УДК 681.3.06 **DOI:10.30837/rt.2022.2.209.12**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук, Ю.С. ОСИПЕНКО

КОНЦЕПЦІЯ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ

Вважається, що основним підходом до забезпечення кібер- і інформаційної безпеки інформаційної системи є стратегія захисту на основі ризику [1]. Одним з головних завдань управління інформаційними ризиками є об'єктивно ідентифікувати і оцінити найбільш значущі для об'єкта критичної інфраструктури ризики. В [2] визначені критерії підходів до вибору методів оцінки і управління ризиками безпеки. Саме тому, на наш погляд, актуальним є пошук методів оцінки і управління ризиками безпеки, які в певній мірі відповідають визначеним критеріям. У цьому дослідженні використано один з відомих підходів до моделювання, – «дерево атак» [3]. Метод «дерева атак» є систематичним методом визначення характеристик безпеки системи на основі всіх атак, яким піддається інформаційна система. Виявлення всіх можливих атак полегшує аналіз можливих шляхів реалізації кібератак та вибір адекватних контрзаходів і їх оптимальне використання. Дерево атаки складається з вузлів, ребер та з'єднувальних елементів, де кожен вузол відповідає кроку атаки. Кореневий вузол є кінцевою метою зловмисника, а дочірні вузли даного вузла представляють підцілі. Ребра представляють зміну стану, спричинену діями зловмисника. З'єднувальний елемент – це шлях для просування до мети атаки: АБО (диз'юнктивне), чи І (кон'юнктивне) для вузлів із двома або більше дочірніми елементами.

Основні результати досліджень

Архітектура інформаційної системи

Інформаційна система компанії, відповідно до її компонентів, може бути розділена на дві частини: компоненти, які доступні користувачеві (наприклад, термінал), і компоненти, які доступні тільки постачальнику послуг, такі як сервер центрального офісу компанії. Можливі сценарії загроз безпеки, засновані на потоці інформації через зазначені компоненти, наведені нижче [4, 5] (рис. 1):

1) Поширення шкідливого коду у обладнанні, порушення бар'єру безпеки, доступ до конфіденційної інформації користувача та отримання доступу до основного сервера через сенсорний пристрій.

2) Виток інформації або підробка даних у процесі передачі даних.

3) Виявлення (вимірювання) ризиків витоку даних через вразливості у персональному комп'ютері (ПК), смарт-пристрої чи шлюзі, який використовується для передачі даних сховищем або персоналом.

4) Ризики кібератак через вразливість основного сервера та репозиторію в зоні дії провайдера.

Виявлення та ідентифікація загроз інформаційної системи компанії

Для того щоб виявити загрози, що можуть бути використані для побудови дерева атак інформаційної системи компанії, доцільно обрати типові та засновані на відповідних сценаріях загрози безпеки відповідно до ISO/IEC 27005 [6, 7]. Нарешті, щоб визначити вразливості інформаційної системи компанії, доцільно структурувати використані загрози, щоб зробити їх придатними для середовища інформаційної системи компанії відповідно до ISO/IEC 27005. Отримані дані використовувалися як компоненти дерева атак інформаційної системи компанії. Відповідно до архітектури системи, виявлених загроз безпеки та уразливостей, пропонується виділити сім областей загроз безпеці інформаційної системи компанії (рис. 2).

Рис. 1. Архітектура інформаційної системи компанії

Рис. 2. Області, що пов'язані із загрозами безпеки

Варіанти використання областей загроз безпеки інформаційної системи

З а г р о з а 1 : Користувач

При використанні користувачами терміналів часто виникають загрози безпеці, що пов'язані з помилками використання пристроїв, слабкими паролями, втратою пристроїв, фішингом тощо.

З а г р о з а 2 : Пристрої

Термінали засновані або на операційній системі загального призначення (GPOS) або на вбудованій операційній системі реального часу (RTOS). Пристрої на базі RTOS захищені від несанкціонованого доступу, оскільки вони оптимізовані для конкретних функцій на етапах проектування та виробництва. І навпаки, пристрої на основі GPOS, такі як смартфони, вразливі для загроз безпеки, оскільки вони використовують зовнішні програми. Використання терміналів у таких умовах робить їх вразливими для загроз безпеки через функції збереження та обміну даними цих пристроїв, а також ризик втрати/крадіжки пристрою, уразливості додатків та передачі відкритого тексту.

