компонентом при тестуванні встановлено **тестовий варіант**, який визначено як документовану інструкцію для тестувальника відносно функцій, що тестуються, опису специфікованої процедури та очікуваних результатів тестування.

Визначена сукупність тестових варіантів формує **план тестування**. Окрім цього, для реалізації тестових дій необхідно створити тестове середовище, яке передбачає виконання попередніх умов, а саме: наявність всіх елементів ОО, середовища функціонування ОО та кваліфікованого експерта (рис. 2).

Тестові дії передбачають виконання тестів у тестовому середовищі відповідно до плану тестування та отримання результатів тестування, в тому числі і негативних, тобто таких, що не відповідають очікуваним. Результати тестування оформлюються як тестові записи. Спираючись на результати тестування експерти складають **звіт про тестування**, який містить:

– ідентифікацію ОО;

– конфігурацію апаратного та програмного забезпечення;

– перелік документів, які використані при тестуванні;

– результати тестування;

– список невідповідностей вимогам;

– дату проведення тестування.

Стандарт [8] містить аспекти, які пов'язані з визначенням загальних характеристик тестування при оцінці безпеки ПЗ та форм представлення результатів тестування, що також робить корисним використання деяких його положень. Зокрема, стандарт рекомендує представляти повноту тестового покриття у вигляді таблиці зіставлення тестів з функціональною специфікацією ОО.

Основні засади методики тестування безпеки ОО

Базуючись на документах [1, 3, 8] пропонується методика тестування для оцінки безпеки ОО, яка забезпечує вирішення наступних задач:

– визначення функцій безпеки ОО, що підлягають тестуванню;

– формалізація плану тестування та тестових варіантів;

– мінімізація кількості та обсягу тестів;

– чітке зіставлення функціональності безпеки ОО та відповідних тестів;

– забезпечення демонстрації обсягу тестування та повноти тестового покриття.

Визначення функцій безпеки ОО, що підлягають тестуванню

В основі методики, яка пропонується для тестування при оцінці безпеки ПЗ, лежить чітке співставлення тестів з функціональністю ОО, що реалізує вимоги безпеки.

Для цього запроваджується поняття функції безпеки, яке представляє найменший ідентифікований елемент функціональності безпеки ОО. В такому разі, тестування спрямоване на підтвердження того,

що функції безпеки виконуються відповідно до їх специфікацій.

Визначення сукупності функцій безпеки, що реалізуються ОО, виконується в межах специфікації ОО щодо вимог безпеки. Експерти здійснюють специфікацію на основі опису ОО в документації розробника шляхом виділення функціональних можливостей ОО, що стосуються реалізації безпеки. Ці можливості структуруються відповідно до вимог безпеки. У запропонованій методиці запроваджено поняття сервісу безпеки, як іменованого елементу структуризації опису ОО розробником щодо функціональних можливостей безпеки ОО. Використання сервісів безпеки при специфікації ОО спрощує для експертів задачу формалізації та структуризації опису ОО у відповідності до структури НК [1]. Кожному сервісу безпеки ОО надається власна назва, яка може співпадати з назвою послуги, яку від реалізує, або відображає той факт, що сервіс містить механізми реалізації вимог декількох функціональних послуг безпеки НК. Наприклад, сервіс безпеки «Використання ресурсів» реалізує послугу НК «Використання ресурсів», а сервіс «Захист даних користувача» – послуги НК «Довірча конфіденційність», «Довірча цілісність» і «Повторне використання об'єктів».

Таким чином, опис ОО, наданий у специфікації розробника, структурується експертами у вигляді сукупності сервісів безпеки ОО. При співставленні сервісів безпеки ОО з елементами вимог функціональних послуг безпеки [1] кожний ідентифікований експертом перетин утворює функцію безпеки. Функціональність ОО описується експертами як множина функцій безпеки (рис. 4), специфікованих в межах сервісів безпеки. Визначена множина функцій безпеки є основою для подальшої розробки тестових варіантів і відображує обсяг тестування.

