УДК 004.9

МОДЕЛЬ ФАКТОРІВ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ МОБІЛЬНИХ ПРИСТРОЇВ

Ю. Ф. Петяк

Українська академія друкарства,
вул. Підголоско, 19, Львів, 79020, Україна

Створено орієнтований граф визначеної експертним опитуванням множини факторів, які сприяють виникненню загроз інформаційній безпеці мобільних пристроїв, проаналізовано взаємозв'язки між ними. Розроблено ієрархічну модель пріоритетного впливу ключових факторів загроз.

Ключові слова: *інформаційна безпека, загроза, мобільні пристрої, орієнтований граф, ієрархічна модель, матриця досяжності.*

Постановка проблеми. В умовах розвитку інформаційного суспільства, в якому важливу роль відіграють мобільні технології, необхідно більше уваги надавати питанням забезпечення захисту даних на мобільних пристроях. Галузь мобільних технологій динамічно розвивається, з'являються нові способи застосування мобільних пристроїв, у зв'язку з чим постають нові проблеми, розв'язання яких потребує розробки досконаліших технологій захисту даних. Аналіз негативних наслідків для інформаційної безпеки (ІБ) вимагає обов'язкової ідентифікації актуальних загроз ІБ мобільних пристроїв та факторів, які сприяють їх появі. У процесі такого аналізу треба переконатися, що визначено всі джерела загроз та зіставлені з ними всі можливі фактори. Ці фактори можуть мати різну природу (зумовлену властивостями архітектури та умовами функціонування системи, використаним програмним забезпеченням й апаратною платформою) і ступінь небезпеки. Це, своєю чергою, потребує різної реакції на появу конкретної загрози.

Аналіз останніх досліджень та публікацій. Для керування ризиками в сфері ІБ використовуються відповідні методики. Наприклад, в роботах [1–2] розглянуто одну з найперших методик CRAMM (CCTA Risk Analysis and Management Method), розроблену за підтримки агентства з комп'ютерів і телекомунікацій (CCTA) Великобританії. В основі методу CRAMM лежить комплексний підхід до оцінювання ризиків, що поєднує кількісні та якісні методи аналізу. Метод є універсальним і підходить для великих та дрібних організацій як урядового, так і комерційного сектора. Останнім часом популярною методикою оцінювання ризиків стала OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), яку розробляє інститут Software Engineering Institute (SEI) при університеті Карнегі Меллон (Carnegie Mellon University), її застосування розглянуто в працях [3–4]. Обидві методики розбивають весь процес виявлення та оцінювання ризиків на етапи, зокрема етап ідентифікації цінних ресурсів і границі системи, етап визначення загроз і вразливостей, етап розробки стратегії захисту та політики безпеки. Однак ці методики є високорівневими, охоплюють широкий спектр проблем та питань стосовно ІБ, і недостатньо

уваги надають питанням визначення факторів та їх пріоритетів, котрі сприяють появі загроз ІБ.

Ризики ІБ зумовлені багатьма факторами. Визначити їх можуть лише експерти, використовуючи для цього власний досвід та евристичні методи досліджень. Однак думки експертів можуть відрізнятися, що пов'язано з досвідом експерта та його компетенцією. Тому на завершальному етапі проведення експертного опитування важливо отримати узгоджену оцінку залучених експертів, яка є більш наближеною до істинного значення, ніж індивідуальні оцінки експертів [5].

Мета статті — визначити пріоритети факторів загроз та розробити модель ієрархії факторів за допомогою засобів теорії графів і методів системного аналізу [6], що дасть можливість встановити взаємозв'язки цих факторів та оцінити їх важливість, щоб прийняти обґрунтоване рішення щодо протидії атаці.

Виклад основного матеріалу дослідження. Нехай сукупність факторів, які мають вплив на можливість реалізації атаки, належить до деякої множини. З цієї множини оберемо підмножину важливіших ключових факторів. Для полегшення формального опису факторів доповнимо їх мнемонічними назвами та подамо в табл. 1.

Таблиця 1

Фактори впливу на рівень захисту даних МП

Елемент множини	Назва фактора	Мнемонічна назва
z_1	Несанкціоноване розробником втручання у систему	НВС
z_2	Наявність каналів передавання даних	КПД
z_3	Локація	Л
z_4	Кваліфікація користувача	КК
z_5	Технічна підтримка розробника	ТП
z_6	Наявність засобів захисту інформації	ЗЗ
z_7	Інтегрований показник надійності встановленого ПЗ	ІПН
z_8	Можливість встановлення ПЗ із сторонніх джерел	СД

Аналіз множини факторів та зв'язків між ними дає змогу зобразити їх у вигляді орієнтованого графа (рис. 1).