З а г р о з а 3 : Домашня мережа (мережа філіалу компанії)

Передача інформації між терміналом в особистому просторі користувача (вдома або в офісі) та до серверу центрального офісу компанії відбувається переважно бездротовою мережею. Як показано на рис. 3, типи мереж, що використовуються в домашніх умовах, включають LAN (локальна обчислювальна мережа), Wi-Fi, Bluetooth, NFC (комунікація ближнього радіусу дії) та мережі довгострокової еволюції. У той час як деякі пристрої вбудованого типу повинні бути підключені до локальних мереж, інтелектуальні пристрої на основі GPOS можуть зв'язуватися із сервером центрального офісу компанії. У таких умовах сервісні

системи на базі домашніх мереж піддаються загрозам безпеці, пов'язаним із наскрізною передачею відкритого тексту та атаками посередника (MITM-атаками) (рис. 3) [8].

З а г р о з а 4 : Шлюз, наприклад, VPN

Шлюз відіграє роль посередника між користувачем та сервером центрального офісу компанії, піддаючи систему загрозам безпеці, пов'язаними з шахрайськими шлюзами, а також втратою/крадіжкою шлюзів та MITM атаками [8].

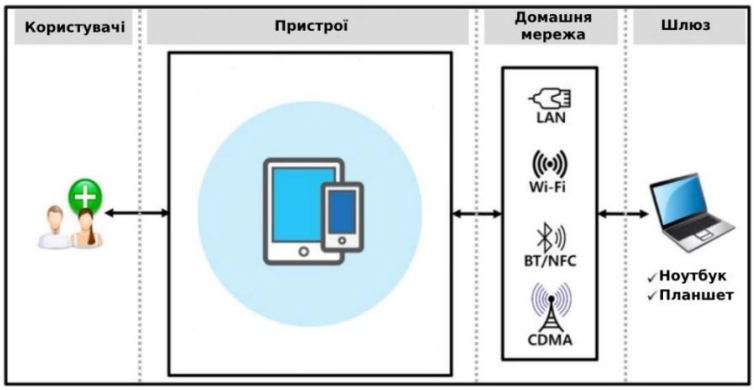

Рис. 3. Домашня мережа

З а г р о з а 5 : Інтернет (загальнодоступна мережа)

Зв'язок між користувачем та сервером центрального офісу компанії відбувається через мережу загального користування (Інтернет). Оскільки особиста інформація передається через загальнодоступний Інтернет, важливо встановити наскрізні правила безпеки. Крім того, потрібна зашифрована передача даних. У таких умовах інформаційна система компанії вразлива для загроз безпеки, пов'язаних з перехопленням даних, підробкою/зміною та підвищенням привілеїв [8].

З а г р о з а 6 : Сервер центрального офісу компанії

Сервер центрального офісу компанії знаходиться у місці розташування постачальника послуг. Він складається з ПК та програмного забезпечення, необхідного для віддалених консультацій, а його користувачами є персонал та системні адміністратори (співробітник служби безпеки та інший допоміжний персонал). Ця система дуже важлива, тому що вона опрацьовує всі дані користувачів. Крім того, якщо сервер центрального офісу компанії підключений до відповідних установ через урядовий мережевий концентратор, необхідні суворі правила безпеки для запобігання проникненню в державну систему. У таких умовах інформаційна система компанії може піддаватися загрозам безпеки, пов'язаним з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до мережі за допомогою обходу перевірок фізичної безпеки [8].

З а г р о з а 7 : Реалізація послуг, що надаються центральним офісом – постачальником послуг

У таких умовах інформаційна система компанії може приваблювати загрози безпеки, пов'язані з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до Korea-Net, оминаючи наявні перевірки фізичної безпеки [8]. Ця область також може бути вразливою для загроз безпеки, пов'язаних з помилками використання пристрою, витоком важливих даних та прослуховуванням телефонних розмов.

Метод дерева атак

Першим кроком в оцінці ризику безпеки є визначення задіяних активів та розрахунок їхньої вартості. Дерево атак використовується для оцінки всіх загроз безпеці, з якими може зіткнутися кожен актив, як визначено у кожній із семи областей загроз безпеці. Як показано на рис. 5, ймовірність виникнення атаки обчислюється з використанням з'єднувальних елементів АБО та І, які є входом для кожного вузла, що представляє просування атаки до мети.

