УДК 004.7

О.А. МЯСІЩЕВ, О.О. МАРТИНЮК, Н.М. ГІНЕВСЬКА
Хмельницький національний університет

МЕТОД ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ НА ЕТАПАХ ПРОЕКТУВАННЯ І ЕКСПЛУАТАЦІЇ

У статті розглядається метод захищеності комп'ютерних мереж на основі побудови дерева атак на етапах проектування і експлуатації. Детально описано постановку завдання дослідження та методику аналізу захищеності комп'ютерних мереж.

Ключові слова: система аналізу захисту, СУБД, ПЗ, комп'ютерна мережа, ОС, безпека.

O.A. MYASISCHEV, O.O. MARTYNYUK, N.M. GINEVSKA
Khmelnitsky national university, Ukraine

METHOD OF COMPUTER NETWORKS SECURITY DURING THE DESIGN AND OPERATION

In the article the method of protection of computer networks from attacks wood building during the design and operation. Described in detail the supply of research objectives and methods of security analysis of computer networks. The proposed method for analyzing the security of computer networks during the design and operation can detect vulnerabilities used software and hardware, violation of security policy "bottlenecks" in the security of a computer network to assist in planning and implementing information security during the design and operation computer networks. Also allows selecting used to justify (or planned for use) of information security and assess the effectiveness of various information security, to compare different versions of their use. The results of evaluation of the effectiveness of methods of security analysis of computer networks during the design and operation showed meet the requirements that were presented.

Keywords: protection system analysis, database, software, computer network, operating system security.

Вступ. На змістовному рівні наукове завдання даного дослідження можна сформулювати таким чином: розробити методику аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації, що базується на побудові дерева атак і розрахунку безлічі показників, що характеризують рівень захищеності комп'ютерної мережі в цілому і окремих її компонентів. Реалізація цієї методики системами аналізу захищеності повинна дозволяти не лише оцінювати рівень захищеності мережі, але і досягати його необхідного значення шляхом зміни конфігурації аналізованої мережі і політики безпеки, що реалізовується в ній [1].

Для реалізації аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації необхідно розробити моделі комп'ютерних атак і порушника, аналізованої комп'ютерної мережі, побудови дерева атак і оцінки рівня захищеності [3].

Постановка завдання дослідження. В ході постановки завдання дослідження скористаємося представленням системи аналізу захищеності (рис. 1).

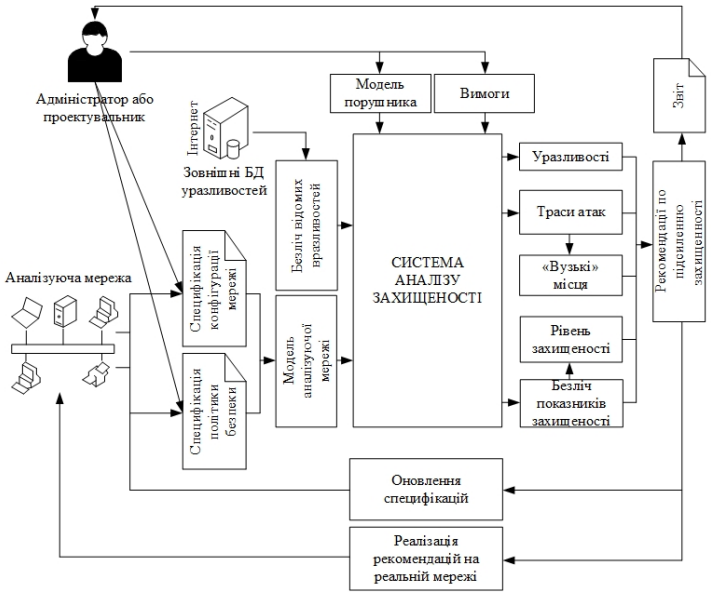

Рис. 1. Представлення системи аналізу захищеності

Система аналізу захисту (САЗ) повинна реалізовувати аналіз захищеності комп'ютерних мереж на етапі проектування і експлуатації. Для задоволення цієї вимоги передбачається використати підхід, при якому аналізується модель комп'ютерної мережі. Ця модель будується на базі специфікацій, що описують конфігурацію мережі (топологію, склад програмного забезпечення і апаратного забезпечення) і політику безпеки, що реалізовується в ній. Специфікації описуються на спеціалізованих мовах, ґрунтованих на XML.

