УДК 621

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

АНАЛІЗ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ ПОБУДОВИ ДЕРЕВА АТАК

У статті розглядається аналіз захищеності комп'ютерних мереж на етапах проектування і експлуатації (а також програмні засоби для його автоматизації). Описані основні етапи базового аналізу захищеності, методи аналізу ризиків, які дозволяють провести оцінку на базовому рівні. Також описана топологія комп'ютерної мережі у вигляді гіперграфа та представлений зв'язок між хостами у вигляді матриць.

Ключові слова: комп'ютерна мережа, гіперграф, засоби обчислювальної техніки, аутентифікація, автоматизована система, хост.

O.A. MYASISCHEV, O.O. MARTYNYUK, N.M. GINEVSKA
Khmelnytsky National University

ANALYZING SECURITY NETWORKS BASED ON WOOD CONSTRUCTION ATTACKS

In the article the analysis of computer network security during the design and operation (and its software for automation). The basic steps basic security analysis, risk analysis methods that allow you to assess at a basic level. Also described computer network topology in a hypergraph and presented communication between hosts in a matrix.

Keywords: computer network, hypergraph, computer aids, authentication, automated system, host.

Вступ. Завдання аналізу захищеності комп'ютерних мереж на різних етапах їх життєвого циклу, основними з яких є етапи проектування і експлуатації, все частіше стає об'єктом обговорення на спеціалізованих конференціях, присвячених забезпеченню інформаційної безпеки. Така пильна увага до даної задачі пояснюється тим, що аналіз захищеності необхідний при контролі та моніторингу захищеності комп'ютерних мереж, при атестації автоматизованих систем (комп'ютерних мереж) та сертифікації засобів обчислювальної техніки за вимогами діючих нормативних документів і вимагає обробки великого обсягу даних в умовах дефіциту часу.

Захищеність комп'ютерної мережі визначається як ступінь адекватності реалізованих в ній механізмів захисту інформації (такі, як ідентифікація і аутентифікація, управління доступом, протоколювання і аудит, криптографія, екранування) існуючим в даному середовищі функціонування ризиків, пов'язаних із здійсненням погроз безпеки інформації, тобто здатність механізмів захисту забезпечити конфіденційність, цілісність і доступність інформації. Захищеність може надавати і часто надає вирішальний вплив на показники ефективності функціонування комп'ютерних мереж. Під загрозою розуміється сукупність умов і факторів, що визначають потенційну або реально існуючу небезпеку виникнення інциденту, який може привести до нанесення збитку функціонуванню комп'ютерної мережі. Загрози можуть класифікуватися за різними ознаками. Зокрема, за характером походження загрози поділяються на дві групи: навмисні і природні. Основними умисними погрозами вважаються: підключення порушника до каналів зв'язку; несанкціонований доступ; розкрадання носіїв інформації. До основних природних загроз відносяться: нещасні випадки (пожежі, аварії, вибухи); стихійні лиха (урагани, повені, землетруси); помилки в процесі обробки інформації (збої апаратури). При аналізі захищеності комп'ютерних мереж до уваги слід приймати всі різновиди загроз, проте найбільшу увагу має бути приділено тим з них, які пов'язані з діями людини, зловмисними або іншими. Тому природні загрози в даній роботі не розглядаються.

В загальному випадку, під атакою розуміється «несанкціонована спроба використання вразливого місця». Проте, як правило, атака складається з множини дій порушника, що виконуються в певній послідовності. Таким чином, необхідно розрізняти атомарні дії порушника (запуск на виконання програмного додатка для отримання інформації про атакуючий об'єкт, для використання вразливості і т.д.), які будемо називати атакуючою дією, і множина атакуючих дій, що використовуються в певній послідовності і дозволяє порушнику досягти деякої загальної цілі (як правило, це ціль, що досягається останньою атакуючою дією, наприклад, порушення доступності конкретного мережевого сервісу), яке будемо називати атакою. Множина атакуючих дій порушника, що складають атаку, і порядок їх виконання складають сценарій атаки. Формальним представленням можливих атакуючих дій порушника, що дозволяє наглядно продемонструвати сценарій атак, можуть виступати граф або дерево атак.