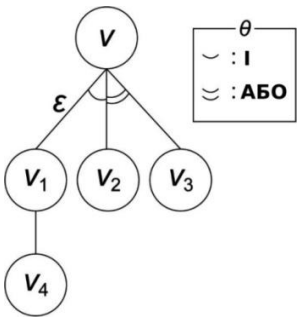

Рис. 5. Дерево атак

Теоретично, ймовірність успіху потенційної атаки збільшується прямо пропорційно до мотивації зловмисника і обернено пропорційно до зусиль, необхідних для організації атаки. У цьому дослідженні вартість активів, ймовірність виникнення атаки та ймовірність успіху атаки використовувалися як параметри оцінки ризиків безпеки, пов'язаних з інформаційною системою компанії.

На рис. 6 наведено приклад того, як проводиться оцінка ризиків. Методика оцінки ризику може бути стисло викладена наступним чином.

1. Оцінка вартості активів інформаційної системи компанії (див. табл. 1 – 3).

Таблиця 1

Критерії оцінки вартості активів

Розподіл	**Низький**	**Помірний**	**Високий**
Конфіденційність	1	2	3
Цілісність	1	2	3
Доступність	1	2	3
Внесок активів	1	2	3

Таблиця 2

Класифікація вартості активів

Мета безпеки	**Потенційна дія**	**Опис**
Конфіденційність	Високий	Повинний бути доступним усередині лише уповноваженим особам; несанкціоноване розкриття інформації може призвести до порушення конфіденційності особи та/або фатального пошкодження інформаційної системи компанії.
	Помірний	Може бути розкритий усередині, але у разі зовнішнього впливу може викликати серйозні проблеми щодо конфіденційності та інформаційної системи компанії.
	Низький	При впливі зовнішніх осіб матиме незначний вплив на приватне життя та інформаційну систему компанії.
Цілісність	Високий	Випадкові або навмисні зміни можуть завдати серйозної шкоди приватному життю або інформаційній системі компанії.
	Помірний	Випадкові або навмисні зміни можуть завдати значної шкоди особистому життю або інформаційній системі компанії.
	Низький	Випадкові або навмисні зміни матимуть незначний вплив на особисте життя або інформаційну систему компанії.
Доступність	Високий	Переривання обслуговування може призвести до фатального пошкодження інформаційної системи компанії.
	Помірний	Переривання обслуговування може призвести до значного пошкодження інформаційної системи компанії.
	Низький	Переривання обслуговування завдасть незначної шкоди інформаційній системі компанії.
Внесок активів	Високий	Актив необхідний для послуг інформаційної системи компанії.
	Помірний	Актив частково потрібний для обслуговування інформаційної системи компанії.
	Низький	Актив відіграє допоміжну роль у послугах інформаційної системи компанії.

Таблиця 3

Класифікація вартості активів

Шкала важливості	Сумарна оцінка	Опис
1	4-5	Може завдати шкоди активам, однак майже не впливає на інформаційну систему компанії.
2	6-7	Пошкоджений актив незначно впливає на пов'язаний домен або систему.
3	8-9	Пошкодження активів призводить до значних втрат для бізнесу.
4	10-11	Пошкодження активів призводить до дуже значних втрат для бізнесу.
5	12	Пошкодження активів призводять до великих втрат для бізнесу, який може перестати функціонувати.

2. Оцінка ймовірності виникнення внутрішніх та зовнішніх атак на інформаційну систему компанії (див. табл. 4).

Таблиця 4

Критерії оцінки ймовірності виникнення атаки

Розподіл	Низький	Помірний	Високий
	1	2	3
Ймовірність виникнення атаки	1-50%	51-80%	81-100%

3. Оцінка ймовірності успіху внутрішніх та зовнішніх атак на інформаційну систему компанії (див. табл. 5 – 7).