Формалізація плану тестування та тестових варіантів

Для зручності документування тестування кожен тестовий варіант унікально кодується (рис.5).

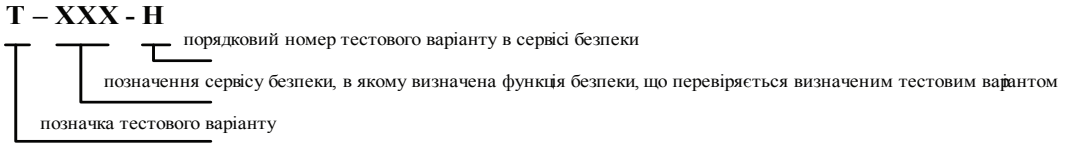

Рис. 5. Позначення тестового варіанту

План тестування представляється у вигляді переліку тестових варіантів для кожного сервісу безпеки. Безпосередньо сам тест містить наступне:

– твердження, що підлягає перевірці при тестуванні, а також описує очікуваний позитивний результат тестування;

– посилання на функції безпеки, які перевіряються цим тестом;

– необхідні умови для проведення тестування;

– опис дій тестувальника, який відображує порядок виконання тесту, тобто чітку узгоджену процедуру.

Відповідність структури тестового варінту згідно з методикою і ДСТУ ISO/IEC 12119:2003 [3] наведена у табл. 1.

Таблиця 1

Тестовий варіант згідно з методикою	Тестовий варіант згідно з ДСТУ ISO/IEC 12119:2003					
	мета тесту	функції, що тестуються	середовище тестування	дані тесту	процедура тестування	очікуваний результат
твердження, що перевіряється	X					X
функції безпеки		X				
необхідні умови			X	X		
опис дій тестувальника					X	

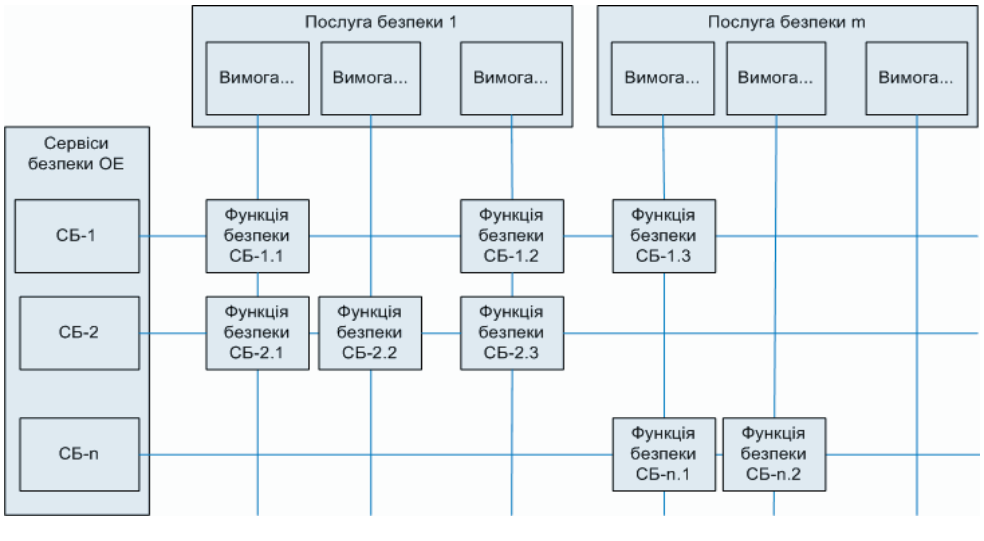

Рис 4. Схема формування множини функцій безпеки ОО

Мінімізація кількості тестів та обсягу тестування

Хоча методикою передбачено чітке та однозначне зіставлення тестів і функцій безпеки, кількість тестів і функцій безпеки не рівнозначне. Це обумовлюється наступним:

1) тестування однієї функції безпеки може виконуватися для різних категорій користувачів або із застосуванням різних зовнішніх