Зауважимо, що більшість використовуваних в організація комп'ютерних мереж через відсутність повної інформації про програмне і апаратне забезпечення не можуть пройти атестацію (а також періодично піддаються контролю і моніторингу захищеності) на основі базового аналізу захищеності. Саме тому Ю.С. Васильєв і П.Д. Зегжда виділили вдосконалення і автоматизацію методів і засобів (детального) аналізу захищеності програмно-апаратних комплексів з урахуванням відсутності повної інформації про них, у тому числі й аналіз програм у відсутності початкових текстів, в якості особливого напрямку забезпечення інформаційної безпеки.

Основні етапи базового аналізу захищеності. Розглянемо основні визначення і нормативні

документи, використовувані в завданні аналізу захищеності комп'ютерних мереж і дозволяючі визначити місце і роль АЗ КМ. Під комп'ютерною мережею (КМ) (чи розподіленою автоматизованою системою) розуміється сполучені каналами зв'язки системи обробки даних, орієнтовані на конкретного користувача. Автоматизована система (АС) визначається як система, що складається з персоналу і комплексу засобів автоматизації його діяльності (засобів обчислювальної техніки – ЗОТ), що реалізовує інформаційну технологію виконання встановлених функцій. У свою чергу засоби обчислювальної техніки визначаються як програмно-технічні засоби, що розробляються і поставляються на ринок як елементи, з яких будуються автоматизовані системи. Відповідно до чинних в нашій країні нормативних документів, при розгляді питань захисту ЗОТ від несанкціонованого доступу (НСД) обмежуються тільки програмно-технічними аспектами функціонування системи, тоді як захист АС припускає розгляд організаційних заходів захисту, питань фізичного доступу і т.д. Таким чином основними етапами базового аналізу захищеності є (рис. 1):

1. Оцінка адекватності вимог безпеки. На цьому етапі проводиться: (а) визначення і документування вимог безпеки; (б) критичний аналіз вимог безпеки з метою визначення їх придатності для цілей аналізу захищеності.

2. Оцінка адекватності механізмів захисту. На цьому етапі використовуються чек-листи, що містять, наприклад, наступне питання : чи "Виконується реєстрація спроб доступу до мережевого принтера"? Питання можуть бути різної міри деталізації залежно від вимог безпеки, які можуть визначати в одному випадку лише наявність конкретного механізму захисту (наприклад, аутентифікація видалених користувачів), в іншому – регламентувати реалізацію цього механізму (наприклад, використання певної схеми аутентифікації).

3. Перевірка існування механізмів захисту. На цьому етапі проводиться перевірка наявності представлених у функціональних специфікаціях АС механізмів захисту. При цьому не проводиться аналіз якості функцій, що реалізовуються ними. Тестування проводиться по методу "чорного ящика" (таке тестування припускає відсутність у тестуючої сторони яких-небудь спеціальних знань про конфігурацію і внутрішню структуру АС) для механізмів захисту, реалізованих програмними і технічними засобами (наприклад, чи проводиться аутентифікація користувача перед будь-якими його діями в АС), і простим візуальним оглядом для адміністративних заходів захисту (наприклад, чи здійснюється контроль фізичного доступу до АС).

4. Огляд методології проектування. Цей етап дозволяє судити про міру надійності реалізації механізмів захисту.