Таблиця 5

Оцінки різних аспектів потенціалу атаки

Фактор	Рівень	Значення
Витрачений час	≤ 1 день	0
	≤ 1 тиждень	1
	≤ 1 місяць	4
	≤ 3 місяці	10
	≤ 6 місяців	17
	>6 місяців	19
	недоцільно	∞
Експертиза	Непрофесіонал	0
	Досвідчений	3
	Експерт	6
	Численні експерти	8
Знання системи	Відкритий	0
	Обмежений	3
	Секретний	7
	Критичний	11
Можливість доступу	Непотрібний/необмежений	0
	Легкий	1
	Помірний	4
	Важкий	10
	Відсутній	∞
Обладнання	Стандартний	0
	Спеціалізований	4
	Індивідуальний	7
	Ряд індивідуальних	9

Таблиця 6

Оцінки ймовірності успіху атаки

Значення	**Потенціал атаки, необхідний для виявлення та використання сценарію атаки**	**Ймовірність успіху атаки**
0-9	Базовий	5
10-13	Розширений базовий	4
14-19	Помірний	3
20-24	Високий	2
≥ 25	За межами високого	1

Таблиця 7

Приклади оцінок ймовірності успіху атаки

Атака	**Витрачений час**	**Експертиза**	**Знання системи**	**Можливість доступу**	**Обладнання**	**Потрібний потенціал атаки**	
						Сума	Оцінка
Витік інформації про клієнта з пристрою	0	6	7	4	4	21	Високий
Підробка шляхом прослуховування телефонних розмов та спуфінг	0	3	0	4	4	11	Помірний
MITM-атаки з використанням шахрайської точки доступу	0	6	3	10	4	23	Високий
Підбір інформації	0	0	0	4	4	8	Базовий

4. Вибір пріоритетної мети для забезпечення безпеки інформаційної системи компанії (див. табл. 8 та 9).

Таблиця 8

Оцінки значення ризику

Значення	**Рівень**
1-12	Низький
13-32	Помірний
≥33	Високий

Таблиця 9

Оцінки значення ризику

Актив		**Вартість активу**	**Проблема**	**Ймовірність виникнення атаки AOP)**	**Ймовірність успіху атаки (ASP)**	**Значення ризику (RV)**	
Пристрій	RTOS	5	Витік інформації про користувачів	1	2	10	H
	GPOS	5	Ненадійний пароль	2	5	50	B
	Шлюз	5	Критична інформація, що передається через помилки в роботі пристрою	3	4	60	B
		5	Збитки через неправильне поводження з пристроєм	2	5	50	B

Продовження табл. 9

		5	Доступ до внутрішньої системи та розкриття важливої нформації через вразливість застосунків пристрою	2	4	40	В
		5	Пристрій: передача відкритого тексту між внутрішньою системою	3	5	75	В
		5	Пристрій: передача відкритого тексту між інформаційною системою компанії	3	5	75	В
		5	Пристрій: MITM-атаки між інформаційною системою компанії	3	1	15	П
		5	Шлюз: передача відкритого тексту між внутрішньою системою	3	3	27	П
		5	Витік інформації через зараження шкідливе ПЗ	1	2	10	Н
		5	Розкриття важливої інформації шляхом зламування шлюзу	2	1	10	Н
		5	MITM-атаки з використанням шахрайського шлюзу	2	1	10	Н
		5	Значний витік інформації з втраченого/викраденого шлюзового пристрою	2	3	30	П
ПК	ПК	4	Підробка шляхом прослуховування телефонних розмов та спуфінгу	3	5	60	В
		4	Несанкціонований доступ через MITM-атаки	2	3	24	П
		4	Шлюз: передача відкритого тексту між інформаційною системою компанії	3	5	60	В
		4	MITM-атаки з використанням шахрайської точки доступу	2	1	8	Н
		4	Витік інформації через зараження шкідливим ПЗ	1	2	8	Н
		4	Розкриття важливої інформації через злам шлюзу	1	1	4	Н
		5	Доступ до внутрішньої системи, що використовується незатвердженим пристроєм	1	1	5	Н
		5	Витік інформації з пристрою через зараження шкідливим ПЗ	1	1	5	Н
		5	Збереження важливої інформації у пристрої	2	4	40	В
		5	Витік важливої інформації з втраченого/викраденого пристрою	2	4	40	В