Вершини графа — елементи множини Z_1, а дуги з'єднують суміжні пари вершин (z_i, z_j), зв'язок між якими вказує на залежність одного z_i фактора від іншого z_j. Наприклад, технічна підтримка (ТП) розробника мобільного пристрою для підтримки його операційної системи в актуальному стані та наявність програмних засобів захисту даних (ЗЗ) практично не впливають на рівень безпеки пристрою, якщо було здійснено несанкціоноване розробником втручання у систему (НВС), тобто зміна режиму роботи системних елементів. В цьому випадку фактори ТП та ЗЗ прямо залежать від фактора НВС.

На основі поданого графа будуємо бінарну матрицю залежності А для множини Z_1, використовуючи алгоритм:

$$a_{ij} = \begin{cases} 1, \text{якщо фактор } i \text{ залежить від фактора } j, \\ 0, \text{якщо фактор } i \text{ незалежить від фактора } j. \end{cases} \quad (1)$$

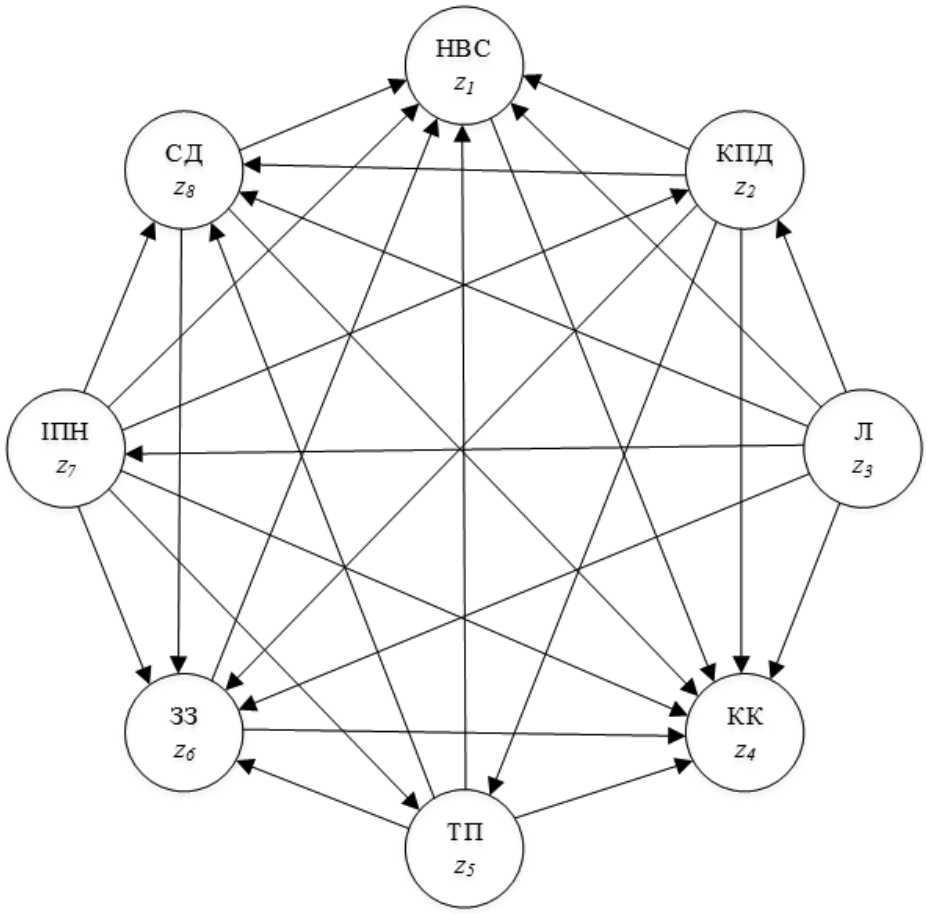

Рис. 1. Граф зв’язків між факторами впливу на можливість реалізації атаки

Матриця залежності А розмірністю 8х8 елементів має такий вигляд:

	ННВС	ККПД	ЛЛ	ККК	ТТП	ЗЗ	ІІПН	ССД
НВС	0	0	0	1	0	0	0	0
КПД	1	0	0	1	1	1	0	1
Л	1	1	0	1	0	1	1	1
КК	0	0	0	1	0	0	0	0
ТП	1	0	0	0	0	1	0	1
ЗЗ	1	0	0	1	0	0	0	0
ІПН	1	1	0	1	1	1	0	1
СД	1	0	0	1	0	1	0	0

Використовуючи матрицю залежності А, будуємо матрицю досяжності А´ таким чином. Формуємо бінарну матрицю (М + А), де М — одинична матриця. В результаті матриця досяжності має задовольняти умову:

$$(\mathrm{M}+\mathrm{A})^{k-1} \leq (\mathrm{M}+\mathrm{A})^{k} = (\mathrm{M}+\mathrm{A})^{k+1}. \quad (2)$$

Побудова матриці досяжності A′ зводиться до заповнення її бінарними елементами за таким правилом:

$$a'_{ij} = \begin{cases} 1, \text{якщо з вершини } i \text{ можна потрапити у вершину } j, \\ 0, \text{в іншому випадку.} \end{cases} \quad (3)$$

Будуємо бінарну матрицю досяжності A′ для множини вершин Z_1.