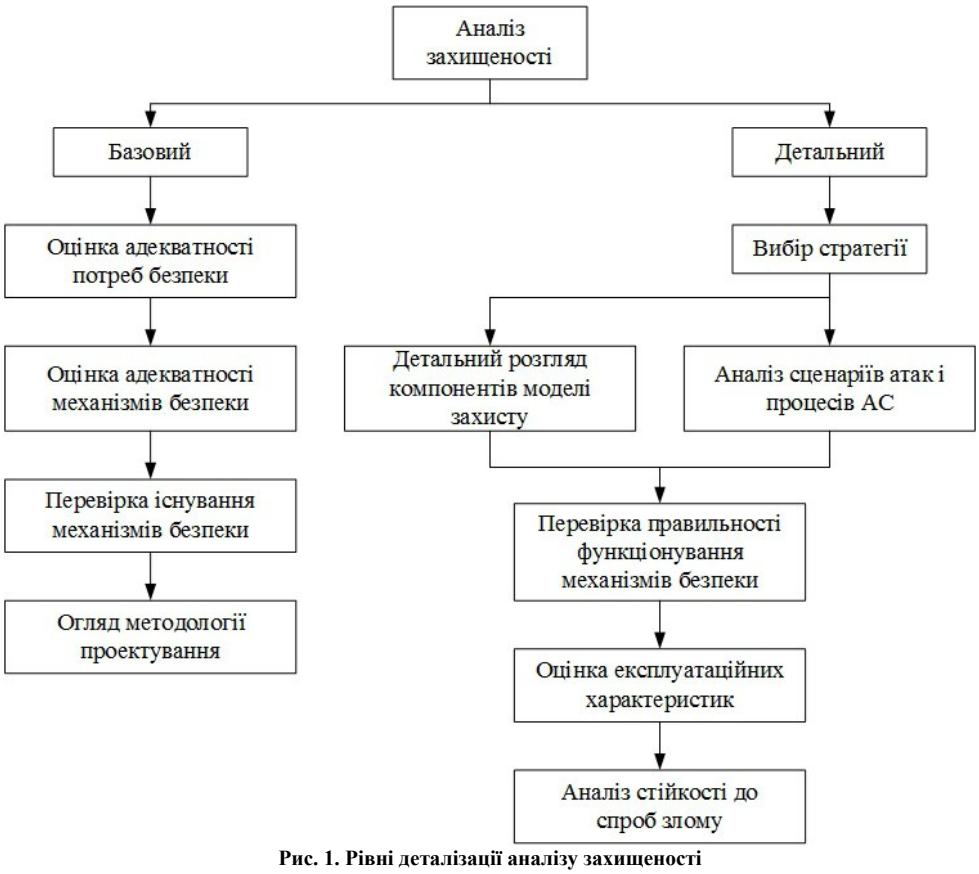

Рис. 1. Рівні деталізації аналізу захищеності

Для проведення базового аналізу необхідно надати експертам проектну документацію і початкові тексти програмного забезпечення, що не завжди можливо. В умовах, коли інформації про тих, що реалізовуються в АС функціях недостатньо для базового аналізу (наприклад, відсутній доступ до

початкових кодів програм), експерти вимушені проводити детальний аналіз захищеності.

Метод аналізу ризиків. Для аналізу захищеності комп'ютерних мереж на етапі проектування використовуються методи аналізу ризиків, які дозволяють провести оцінку на базовому рівні. Виділяють два підходи: (1) аналіз ризиків по двох чинниках і (2) аналіз ризиків по трьох чинниках.

У першому підході використовуються наступні чинники: коефіцієнт, що характеризує частоту появи події($P_{\text{подія}}$) і тяжкість можливих наслідків($Ціна_{\text{втрати}}$). Вважається, що ризик тим більше, чим більше $P_{\text{подія}}$ і $Ціна_{\text{втрати}}$. Загальна ідея може бути виражена наступною формулою: Ризик = $P_{\text{подія}} \cdot Ціна_{\text{втрати}}$. Якщо $P_{\text{подія}}$ і $Ціна_{\text{втрати}}$ є кількісними величинами, тоді ризик — оцінка математичного очікування втрат; якщо якісними величинами, тоді операція множення не визначена і ризик визначається за допомогою матриці («матриці ризиків»). У цій матриці (рис. 2) по стовпцях розташовані значення коефіцієнта, що характеризує частоту появи події(наприклад, з використанням наступної шкали:(А) подія практично ніколи не відбувається; (Б) подія трапляється рідко; (В) вірогідність події за даний проміжок часу близько 0,5; (Г) швидше за все, подія станеться; (Д) подія майже обов'язково станеться). По рядках розташовується серйозність події (наприклад, наступні значення: (а) Negligible — подією можна нехтувати; (б) Minor — незначна подія; (в) Moderate — подія з помірними результатами (дії незначна і не зачіпає критично важливі завдання); (г) Serious — подію з серйозними наслідками (дія зачіпає критично важливі завдання); (д) Critical — подія призводить до неможливості рішення критично важливих завдань. Для оцінки ризиків визначається змінна з трьох значень: низький ризик, середній ризик і високий ризик. Шкали чинників ризику ($P_{\text{подія}}$ і $Ціна_{\text{втрати}}$) і сама таблиця можуть бути визначені інакше, мати інше число градацій. При використанні цього підходу необхідно враховувати наступні особливості: (1) значення шкал мають бути чітко визначені і розумітися однаково усіма учасниками процедури оцінки; (2) потрібно обґрунтування вибраній таблиці, тобто необхідно переконатися, що різні інциденти, що характеризуються однаковими поєднаннями чинників ризику, мають з точки зору експертів однаковий рівень ризику.