Закінчення табл. 9

		4	Внутрішній доступ до національних мереж зв'язку шляхом засобів фізичного захисту	1	1	4	Н
		4	Внутрішній доступ до національних мереж зв'язку шляхом використання вразливості бездротової мережі	1	1	4	Н
		4	Залишення робочого місця на тривалий час після входу в систему	2	5	40	В
		4	Збій безвідмовності через відсутність збереження записів, до яких здійснюється доступ	1	5	20	П
		4	Аварія через помилки в роботі інформаційної системи компанії	1	5	20	П
ПЗ	ПЗ для передачі даних	3	Доступ до внутрішньої системи та розкриття важливої інформації шляхом експлуатації вразливості програми, що використовується	1	1	3	Н
	ПЗ для моніторингу	2	Доступ до внутрішньої системи через файли оновлень для ПЗ	2	1	4	Н
Інформація	Особиста інформація	4	Підбір	3	3	36	В

Вартість активів

Національний інститут стандартів та технологій США (NIST) розробив концепцію управління ризиками: Risk Management Framework for Information Systems and Organizations для захисту комп'ютерних мереж від кібератак [2]. Керівні принципи NIST-RMF поділяють дії з управління ризиками на наступні етапи життєвого циклу: 1) підготовка організації до впровадження концепції RMF. 2) категоріювання інформації та інформаційних систем; 2) вибір (на основі таких факторів, як мінімальні вимоги безпеки та аналіз витрат) заходів захисту; 3) впровадження заходів безпеки); 4) оцінювання безпеки; 5) авторизація безпеки; 6) постійний моніторинг безпеки. Зазначені елементи концепції RMF запропоновані і гармонійно відповідають моделі побудови системи управління інформаційною безпекою організації: ПВПД (плануй, виконуй, перевіряй, дій), яка визначена у стандарті ISO/IEC 27005 [6], і яка, у свою чергу, є частино системи управління організацією. Публікація FIPS PUB 199 [9] визначає критерії категоризації інформації та безпеки інформаційних систем (на основі потенційного впливу системи). FIPS PUB 199 встановлює три цілі безпеки (конфіденційність, цілісність та доступність) та визначає рівні потенційного впливу порушень безпеки на окремих осіб та організації як низький, помірний та високий. При категоризації загальна вартість кожного активу (рис. 6), що підлягає захисту, розраховується наступним чином:

$$AV_a = \sum_{i=1}^{n} A_i\,, \tag{1}$$

де AV_a – сума значень активів (3–12) активу a, розрахована як сума коефіцієнтів, пов'язаних із значеннями активів (1–3: вклад конфіденційності, цілісності та доступності).

У табл. 1 наведено критерії оцінки вартості активів. Вартість активів кожного з чотирьох елементів (цілей безпеки) оцінюється за трибальною шкалою. Загальна оцінка вартості активів розраховується шляхом додавання всіх індивідуальних оцінок, а клас вартості активів

визначається на основі обчисленого результату. Вартість активів оцінюється по відношенню до кожної з цілей безпеки за допомогою трьох рівнів, що відповідають потенційним наслідкам кожної мети безпеки, як описано в табл. 2, і варіюються від 3 до 12. Підставляючи розраховане значення рівняння (1) можна отримати ступінь важливості активу, залежну від вартості активу, яка варіюється від 1 до 5.

У табл. 3 представлені визначення кожного зі ступенів важливості активів, класифікованих вище. Оцінені вартості активів аналізуються з використанням положень, визначених у ISO/IEC 27005 [6] та ISO 31000 RM [10] та перевіряються з використанням методу оцінки ризику, заснованого на урахуванні конфіденційності, цілісності та доступності, відповідно до NIST 800–37 RMF, FIPS PUB 199, виду відмови, наслідків загроз та аналізу критичності активу.