інтерфейсів, що потребує розробки та виконання для неї декількох тестів;

2) один тест може використовуватися для випробування декількох функцій безпеки. Наприклад, один тест може перевіряти як функцію перегляду журналу аудиту, так і функцію щодо наявності привілеїв користувача при доступі до цього журналу. В такому разі, позначка тестового варіанту містить позначення того сервісу безпеки, для якого вона первинно визначена;

3) для кожної функції безпеки розглядається два можливих результати: успішний та неуспішний. Наприклад, тест функції автентифікації із застосуванням паролю може передбачати успішний результат, якщо користувач увів вірний пароль, та випадок відмови у вході, якщо користувач увів невірний пароль;

4) для зниження обсягу робіт з розробки та виконання тестів методика передбачає можливість побудови тесту як виконання декількох інших, вже визначених тестів, та аналізу їх результатів. Наприклад для аналізу записів журналу безпеки, пов'язаних з певними подіями, необхідно виконати певні тести, за якими ці події реєструються у журналі.

Демонстрація обсягу тестування та повноти тестового покриття

Для демонстрації повноти тестового покриття та відстеження виконання тестів в процесі оцінки ОО формується матриця зіставлення тестових варіантів з функціями безпеки (рис. 6).

Тестові варіанти / Функції безпеки	Т-СБ-1-1	Т-СБ-1-2	Т-СБ-1-3	Т-СБ-1-4	Т-СБ-1-5	Т-СБ-2-1	Т-СБ-2-2	Т-СБ-2-3	Т-СБ-2-5	…	Т-СБ-n-1	Т-СБ-n-2	Т-СБ-n-3
Сервіс безпеки СБ-1													
СБ-1.1	x	x	x										
СБ-1.2		x	x	x	x								
СБ-1.3					x								
Сервіс безпеки СБ-2													
СБ-2.1			x				x						
СБ-2.2								x					
СБ-2.3							x		x				
Сервіс безпеки СБ-n													
СБ-n.1											x	x	
СБ-n.2													x

Рис. 6. Матриця зіставлення тестових варіантів з функціями безпеки ОО

Висновки

Запропонована методика тестування ОО при проведенні оцінки безпеки ПЗ дозволяє:

1) визначити сервіси безпеки ОО - елементи структуризації специфікацій розробника щодо функціональних можливостей безпеки ОО;

2) узгодити вимоги НК з визначеними сервісами безпеки ОО;

3) визначити функції безпеки – ідентифіковані елементи сервісів безпеки, що підлягають тестуванню на відповідність вимогам НК;

4) формалізувати співставлення тестів з функціональністю ПЗ та продемонструвати тестове покриття за допомогою матриці „функції безпеки – тести";

5) визначити чітку структуру опису тестів та результатів тестування.

Методика була випробувана в процесі експертизи сервісів безпеки операційних систем Microsoft Windows XP Professional [9], Windows Vista та системи Oracle E-Business Suite [10].

Література

1. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
2. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу.
3. ДСТУ ISO/IEC 12119:2003 Пакети програм. Тестування і вимоги до якості.
4. ДСТУ 3918-99 (ISO/IEC 12207:1995) Інформаційні технології. Процеси життєвого циклу програмного забезпечення.
5. Соммервил И. Инженерия программного обеспечения. – М.: Издательский дом «Вильямс», 2002. – 624с.
6. ДСТУ 2853-94. Програмні засоби ЕОМ. Підготовлення і проведення випробувань.
7. ДСТУ 2851-94. Програмні засоби ЕОМ. Документування результатів випробувань.
8. ГОСТ Р ИСО/МЭК 15408-1-02 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. - Госстандарт России. - Москва – 2002.
9. Сайт фірми Microsoft/ Новини/ Архів [Електронний ресурс]. – Режим доступу: http://www.microsoft.com/Ukraine/News/Issues/2005/08/OS.mspx
10. ДССЗЗИ/ Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України [Електронний ресурс]. – Режим доступу : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=78319&cat_id=39181.