	Negligible	Minor	Moderate	Serious	Critical
А	Низький	Низький	Низький	Середній	Середній
Б	Низький	Низький	Середній	Середній	Високий
В	Низький	Середній	Середній	Середній	Високий
Г	Середній	Середній	Середній	Середній	Високий
Д	Середній	Високий	Високий	Високий	Високий

Рис. 2. Приклад матриці для визначення ризику залежно від двох чинників

У підході аналізу ризиків по трьох чинниках використовуються чинники «загроза», «вразливість» і «ціна втрати». Коефіцієнт, що характеризує частоту появи події, в цьому підході визначається таким чином:

$P_{\text{подія}} = P_{\text{загрози}} \cdot P_{\text{вразливості}}$. Тоді Ризик = $P_{\text{загрози}} \cdot P_{\text{вразливості}} \cdot Ціна_{\text{втрати}}$. Якщо $P_{\text{загрози}}$, $P_{\text{вразливості}}$ і $Ціна_{\text{втрати}}$ є кількісними величинами, тоді останній вираз використовується як математична формула, інакше — як формулювання загальної ідеї (в даному випадку ризик визначається з використанням матриць ризику, наприклад, рис. 3). У матриці, представленій на рис. 3, рівні уразливості Н, З, В означають відповідно: низький, середній високий рівень, а показник ризику вимірюється в шкалі від 0 до 8 з наступними визначеннями рівнів ризику: 1 — ризик практично відсутній(теоретично можливі ситуації, при яких подія настає, але на практиці це трапляється рідко, а потенційний збиток порівняно невеликий); 2 — ризик дуже малий(події подібного роду траплялися досить рідко, крім того, негативні наслідки порівняно невеликі); 8 — ризик дуже великий(подія швидше за все настане, і наслідки будуть надзвичайно важкими).

Міра серйозності події (ціна втрати)	Рівень загрози								
	Низький			Середній			Високий		
	Рівні уразливості								
	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

Рис. 3. Приклад матриці для визначення ризику залежно від трьох чинників

Топологія комп'ютерної мережі. Для представлення топології представлений гіперграф, в якому як вершини використовуються мережеві інтерфейси хостів, а ребра представляють підмножину безлічі інтерфейсів (у стандартному графові ребра сполучають пари вершин, в гіперграфі — підмножина вершин). У цій моделі виділяється два види ребер: (1) ребра, що описують хости (дозволяють представити хости з декількома мережевими інтерфейсами, наприклад, ребро $H4 = \{i_4, i_5\}$на рис. 4) і (2) ребра, що описують зв'язки хостів між собою (наприклад, ребро $L1 = \{i_1, i_2, i_3, i_4\}$).

На рис. 4 зображений гіперграф, що представляє приклад невеликої мережі. Множина $\{i_1, i_2, \ldots, i_7\}$

– вершини графа(мережеві інтерфейси хостів); множина {*H*1, *H*2, . . . , *H*7} – ребра графа, які описують хости; {*L*1, *L*2} – ребра, що описують зв'язки хостів між собою.