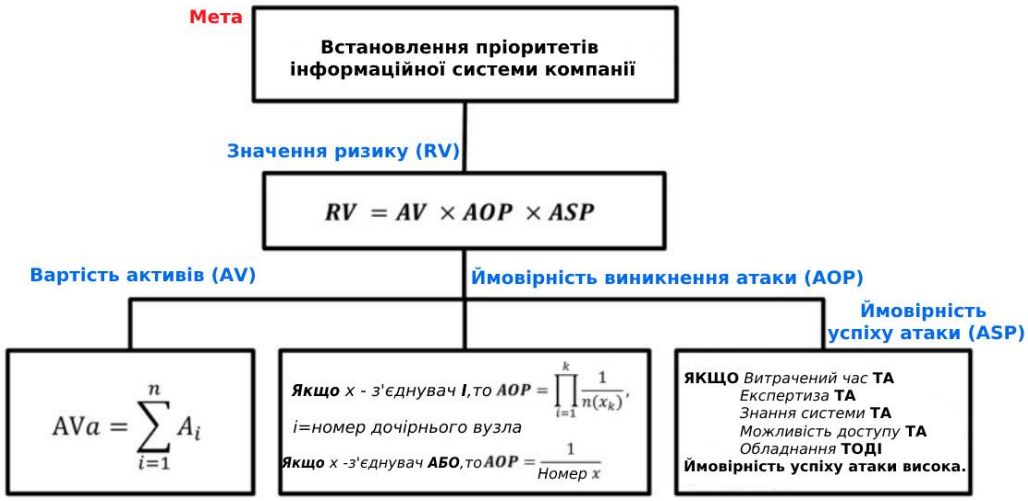

Рис. 6. Етапи оцінки ризиків інформаційної системи компанії

Ймовірність виникнення атаки

Ймовірність виникнення атаки (AOP – Attack occurrence probability) визначається як відношення кількості подій атаки всіх вузлів до кількості дочірніх вузлів атаки, пов'язаних із кореневим вузлом із ціллю досягнення мети атаки кореневого вузла. Нехай один з вузлів – X буде кінцевим вузлом, тоді AOP = 1 (див. рівняння (2), (3)).

$$\text{Якщо } x - \text{з}'\text{єднувальний елемент I, то } AOP = \prod_{i=1}^{k} \frac{1}{n(x_k)}, \quad i = \text{номер вузла}. \tag{2}$$

$$\text{Якщо } x - \text{з}'\text{єднувальний елемент АБО, то } AOP = \frac{1}{\text{Номер } x}. \tag{3}$$

Однак у цьому випадку дерево атак має два основних обмеження. По-перше, вузлам не привласнюється вага, хоча кожен вузол має різний рівень ризику та його потенційна загроза може призвести до різного ступеня збитків. По-друге, замість порівняння ймовірностей появи вузлів вказується лише ймовірність досягнення мети верхнього вузла без урахування частоти появи вузла та рівня ризику кожного вузла, що ускладнює кількісну оцінку вразливостей загроз для безпеки пристроїв. Ймовірність виникнення атаки розраховується шляхом розробки дерева атак для кожного сценарію загроз безпеки відповідно до сімох областей загроз безпеки, як показано на рис. 7. Ймовірність виникнення атаки для прикладу на рис. 7 можна розрахувати в такий спосіб. Оскільки для досягнення v_4 можна вибрати v_8 або v_9, v_2 має ймовірність виникнення атаки 1/2. Крім того, оскільки для досягнення v_4 необхідно вибрати один з методів, представлених v_4, v_5, v_6 і v_7, його ймовірність виникнення атаки становить 1/4. Оскільки для досягнення v_1 обрано єдиний вузол v_3, його ймовірність виникнення

атаки дорівнює 1. Отже, якщо метою атаки є користувач, ймовірність виникнення атаки для витоку інформації про користувача становить 6,25%, як показано нижче:

$$AOP = \frac{1}{2} \times \frac{1}{4} \times \frac{1}{2} = \frac{1}{16} \times 100. \quad (4)$$

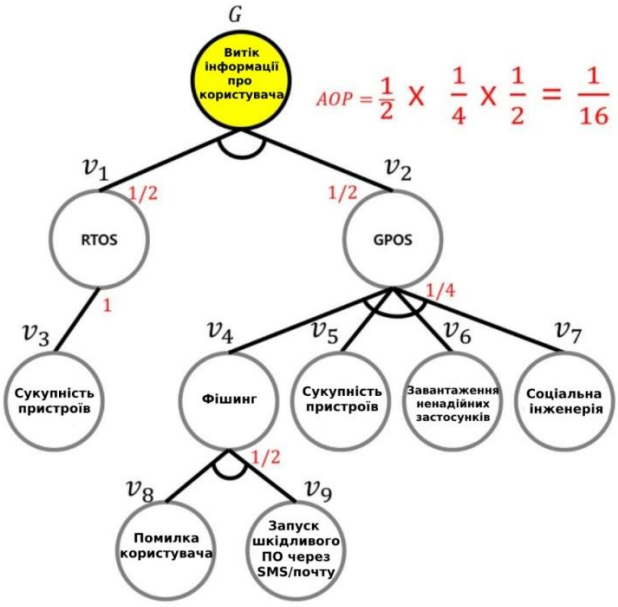

Рис. 7. Приклад дерева атак сценарію загроз безпеки для користувача

Після побудови дерева атак для кожної із семи областей загроз безпеки розраховується ймовірність виникнення атаки кожного дерева атак і, відповідно, кожній області надається оцінка. Оцінка надається кожній області на основі трибальної шкали відповідно до значення ймовірність виникнення атаки, розрахованого за рівнянням (4) та відповідно до критеріїв оцінки (табл. 4).

