УДК 004.942:621.317

І. Я. Тишик, Ю. К. Груздєва
Національний університет “Львівська політехніка”,
кафедра захисту інформації

МОДЕЛЮВАННЯ РЕАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА РІЗНИХ РІВНЯХ СТЕКУ TCP/IP

Наведено основні класичні моделі безпеки інформаційних систем та подано їхню характеристику. Здійснено статистичний аналіз спроб реалізації загроз інформації в інформаційних системах з відкритою архітектурою. Проведено моделювання ймовірності реалізації загроз інформації на різних рівнях стеку протоколів TCP/IP; проаналізовано результати моделювання.

Ключові слова: моделі безпеки, інформаційні системи, система з відкритою архітектурою, математична модель стек-протоколів TCP/IP

The article gives the basic classical models of information systems security and their description. Statistical analysis of information threats attempts in information systems with open architecture is performed. The simulation of probability of information threats at different levels of the protocol stack TCP/IP is conducted, the simulation results are analyzed

Key words: security model, information systems, system with open architecture, mathematical model protocol stack TCP/IP.

Вступ

Одним із головних напрямків розвитку інформаційних технологій, що визначає ефективність сучасних інформаційних систем (ІС), є розробка та впровадження технології систем з відкритою архітектурою. Суть цієї технології полягає у забезпеченні можливості застосування тих самих прикладних систем для різних програмно-апаратних платформ та організації взаємодії між ними завдяки відкритим специфікаціям [4]. Використання під час розробки ІС відкритих специфікацій дає змогу третім сторонам розробляти для цих систем різні апаратні/програмні засоби розширення і модифікації, а також створювати програмно-апаратні комплекси з продуктів різних виробників. Проте позитивні якості ІС з відкритою архітектурою є певним джерелом додаткових уразливостей, що істотно знижує рівень захищеності функціонуючої у таких системах інформації. Сьогодні проблема захисту інформації в ІС з відкритою архітектурою є актуальним завданням, яке потребує подальших ґрунтовних досліджень. Відомі математичні моделі захищених ІС недостатньою мірою враховують особливості, пов’язані з їх відкритою архітектурою, а також їхнє функціонування в умовах ризику за невідомих ймовірностей реалізації загроз інформації. Враховуючи це, виникає необхідність у розробленні нових методик моделювання атак та механізмів захисту в ІС з відкритою архітектурою.

Аналіз досліджень та публікацій

Для забезпечення безпеки ІС сьогодні широко застосовуються фундаментальні моделі безпеки, такі як Take-Grant, HRU, Bell-lapadula, LWM [1–3].

Модель Take-Grant використовується для аналізу систем дискреційного розмежування прав доступу, насамперед для аналізу шляхів поширення прав доступу у таких системах. Метою застосування моделі є одержання відповіді на питання про можливість отримання прав доступу суб’єктом системи на об’єкт стану, який описується графом доступів. Отже, стан системи описується його графом доступів. Перехід системи із стану в стан визначається операціями або правилами перетворення графа доступу. Take-Grant ґрунтується на істотному спрощенні реальної

операційної системи з абстрагуванням усього, крім взаємозв'язків між різними процесами і/або користувачами у системі, і моделюванням динамічних змін параметрів доступу, які здійснюються за допомогою набору правил перетворення напрямленого графа, який відображає ці взаємозв'язки.

У розширеній моделі Take-Grant розглядаються шляхи і вартості виникнення інформаційних потоків у системах з дискреційним розмежуванням доступу. Тут додатково розглядаються права доступу: на читання даних та їх запис, а також додаткові права перетворення графів доступу. Ці правила використовуються для пошуку шляхів виникнення можливих інформаційних потоків у системі, які є наслідком уже існуючих прав доступу для об'єктів системи і можуть стати причиною виникнення інформаційного потоку між об'єктами без їх безпосередньої взаємодії.

Універсальна модель для моделювання усіх типів механізму захисту HRU (Harrison, Ruzzo, Ullman) використовується переважно для аналізу системи захисту, яка реалізує дискреційну політику безпеки і її головного елемента – матриці доступу. Функціонування системи розглядається лише з погляду змін у матриці доступу. При цьому систему подано скінченним автоматом, який функціонує згідно з певними правилами переходу.