	ННВС	ККПД	ЛЛ	ККК	ТТП	ЗЗ	ІІПН	ССД
НВС	1	0	0	1	0	0	0	0
КПД	1	1	0	1	1	1	0	1
Л	1	1	1	1	1	1	1	1
КК	0	0	0	1	0	0	0	0
ТП	1	0	0	1	1	1	0	1
ЗЗ	1	0	0	1	0	1	0	0
ІПН	1	1	0	1	1	1	1	1
СД	1	0	0	1	0	1	0	1

Вершина Z_j досягається з вершини Z_i, якщо в графі (рис. 1) існує шлях, який приводить з вершини Z_i до вершини Z_j. Така вершина називається досяжною. Позначимо їх підмножину через $N(z_i)$. Аналогічно вершина z_i є попередницею вершини Z_j, якщо вона досягається з цієї вершини. Позначимо сукупність вершин-попередниць через $W(z_i)$. Відповідно, перетин підмножин вершин досягнутих і вершин попередниць позначимо, як

$$Q(z_i) = N(z_i) \cap W(z_i). \quad (4)$$

Вершини підмножини $Q(z_i)$ не досягаються з будь-якої з вершин множини $N(z_i)$, що залишилися. Ця множина визначає певний рівень ієрархії пріоритетності дії факторів, які відповідають цим вершинам. Додатковою умовою при цьому є забезпечення рівності

$$W(z_i) = Q(z_i). \quad (5)$$

Виконання описаних дій визначає початковий (найнижчий) рівень ієрархії факторів. Для отримання вказаного рівня на основі матриці досяжності A′ та з використанням залежностей (4) та (5) будуємо таблицю першої ітерації (табл. 2).

Таблиця 2

Перша ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
1	1, 4	1, 2, 3, 5, 6, 7, 8	1
2	1, 2, 4, 5, 6, 8	2, 3, 7	2
3	1, 2, 3, 4, 5, 6, 7, 8	3	3
4	4	1, 2, 3, 4, 5, 6, 7, 8	4
5	1, 4, 5, 6, 8	1, 2, 5, 7,	1, 5
6	1, 4, 6,	2, 3, 5, 6, 7, 8	6
7	1, 2, 4, 5, 6, 7, 8	3, 7	7
8	1, 4, 6, 8	2, 3, 5, 7, 8	8

Як видно з табл. 2, на першій ітерації рівність (5) виконується для фактора номер 3 (локація). Цей фактор буде елементом першого рівня ієрархії, який має найнижчу пріоритетність впливу на процес визначення загроз ІБ на мобільних пристроях. Згідно з методом аналізу ієрархій [7], вилучаємо з табл.2 рядок елемента за номером 3, а в другому стовпчику викреслюємо цифру 3. Таким чином отримуємо нову таблицю для проведення другої ітерації знаходження номерів факторів, які визначають другий рівень ієрархії.

Аналогічно проводимо наступні ітерації з повторенням відповідних обчислень для визначення з 2-го по 7-й рівень ієрархії. У результаті отримуємо таке розміщення факторів за рівнями ієрархії: 2-й рівень — фактор 7 (інтегрований показник надійності встановленого ПЗ) (табл. 3), 3-й рівень — фактор 2 (наявність каналів передачі даних) (табл. 4), 4-й рівень — фактор 5 (технічна підтримка розробника) (табл. 5), 5-й рівень — фактор 8 (можливість встановлення ПЗ зі сторонніх джерел) (табл. 6), 6-й рівень — фактор 6 (наявність засобів захисту інформації) (табл. 7), 7-й рівень — фактор 1 (несанкціоноване розробником втручання у систему) (табл. 9), а найвищому рівню відповідає фактор 4 (кваліфікація користувача).