Ймовірність успіху атаки

Ймовірність успіху атаки (ASP–Attack success probability), визначена у ISO/IEC 15408 [11] та ISO/IEC 18045 [12], і оцінюється на основі наступних факторів [12]:

- Час, що витрачається зловмисником на виявлення вразливості, розробку методу атаки та проведення атаки;
- Необхідні спеціальні експертні знання;
- Знання досліджуваної системи;
- Можливість доступу до мети атаки;
- IT-апаратне/програмне забезпечення або інше обладнання, необхідне для виявлення та використання вразливості.

Ці фактори, що впливають на ймовірність успіху атаки, не є незалежними, а скоріше взаємозамінні з різних точок зору. Наприклад, необхідні знання та обладнання можуть бути замінені витраченим часом (див. табл. 5).

Ймовірність успіху атаки розраховується шляхом застосування значення коефіцієнта (табл. 5) відповідно до сценарію атаки для семи областей загроз безпеки. Потім надається оцінка на основі значення потенціалу атаки (див. таблицю 6), а категоризація виконується на основі рівня потенціалу атаки (див. табл. 7). Для розрахунку ймовірності успіху атаки кожної загрози безпеці рівні ймовірності успіху атаки порівнюються з кінцевими вузлами дерева атак. Наприклад, кожен вузол на рис. 7 відображається на призначеному йому рівні ймовірності успіху атаки відповідно до оцінок ймовірності успіху атаки (див. табл. 7).

Розрахунок значення ризиків

Значення ризику (RV – Risk value) є добутком вартості активів (AV – Asset value), ймовірності виникнення атаки (AOP – Attack occurrence probability) та ймовірності успіху атаки (ASP – Attack success probability):

$$RV = AV \times AOP \times ASP\ . \tag{5}$$

Розраховані значення ризиків оцінюються на трьох рівнях: низькому, помірному та високому (див. табл. 8). При інтерпретації результатів оцінки ризику чим вище вартість активів, ймовірність виникнення атаки і ймовірність успіху атаки, тим вище значення ризику.

Результати аналізу ризиків інформаційної системи компанії відображають рівні ризику загроз безпеці і можуть бути інтерпретовані з погляду відносного ефекту даної атаки. Необхідно встановити відповідні рекомендації щодо безпеки на основі вартості активів кожної загрози з урахуванням її ймовірності виникнення атаки та ймовірності успіху атаки (див. табл. 10).

Таблиця 10

Результати аналізу ризиків

RV = AV × AOP × ASP						
Вартість активів (AV)	Ймовірність виникнення атаки (AOP)	Ймовірність успіху атаки(ASP)				
		За межами високої	Помірна	Висока	Розширена базова	Базова
Оцінка 5	Низька	5	10	15	20	25
	Помірна	10	20	30	40	50
	Висока	15	30	45	60	75
Оцінка 4	Низька	4	8	12	16	20
	Помірна	8	16	24	32	40
	Висока	12	24	36	48	60
Оцінка 3	Низька	3	6	9	12	15
	Помірна	6	12	18	24	30
	Висока	9	18	27	36	45
Оцінка 2	Низька	2	4	6	8	10
	Помірна	4	8	12	16	20
	Висока	6	12	18	24	30
Оцінка 1	Низька	1	2	3	4	5
	Помірна	2	4	6	8	10
	Висока	3	6	9	12	15

Висновки

1. Метод «дерева атак» є систематичним методом визначення характеристик безпеки системи на основі всіх атак, яким піддається інформаційна система. Виявлення всіх можливих атак полегшує аналіз можливих шляхів реалізації кібератак та вибір адекватних контрзаходів і їх оптимальне використання.