На етапі проектування комп'ютерної мережі специфікації формуються проектувальником, на етапі експлуатації — в автоматичному режимі за допомогою програмних агентів, що функціонують на хостах [2].

Під час роботи САЗ повинна формувати сценарії (траси) комп'ютерних атак, враховувати модель порушника(первинне положення, рівень знань і умінь, первинні знання про аналізовану мережу), робити розрахунок безлічі показників, що характеризують захищеність комп'ютерної мережі в цілому і її окремих компонентів, враховувати топологію аналізованої мережі, склад програмного і апаратного забезпечення, політику безпеки, що реалізовується. Результатами роботи САЗ являються безліч виявлених вразливостей, траси атак, «вузькі» місця в захищеності комп'ютерної мережі (найбільш критичні компоненти комп'ютерної мережі, вірогідність атаки яких найвища), безліч показників захищеності, рекомендації по підвищенню рівня захищеності аналізованої мережі. Отримані результати гарантують вироблення обґрунтованих рекомендацій по усуненню виявлених «вузьких» місць і посиленню захищеності комп'ютерної мережі в цілому.

На змістовному рівні наукове завдання даного дослідження можна сформулювати таким чином: розробити методику аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації, що базується на побудові дерева атак і розрахунку безлічі показників, що характеризують рівень захищеності комп'ютерної мережі в цілому і окремих її компонентів [3]. Реалізація цієї методики системами аналізу захищеності повинна дозволяти не лише оцінювати рівень захищеності мережі, але і досягати його необхідного значення шляхом зміни конфігурації аналізованої мережі і політики безпеки, що реалізовується в ній.

Для реалізації аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації необхідно розробити моделі комп'ютерних атак і порушника, аналізованої комп'ютерної мережі, побудови дерева атак і оцінки рівня захищеності [4].

Методика аналізу захищеності комп'ютерних мереж. Пропонована методика аналізу захищеності ґрунтується на обліку програмно-технічної складової аналізу захищеності і не використовує активні засоби тестування (передбачається використання імітації дій порушника, спрямованих на модель аналізованої мережі). Основними етапами пропонованої методики аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації є:

1. Підготовчий етап. Цей етап реалізується проектувальником мережі або її системним адміністратором вручну або за допомогою різних автоматизованих засобів. Результатами цього етапу є дані, що обробляються за запропонованою методикою аналізу захищеності. Підготовчий етап складається з наступних основних кроків:

a) визначення ресурсів аналізованої мережі (хостів, ОС, СУБД, додатків і тому подібне), їх рівнів критичності і конфіденційності;

b) визначення використовуваних(чи планованих до використання) засобів забезпечення інформаційної безпеки (міжмережеві екрани, персональні засоби фільтрації мережевого трафіку, антивірусне програмне забезпечення і тому подібне);

c) створення на основі даних, отриманих на перших двох кроках, специфікації комп'ютерної мережі, вираженої на спеціалізованій мові System Description Language (SDL);

d) визначення політики безпеки і її представлення на спеціалізованій мові Security Policy Language (SPL).

2. Етап ініціалізації. Цей етап реалізується проектувальником комп'ютерної мережі або її системним адміністратором. Етап ініціалізації складається з наступних основних кроків:

a) вибір специфікації аналізованої мережі і специфікації політики безпеки (зовнішнє представлення моделі комп'ютерній мережі);

b) формування на основі заданих специфікацій комп'ютерної мережі і політики безпеки внутрішнього представлення моделі аналізованій мережі, що реалізовується;

c) формування завдання на оцінку захищеності;

d) формування вимог на захищеність.

3. Етап побудови дерева атак і його аналізу. Цей етап виконується автоматично програмними засобами аналізу захищеності.