Таблиця 3

Друга ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
1	1,4	1, 2, 5, 6, 7, 8	1
2	1, 2, 4, 5, 6, 8	2, 7	2
4	4	1, 2, 4, 5, 6, 7, 8	4
5	1, 4, 5, 6, 8	1, 2, 5, 7	1,5
6	1, 4, 6	2, 5, 6, 7, 8	6
7	1, 2, 4, 5, 6, 7, 8	7	7
8	1, 4, 6, 8	2, 5, 7, 8	8

Таблиця 4

Третя ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
1	1, 4	1, 2, 5, 6, 8	1
2	1, 2, 4, 5, 6, 8	2	2
4	4	1, 2, 4, 5, 6, 8	4
5	1, 4, 5, 6, 8	1, 2, 5	1,5
6	1, 4, 6	2, 5, 6, 8	6
8	1, 4, 6, 8	2, 5, 8	8

Таблиця 5

Четверта ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
1	1, 4	1, 5, 6, 8	1
4	4	1, 4, 5, 6, 8	4

Продовження табл. 5

5	1, 4, 5, 6, 8	1, 5	1, 5
6	1, 4, 6	5, 6, 8	6
8	1, 4, 6, 8	5, 8	8

Таблиця 6

П’ята ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
1	1, 4	1, 6, 8	1
4	4	1, 4, 6, 8	4
6	1, 4, 6	6, 8	6
8	1, 4, 6, 8	8	8

Таблиця 7

Шоста ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
1	1, 4	1, 6	1
4	4	1, 4, 6	4
6	1, 4, 6	6	6

Таблиця 8

Сьома ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
1	1, 4	1	1
4	4	1, 4	4

Таблиця 9

Восьма ітерація визначення ієрархії пріоритетності дії факторів

i	$N(z_i)$	$W(z_i)$	$N(z_i) \cap W(z_i)$
4	4	4	4

Отже, у результаті виконання дій над елементами вихідного графа (рис. 1) одержимо ієрархічно структуровану за рівнями модель (рис. 2), яка визначає пріоритетність впливу визначених експертним опитуванням факторів загроз ІБ мобільних пристроїв.

У розв’язанні поставленого завдання визначальним є обґрунтований вибір факторів, які мають вирішальний вплив на процес захисту даних, і встановлення експертним методом множини взаємозв’язків між ними. Ці дані задають у вигляді орієнтованого графа і проектують суб’єктивне бачення експертами елементів систем захисту даних. Поява конкретного фактора на конкретному рівні насамперед залежить від кількості та змісту взаємозв’язків між факторами.

Можна стверджувати, що найбільше впливають на захист даних фактори кваліфікації користувача та несанкціонованого розробником втручання у систему, що їх часто називають експерти у звітах інцидентів з приводу ком-

прометації даних на МП. Проте у пропонованій роботі ці фактори отримали теоретичне обґрунтування, що свідчить про достовірність одержаних наукових результатів.

Рис. 2 Модель ієрархії факторів загроз ІБ мобільних пристроїв

Висновки. Результат дослідження — розроблена ієрархічна графічна модель пріоритетного впливу визначених експертним опитуванням факторів загроз ІБ мобільних пристроїв. Перспективним завданням дослідження моделей факторів може бути їх подальша оптимізація для створення автоматизованих систем керування та моніторингу мобільних пристроїв (mobile device management, MDM) для малого та середнього бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zeki Yazar. A Qualitative Risk Analysis and Management Tool – CRAM [Електронний ресурс] // SANS Institute InfoSec Reading Room: [сайт]. — Режим доступу:

https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 (01.10.2015).
2. Симонов С. Технологии и инструментарий для управления рисками / С. Симонов // JetInfo: информационный бюллетень. — 2003. — №2 (117).
3. Alberts C., Dorofee A. OCTAVE threat profiles [Електронний ресурс] // Carnegie Mellon Software Engineering Institute: [сайт]. — Режим доступу: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf (22.09.2015).
4. Storms A. Using vulnerability assessment tools to develop an OCTAVE Risk Profile // SANS Institute. Part of Information security reading room: [сайт]. — Режим доступу: http://www.sans.org/reading-room/whitepapers/auditing/vulnerability-assessment-tools-develop-octave-risk-profile-1353 (29.09.2015).
5. Грабовецький Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання / Б. Є. Грабовецький. — Вінниця : ВНТУ, 2010. — 171 с.
6. Лямець В. И. Системный анализ: Вводный курс / В. И. Лямець. — Харьков : ХНУРЭ. — 2004 — 448 с.
7. Саати Т. Л. Взаимодействие в технических системах / Т. Л. Саати // Техническая кибернетика. — 1979. — №1. — С . 68–84.

MODEL OF FACTORS OF INFORMATION SECURITY THREATS ON MOBILE DEVICES

Yu. F. Petyak

Ukrainian Academy of Printing,
19, Pidholosko St., Lviv, 79020, Ukraine

We have created a directed graph of the set of factors determined by the expert survey, which contribute to information security threats of mobile devices; we have analyzed the relationship between them. We have developed a hierarchical model of priority impact of key factors of threats.

Keywords: *information security, threat, mobile devices, directed graph, hierarchical model, reachability matrix.*

Стаття надійшла до редакції 18.05.2015.