2. Щоб виявити загрози, що можуть бути використані для побудови дерева атак інформаційної системи компанії, доцільно обрати типові та засновані на відповідних сценаріях загрози безпеки відповідно до ISO/IEC 27005, а щоб визначити вразливості інформаційної системи компанії, доцільно структурувати враховані загрози та зробити їх придатними для середовища інформаційної системи компанії також відповідно до ISO/IEC 27005.

3. Основними варіантами загроз безпеки інформаційної системи є: користувач; пристрої; домашня мережа (мережа філіалу компанії); шлюз, наприклад, VPN; інтернет (загальнодоступна мережа); сервер центрального офісу компанії; загрози безпеки, пов'язані з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до KoreaNet, оминаючи наявні перевірки фізичної безпеки.

4. Запропонована концепція припускає визначення: областей загроз безпеки інформаційної системи; задіяних інформаційних активів та розрахунок їхньої вартості; оцінку ймовірності виникнення атак на інформаційну систему; оцінку ймовірності успіху атак на інформаційну систему та інше.

5. Основна перевага метода «дерева атак» в тому, що він дозволяє спеціалістам з захисту ідентифікувати потенційні атаки та впроваджувати відповідні контрзаходи. Недоліки цього підходу полягають у тому, що при його впровадженні важко врахувати всі дії і, при цьому, відсутня можливість для моделювання атак, що включають одночасні дії зловмисників.

6. Обґрунтовані методи оцінки ризику, включаючи урахування ймовірності успіху атаки та ймовірності виникнення атаки, дозволяють усунути зазначені недоліки та забезпечити більш точну ідентифікацію методів атаки, пов'язаних із поведінкою зловмисника.

7. Концепція оцінки ризиків кібербезпеки і методика аналізу та оцінки загроз безпеки, які використані, відповідають підходам до побудови ризикоорієнтованих систем управління інформаційною безпекою і можуть стати основою для розробки системи безпеки інформації в інформаційній системі об’єкта критичної інфраструктури.

Список літератури:

1. Schneier B. Attack trees. Dr Dobbs J. 1999;24:21–29. doi: 10.1002/9781119183631.ch21. [CrossRef] [Google Scholar]
2. NIST SP800–37 Rev. 2. Risk Management Framework for Information Systems and Organizations, 2018.
3. Потій О.В., Горбенко І.Д., Замула О.А., Ісірова К.В. Аналіз методів оцінки і управління ризиками кібер і інформаційної безпеки // Радіотехніка. 2021. Вип. 206. С. 5-23.
4. Maji A, Mukhoty A, Majumdar A, Mukhopadhyay J, Sural S, Paul S, et al. Security analysis and implementation of web-based telemedicine services with a four-tier architecture // Proceedings of the Second International Conference on Pervasive Computing Technologies for Healthcare. Tampere; 2008. p. 46–54. 10.4108/icst.pervasivehealth2008.2518.
5. She H, Lu Z, Jantsch A, Zheng LR, Zhou D. A network-based system architecture for remote medical applications. Asia-Pac Adv Netw. 2007;1:27–31. [Google Scholar].
6. International Organization for Standardization. Information security risk management. (second edition). ISO/IEC 27005:2011. 2011. [Google Scholar].
7. International Organization for Standardization . Health informatics – Information security management in health using ISO/IEC 27002. ISO/DIS 27799:2014(E) 2015. [Google Scholar].
8. Camara C., Peris-Lopez P., Tapiador JE. Security and privacy issues in implantable medical devices: a comprehensive survey. J Biomed Inf. 2015;55:272–289. doi: 10.1016/j.jbi.2015.04.007. [PubMed] [CrossRef] [Google Scholar].
9. Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J, Gulick J. Guide for mapping types of information and information systems to security categories. NIST SP800–64 Rev. 4. 2008. [Google Scholar].
10. International Organization for Standardization. Risk management. ISO 31000:2018. 2018. [Google Scholar].
11. International Organization for Standardization. Information technology – Security techniques – Evaluation criteria for IT security Part 1: Introduction and general model. ISO/IEC 15408–1:2009. 2009. [Google Scholar].
12. International Organization for Standardization. Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045. ISO/IEC 18045. 2015. [Google Scholar].

Надійшла до редколегії 22.05.2022

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, головний конструктор АТ «Інститут інформаційних технологій», Україна; e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

Осипенко Юлія Сергіївна – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: julie.osipenko17@gmail.com