4. Етап аналізу отриманих результатів і виконання рекомендацій, спрямованих на підвищення рівня захищеності комп'ютерної мережі. Результати аналізу захищеності відображаються проектувальникові або системному адміністраторові мережі. Якщо результати не задовольняють проектувальника (адміністратора), він може внести зміни в специфікації мережі і політики безпеки, керуючись сформованими системою аналізу захищеності рекомендаціями, і зробити повторний аналіз.

Методика аналізу захищеності комп'ютерних мереж для етапів проектування і експлуатації має відмінність у формуванні специфікацій аналізованої мережі і політики безпеки, що реалізовується в ній: на етапі проектування цей процес здійснюється проектувальником вручну, на етапі експлуатації специфікації можуть бути створені в автоматичному режимі з використанням різних засобів збору інформації про мережу (наприклад, за допомогою хостових програмних агентів) [5].

Усі операції, що проводяться у рамках методики, розділені на дві групи (рис. 2): (1) дії проектувальника (системного адміністратора) і (2) автоматичні процедури, що виконуються системою аналізу захищеності.

Множина дій проектувальника (адміністратора) складається з наступних елементів:

1) вибір файлу із специфікацією комп'ютерної мережі;
2) вибір файлу із специфікацією безпеки, що реалізовується в мережі політики;
3) завдання первинного положення порушника;
4) завдання первинних знань порушника про мережу;
5) завдання множини аналізованих об'єктів;
6) формування завдання на оцінку рівня захищеності;
7) формування вимог на захищеність мережі;
8) аналіз результатів;
9) ручна модифікація (коригування) специфікацій комп'ютерної мережі і політики безпеки, що реалізовується в ній, згідно з представленими системою аналізу захищеності рекомендаціям по збільшенню загального рівня захищеності мережі у разі отримання незадовільного результату;
10) збереження (запис у файли) остаточних специфікацій мережі і політики безпеки у разі отримання задовільного результату.