Згідно з вимогами більшості критеріїв оцінки безпеки системи повинні будуватися на основі певних математичних моделей, які теоретично обґрунтовують відповідність системи до вимог заданої політики безпеки. Однак, як показують результати аналізу моделі HRU, завдання побудови алгоритму перевірки безпеки систем, які реалізують дискреційну політику розмежування прав доступу, не можуть бути виконані. З одного боку, загальна модель HRU може виражати велику різноманітність політик дискреційного розмежування доступу, але при цьому не існує алгоритму перевірки їх безпеки, з іншого, – можна використовувати монооперацийні системи, для яких існує згаданий алгоритм перевірки, але застосування систем цього класу доволі обмежене.

Класична модель системи безпеки Bell-lapadula призначена для аналізу систем захисту, які реалізують мандатне (повноважне) розмежування доступу. Ця модель визначає, якими властивостями повинні характеризуватися стани та дії безпечної системи, але не вказується, що повинна виконуватись система за запитами суб'єктів на доступ до об'єктів під час переходу із стану у стан, і як саме повинні змінюватися значення елементів моделі.

Модель Law-Water-Mark (LWM) є наближеною до моделі Bell-lapadula підходом до визначення властивостей системи безпеки мандатної політики. Модель LWM пропонує порядок безпечного функціонування системи у разі, коли за запитом суб'єкта йому завжди необхідно надати доступ на запис до об'єкта.

Усі розглянуті моделі безпеки можуть бути використані під час побудови і аналізу детермінованих систем захисту, тобто систем, що не включають елементів ймовірнісної природи. Досліджуючи системи, закономірності функціонування яких складні або фактично не піддаються опису, доцільно використовувати елементи теорії ймовірностей. До таких систем належать глобальні обчислювальні мережі, багатозадачні та багатокористувацькі операційні системи.

Постановка завдання

З метою визначення ефективності реалізації загроз інформації для інформаційних систем з відкритою архітектурою постає завдання проведення статистичного аналізу спроб реалізації загроз інформації у таких інформаційних системах, моделювання ймовірності реалізації загроз інформації в інформаційних системах на різних рівнях стека протоколів TCP/IP, аналіз отриманих значень ймовірності реалізації загроз інформації в інформаційних системах, побудованих на основі TCP/IP.

1. Визначення ефективності реалізації загроз для ІС з відкритою архітектурою

Відомо, що рішення про використання певних механізмів захисту приймається за результатами проведення аналізу загроз інформації, яка опрацьовується в розподілених ІС з відкритою архітектурою, оцінки ймовірності реалізації поданих загроз і величини можливої шкоди. Для характеристики захищеності інформації, яка опрацьовується в ІС, використовують ймовірність збереження захищеності як функцію множини потенційних загроз і множини реалізованих у

системі захисту інформації ІС механізмів захисту. У такому випадку для ІС з відкритою архітектурою та багаторівневим стеком протоколів вираз матиме такий вигляд [2]:

$$\mathrm{P}(E,M)=\prod_{i=1}^{L}\left(\prod_{j=1}^{N}\left(1-E_{ij}\right)+\sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}\left(1-E_{jk}\right)\cdot\left(\sum_{k=1}^{j}M_{jk}\cdot\prod_{l=k+1}^{j}\left(1-M_{ij}\right)\right)\right]\right), \quad (1)$$

де L – кількість потенційних загроз інформації, яка опрацьовується в ІС; N – кількість рівнів стека протоколів; M_{ij} – змінна, значення якої визначає факт наявності/відсутності механізму захисту від i-ї загрози на протоколі j-го рівня; E_{ij} – показник ефективності реалізації i-ї загрози на протоколі j-го рівня.

Показник ефективності реалізації загрози E_{ij} визначається як показник оцінки ризику, пов'язаний з реалізацією цієї загрози:

$$E_{ij}=\mathrm{Q}_{ij}R_{ij}, \quad (2)$$

де Q_{ij} – показник, що характеризує відносний внесок, який характеризується i-ю загрозою інформації, реалізованою на протоколі j-го рівня стека протоколів ІС; R_{ij} – показник, що характеризує статистичну ймовірність реалізації i-ї загрози інформації на протоколі j-го рівня ІС.

Визначення ефективності реалізації загроз інформації, яка опрацьовується в ІС з відкритою архітектурою, зводиться до визначення показників Q_{ij} та R_{ij}.

Оскільки показник R_{ij} повинен характеризувати статистичну ймовірність реалізації i-ї загрози інформації j-му рівню стека, для його оцінки необхідно скористатися статистичними даними про спроби реалізації тих чи інших загроз в ІС. Для проектованих ІС такі дані, відсутні, проте можуть бути замінені даними, отриманими для вже функціонуючих ІС з аналогічною архітектурою. Оскільки усі ІС з багаторівневою архітектурою стека протоколів, незалежно від конкретного використовуваного стека протоколів, функціонують за подібними принципами оцінювання, отримані для однієї ІС, з достатньо високою точністю справджуються і для інших ІС.