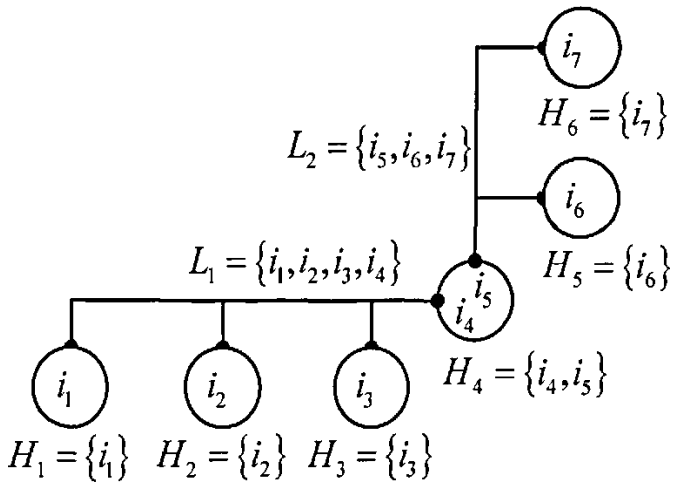

Рис. 4. Представлення топології комп'ютерній мережі у вигляді гіперграфа

Зв'язок між хостами. Наочно зв'язок між хостами можна представити у вигляді матриць, приклад яких наведений на рис. 5. Безліч програмних продуктів утворюють конфігурацію хоста.

Недоліком цієї моделі є неможливість її використання при аналізі захищеності, оскільки (1) модель не відбиває достатньою мірою об'єкт (аналізовану комп'ютерну мережу), наприклад, відсутня можливість опису налаштувань стека протоколів TCP/IP для хостів, що призводить до неможливості обліку в аналізі захищеності політики фільтрації мережевого трафіку і так далі) і (2) модель необхідно доповнити компонентом, що формує відгук мережі (зміна її конфігурації) на ті, що реалізовуються порушником атакуючі дії.

	i_1	i_2	i_3	i_4	i_5	i_6	i_7
L_1	1	1	1	1	0	0	0
L_2	0	0	0	0	1	1	1

	i_1	i_2	i_3	i_4	i_5	i_6	i_7
H_1	1	0	0	0	0	0	0
H_2	0	1	0	0	0	0	0
H_3	0	0	1	0	0	0	0
H_4	0	0	0	1	1	0	0
H_5	0	0	0	0	0	1	0
H_6	0	0	0	0	0	0	1

Рис. 5. Представлення зв'язків між хостами у вигляді матриць

Висновки. Основною метою є підвищення ефективності аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації на основі розробки і використання моделей комп'ютерних атак, порушника, аналізованої комп'ютерної мережі, формування дерева атак, оцінки рівня захищеності і методики аналізу захищеності комп'ютерних мереж.

Література

1. Астахов А. Анализ защищенности корпоративных автоматизированных систем [Електронний ресурс] / А. Астахов // Электрон, текстовые дан. и граф. дан. – [Б. м.: б. и.]. – Режим доступу : http://www.jetinfo.ru/2002/7/1/article1.7.2002.html

2. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – М. : ТИД «ДС», 2002. – 688 с.

3. Паркер Т. TCP/IP. Для профессионалов / Т. Паркер, К. Сиян. – СПб : Питер, 2003.

4. Методы выявления нарушений безопасности [Електронний ресурс] // Электрон, текстовые дан. и граф. дан. – [Б. м. : б. и.]. – Режим доступу : http:/www.ssl.stu.neva.ru/sam/IDS%20Methods.htm.

5. Защита от несанкционированного доступа к информации. Термины и определения [Електронний ресурс] // Электрон, текстовые дан. и граф. дан. – [Б. м. : б. и.]. – Режим доступу : http://www.sbcinfo.ru/articles/doc/gtc_doc/r_nsd_term.htm.

6. Котенко И. В. Оценка уровня защищенности компьютерных сетей на основе построения графа атак / И. В. Котенко, М. В. Степашкин, В. С. Богданов // Труды международной научной школы «Моделирование и анализ безопасности и риска в сложных системах (МАБР-2006)». – СПб, 2006. – С. 150–154.

Рецензія/Peer review : 18.9.2016 р. Надрукована/Printed : 30.10.2016 р.
Рецензент: д.т.н., проф.. Сорокатий Р.В.