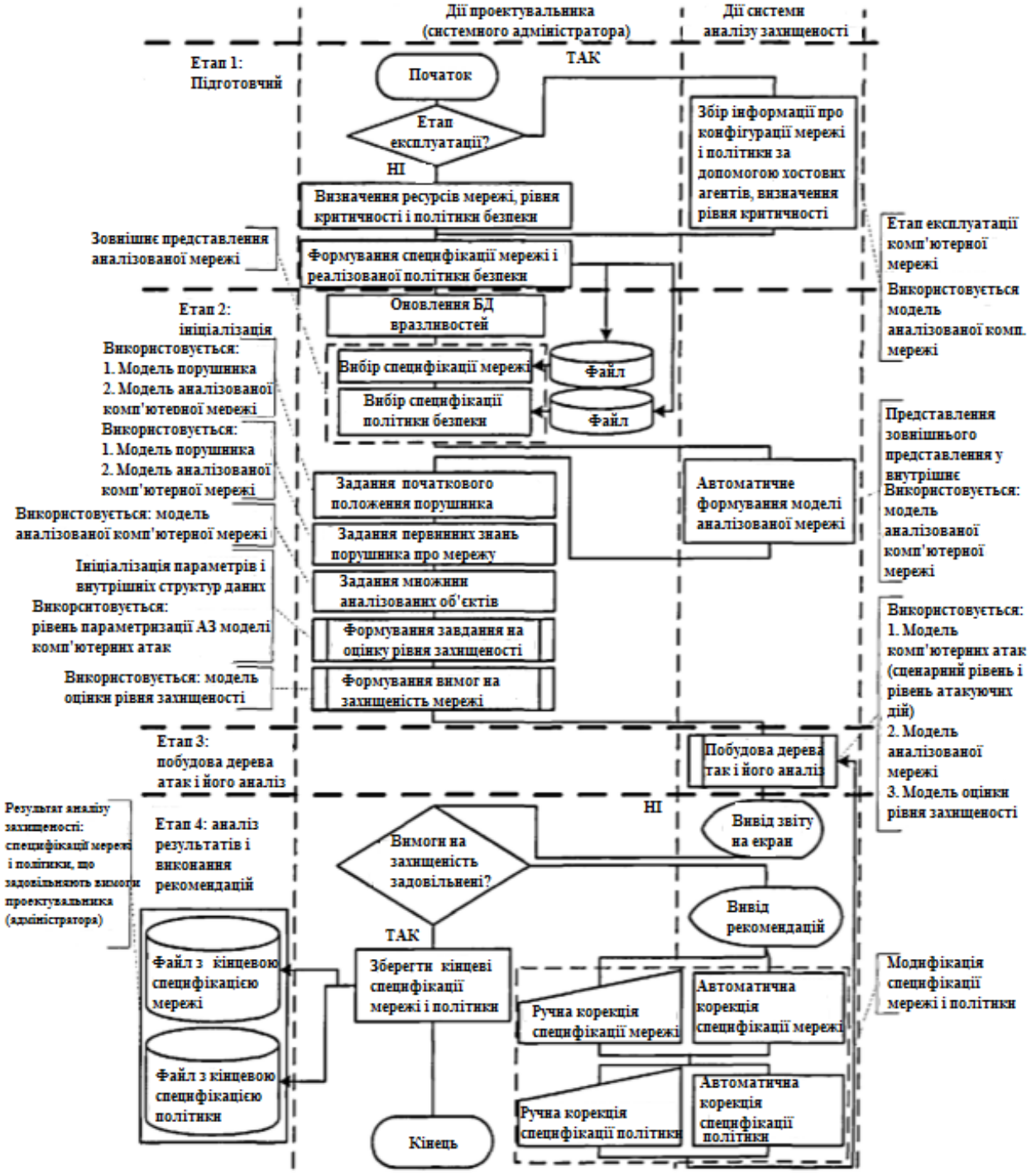

Рис. 2. Методика аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації

Множина процедур, що виконуються системою аналізу захищеності, складається з наступних елементів: (1) автоматичне формування моделі аналізованої комп'ютерної мережі (формування на базі заданих специфікацій конфігурації мережі і політики безпеки внутрішньої моделі мережі); (2) побудова дерева атак і його аналіз; (3) виведення звіту аналізу захищеності на екран; (4) автоматична модифікація (коригування) специфікацій мережі і політики безпеки на основі сформованих рекомендацій у разі отримання незадовільного результату [5].

Висновки. Пропонована методика аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації дозволяє виявити уразливості використовуваного програмного і апаратного забезпечення, порушення політики безпеки, «вузькі місця» в захищеності комп'ютерної мережі, надати допомогу в плануванні і здійсненні інформаційного захисту на етапах проектування і експлуатації комп'ютерних мереж. Також дозволяє обґрунтувати вибирання використовуваних (чи планованих до використання) засобів захисту інформації і оцінити ефективність різних засобів захисту інформації, порівняти різні варіанти їх використання.

Література

1. Введение в компьютерные сети [Электронный ресурс] / Электрон. текстовые дан. и граф. дан. — [Б. м.: б. и.]. — Режим доступа : http://www.kgtu.runnet.ru/E-Library/C_Networks/intro.htm. – (по состоянию на 01.01.2006).

2. Кононов А. Страхование нового века. Как повысить безопасность информационной инфраструктуры / А. Кононов // Connect. — М., 2001. — № 12.

3. Котенко И. В. Интеллектуальная система анализа защищенности компьютерных сетей на различных этапах жизненного цикла / И. В. Котенко, М. В. Степашкин // Труды Международных научно-технических конференций «Интеллектуальные системы (AIS—05)» и «Интеллектуальные САПР (CAD-2005)». — М. : Физматлит, 2005. — Т. 1. — С. 231–237.

4. Механизм работы алгоритма анализа рисков [Электронный ресурс] / Электрон. текстовые дан. и граф. дан. — [Б. м. : б. и.]. — Режим доступа : http://www.usk.ru/articles/905.html. – (по состоянию на 01.01.2006).

5. СУБД MySQL [Электронный ресурс] / Электрон. текстовые дан. и граф. дан. — [Б. м.: б. и.]. — Режим доступа : http://mysql.org. – (по состоянию на 01.03.2007).

Рецензія/Peer review : 27.1.2017 р. Надрукована/Printed :7.2.2017 р.
Статтю представляє: д.т.н., проф. Мясіщев О.А.