2. Оцінювання статистичної імовірності реалізації загроз інформації на рівнях стеку TCP/IP

Найбільш застосовною для виконання статистичного аналізу спроб реалізації різних загроз інформації є найбільша з існуючих розподілених ІС з відкритою архітектурою – Internet, який функціонує на основі стека протоколів TCP/IP, що полегшує аналіз наявності інформації про результати моніторингу інцидентів з безпекою, що публікується різноманітними організаціями (наприклад, CERT CIAC NIPC), а також результатів багатьох досліджень, що тією чи іншою мірою узагальнюють отримані дані.

Для оцінювання показника R_{ij} використані статистичні дані про зареєстровані NIPC факти реалізації загроз інформації у публічній мережі Internet, класифікованих за рівнем стека протоколів TCP/IP, на якому саме реалізувалася атака. При цьому як оцінка R_{ij} використане середнє за часом значення відносної частоти спроб реалізації загроз інформації на різних рівнях стека протоколів.

Згідно з правилами статистичного аналізу часових рядів достовірною можна вважати лише таку оцінку середнього значення, для якої: відсутня автокореляція залишків (відхилень обчислених значень відносних частот від середнього за часом); багато залишків є білим шумом з розподілом, близьким до нормального; сумарне відносне відхилення виміряних значень від середнього доволі мале [5].

Для перевірки наявності/відсутності автокореляції залишків використовується критерій Дарбіна-Уотсона [1]:

$$\mathrm{D}U=\frac{\sum_{k=2}^{N}\left(d_k-d_{k-1}\right)^2}{\sum_{k=1}^{N}d_k^2}, \quad (3)$$

де $d_k=\overline{Y}-Y_k$ – різниця середнього і фактичного значення (залишок) на інтервалі в N точок, для яких Y_k відоме.

Якщо значення *DU* близьке до 2, то автокореляція залишків відсутня, якщо близьке до 0 або до 4, – то присутня.

Для перевірки гіпотези про нормальний розподіл ряду використовується правило Романовського, згідно з яким гіпотеза про нормальний розподіл незалежних випадкових величин приймається у разі виконання нерівності:

$$\frac{c^2 - \mathrm{r}}{\sqrt{2r}} < 3, \tag{4}$$

де r – кількість ступенів свободи розподілу, що дорівнює різниці між кількістю класів розбиття усієї кількості спостережень і чіткістю накладених зв'язків (для нормального закону розподілу – дорівнює 3).

Значення χ^2-критерію обчислюється за формулою

$$c^2 = \sum_{\mathrm{i}=1}^{\mathrm{k}} \frac{\left(\mathrm{m_i} - nP_i^*\right)^2}{nP_i^*}, \tag{5}$$

де k – кількість точок розбиття усієї кількості спостережень на класи; m_i – кількість значень випадкової величини в i-му класі; n – кількість спостережень; P_i^* – теоретична ймовірність потрапляння випадкової величини в i-й клас відповідно до вибраного закону розподілу.

Сумарне відносне відхилення реальних значень від середнього оцінюється за формулою

$$\delta = \sum_{k=1}^{N} \left| \frac{\overline{Y} - Y_k}{\overline{Y}} \right| \cdot 100\ \%, \tag{6}$$

де $\overline{Y}$ – середнє значення відносних частот спроб реалізації загроз інформації; Y_k – k-те спостережне значення; N – кількість спостережень.

На рис. 1–4 показані графіки часових рядів, які відповідають зміні відносних частот (у відсотках) зареєстрованих значень у часі, графіки експериментального (розрах. P_i) і теоретичного нормального розподілу ймовірностей реалізації загроз (P_i теоретична), а в табл. 1 наведені результати аналізу за вказаними критеріями.

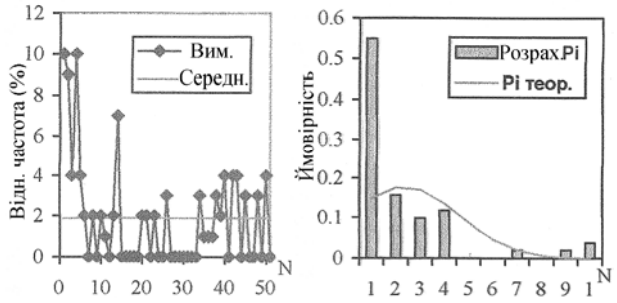

Рис. 1. Відносні частоти спроб реалізації загроз інформації на канальному рівні

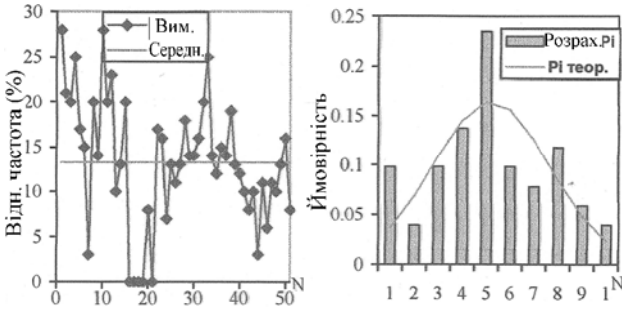

Рис. 2. Відносні частоти спроб реалізації загроз інформації на мережевому рівні

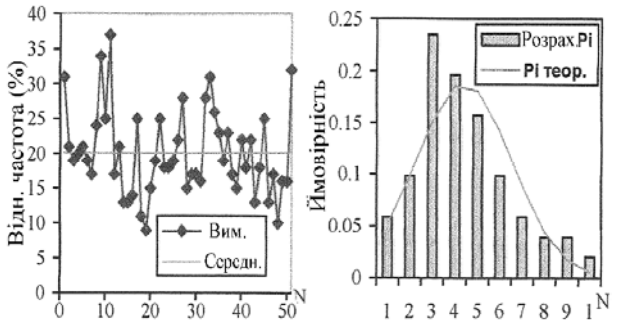

Рис. 3. Відносні частоти спроб реалізації загроз інформації на транспортному рівні

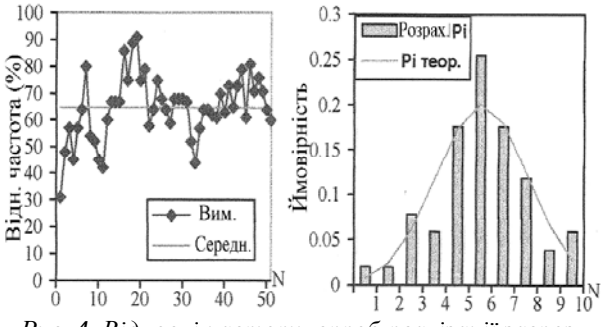

Рис. 4. Відносні частоти спроб реалізації загроз інформації на прикладному рівні

З наведених результатів очевидно, що отримана оцінка середнього значення загалом (для мережевого, транспортного та прикладного рівнів) відповідає критеріям достовірності. Невідповідність критеріям достовірності оцінки, отриманої на основі даних про спроби реалізації загроз на канальному рівні, пояснюється великою кількістю нульових значень відносних частот, що пов'язано з дуже рідкою реалізацією загроз інформації на цьому рівні стека.

Таблиця 1

Статистичні показники реалізації загроз ІС стеку TCP/IP

Показники	Рівні стеку TCP/IP			
	$j = 1$	$j = 2$	$j = 3$	$j = 4$
Середнє значення S_j	1,86	13,22	20,08	64,73
Математичне сподівання M_j	1,83	13,15	19,90	64,35
Дисперсія D_j	4,97	45,51	34,46	138,93
Середньоквадратичне відхилення σ_j	2,23	6,75	5,87	11,79
Значення критерію Дарбіна-Уотсона DU_j	1,12	1,02	1,38	0,77
Значення критерію Романовського	55,82	1,02	0,03	0,33
Сумарне відносне відхилення d_j	101,38	41,13	24,29	13,99

На рис. 5 показані точки, які відповідають експериментально отриманим значенням статистичної ймовірності реалізації загроз інформації на різних рівнях стека протоколів TCP/IP (P_j), а також графік апроксимації цих значень кривою третього порядку:

$$R_{ij}(j) = aj^3, \tag{7}$$

де нормувальний коефіцієнт $a = 1 \Big/ \sum_{k=1}^{N} k^3$; N – кількість рівнів стека протоколів (для TCP/IP $N = 4$); j – номер стека протоколів TCP/IP.

Для оцінки точності запропонованої апроксимації визначається відхилення $\Delta_j = |P_j - R_{ij}(j)|$ теоретичних значень R_{ij}, отриманих згідно з (7), від експериментальних, $P_j = M_j/100$, які порівнюються зі значеннями відповідних середньоквадратичних відхилень $s_{Pj} = s_j/100$ і довірчих інтервалів $3\sigma_{Pj}$ (табл. 2).

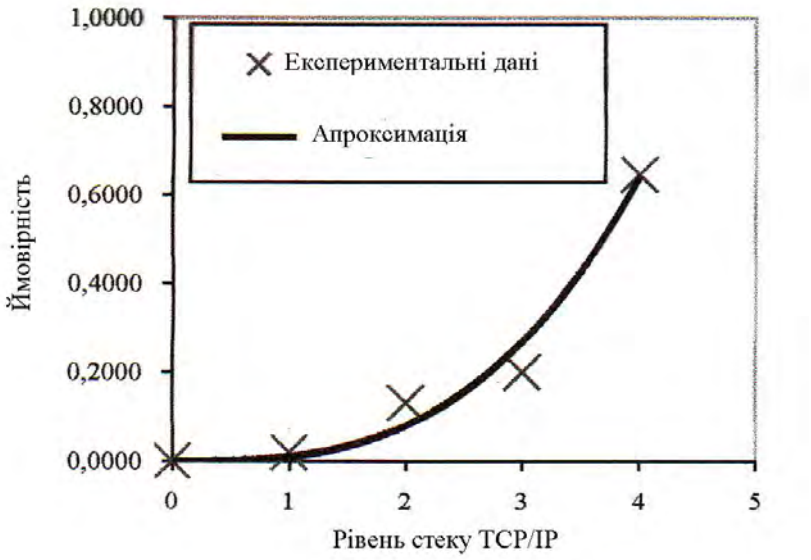

Рис. 5. Ймовірності реалізації загроз інформації на різних рівнях стека TCP/IP

Таблиця 2

Значення статистичних показників на рівнях TCP/IP

Показники	Рівні стека TCP/IP			
	$j = 1$	$j = 2$	$j = 3$	$j = 4$
P_j	0,0186	0,1322	0,2008	0,6473
$R_{ij}(j)$	0,01	0,08	0,27	0,64
Δ_j	0,0086	0,0522	0,0692	0,0073
σ_{Pj}	0,0223	0,0675	0,0587	0,1179

З цієї таблиці очевидно, що значення відхилень Δ_j не перевищуватимуть значень довірчих інтервалів $3s_{Pj}$ і відповідних значень середньоквадратичних відхилень – s_{Pj}. Це дає підстави говорити про достатню точність апроксимації і застосовність її для оцінки статистичної ймовірності реалізації загроз інформації на різних рівнях стека протоколів TCP/IP.

Висновок

В результаті проведеного моделювання одержані значення статистичної ймовірності реалізації загроз інформації в ІС щодо кожного рівня стека протоколів TCP/IP. Встановлено, що одержані значення статистичної ймовірність реалізації загроз інформації загалом збігаються з теоретичними значеннями, що дає підстави стверджувати про достатню точність апроксимації і застосовність її для оцінки статистичної ймовірності реалізації загроз інформації на різних рівнях стека протоколів TCP/IP. Крім того, оскільки ймовірність реалізації загроз інформації зростає з кожним наступним вищим рівнем стека, то є очевидною актуальність щодо подальшої розробки і впровадження протоколів забезпечення безпеки на вищих рівнях стека TCP/IP.

1. Гончар С. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом / С. Гончар // Захист інформації. - 2014. - Т. 16, № 1. – С. 40–46. 2. Боня Ю. Ю. Синтез систем защиты информации с минимальной стоимостью механизмов защиты / Ю. Ю. Боня, А. Н. Новиков // Пробл. упр. и информатики. - 2006. - № 3. - С. 147–156. 3. Сорокопуд С. А. Обеспечение информационной безопасности корпоративной сети предприятия / С. А. Сорокопуд, Л. В. Мудрова, С. В. Ширяев // Захист інформації. - 2005. - № 1. - С. 21–30. 4. Тимошенко А. О. Синтез систем захисту інформації з використанням логіко-імовірнісних методів: автореф. дис... канд. техн. наук: 05.13.21 / А. О. Тимошенко; Нац. техн. ун-т України "Київ. політехн. ін-т". - К., 2002. - 20 с. 5. *Будько М. М., Василенко В. С., Короленко М. П. Варіант формалізації процесу захисту інформації в комп'ютерних системах та оптимізації його цільової функції / М. Будько // Реєстрація, зберігання і обробка даних. – 2000. – № 2, Т. 2.– С. 73–84*

.