УДК 004.056.53

ОЦІНЮВАННЯ РИЗИКУ РЕАЛІЗАЦІЇ КІБЕРНЕТИЧНИХ ЗАГРОЗ СКЛАДНИМ ІНФОРМАЦІЙНИМ СИСТЕМАМ

Ю. Г. Даник, д-р техн. наук, проф.;
В. І. Шестаков, канд. техн. наук, доц.;
С. В. Чернишук

Житомирський військовий інститут ім. С. П. Корольова
Державного університету телекомунікацій

chernuu@yandex.ru

У статті запропоновано удосконалений підхід щодо оцінювання ризику реалізації кібернетичних загроз складним інформаційним системам з урахуванням структурної уразливості таких систем.

Ключові слова: складні інформаційні системи; кібернетичні загрози; оцінювання ризику.

Advanced approach to risk assessment of cyber threats realization towards complex information system with a glance of their structural connectivity is suggested.

Keywords: complex information systems; cybernetic threats; risk assessment.

Постановка проблеми

Визначальною особливістю сучасного інформаційного суспільства є активне застосування в усіх сферах життєдіяльності складних інформаційних систем (СІС), які являють собою впорядковану сукупність значної кількості взаємопов'язаних елементів будь-якої природи, здатних обмінюватися інформацією та взаємодіяти з метою виконання визначених завдань [1].

Всебічна комп'ютеризація таких систем багатократно підвищує їх уразливість до кібернетичних загроз (КЗ) — факторів (подій, явищ) інформаційного, комунікаційного, комп'ютерно-мережевого, соціального та соціотехнічного просторів (або їх комбінації у певному поєднанні), які за умови їх умисного цілеспрямованого використання створюють небезпеку порушення процесів управління, обробки та передачі інформації, що відбуваються в сучасних СІС, або можуть зашкодити елементам таких систем [2].

Протидія КЗ вимагає розробки дієвих підходів до їх виявлення, оцінювання та локалізації. Тому завдання удосконалення методологічних основ оцінювання ризику реалізації КЗ сучасним СІС є актуальним і потребує розв'язку.

Аналіз досліджень і публікацій

Нині оцінюванню ризиків безпеки складних систем різного цільового призначення приділяється все більше уваги у багатьох галузях науки і техніки [3–5].

При цьому відсутність єдиного розуміння таких споріднених понять, як «небезпека», «безпека», «ризик», «загроза», «збиток», зумовлює значні труднощі при розробці єдиного методологічного підходу до їх оцінювання. Тому в контексті даного дослідження під *ризиком реалізації КЗ* розумітимемо міру небезпеки КЗ, яка характеризується ймовірністю появи такої загрози та величиною нанесеного збитку в разі її реалізації [6].

Оцінюванню ризиків у сфері кібернетичної безпеки присвячено значну кількість праць зарубіжних дослідників, зокрема [7–9]. Запропоновані у них підходи мають вузькоспеціалізований характер та здебільшого враховують специфічні показники функціонування складних систем окремих сфер діяльності. При цьому переважна більшість відомих підходів передбачає виконання таких етапів: характеристика системи, ідентифікація загроз та уразливостей, визначення джерел та причин реалізації загроз, розрахунок їх імовірності тощо. Це значно ускладнює процес оцінювання ризику і не дозволяє своєчасно реагувати на його зміну.

У роботах вітчизняних науковців, доступних з відкритих видань, досліджуються переважно ризики інформаційної безпеки. Враховуючи певну спорідненість сфер кібернетичної та інформаційної безпеки, можна припустити, що підходи до оцінювання ризиків у одній сфері можуть бути трансформовані для вирішення аналогічного завдання в іншій. Детальний огляд підходів оцінки ризиків інформаційної безпеки наведено в праці [6], де зазначено, що найбільшого поширення набули метод на основі байєсівських мереж, методологія Risk Management Guide for Information Technology Systems, метод VAR (Value at Risk), методика TRA (Threat and Risk Assessment), методика FRAP (Facilitated Risk Analysis Process), стандарт ISO/IEC 27005:2008 (Information technology — Security techniques — Information security risk management) та ін. Переважна більшість із них ґрунтується на методах експертного та статистичного оцінювання, що у першому випадку не забезпечує достатньої об'єктивності

оцінювання, а у другому — потребує накопичення значних об'ємів статистичних даних проявів КЗ.

Характерним недоліком існуючих моделей аналізу та оцінювання ризику складним системам є неврахування зв'язності об'єктів, які входять до складу таких систем, а також значна складність розрахунків. У результаті знижується адекватність застосовуваних моделей. Тому в умовах інтенсивного виникнення нових та динамічного поширення відомих КЗ виникає потреба у розробці методологічних основ, позбавлених від виявлених недоліків.

Мета дослідження — є розвиток підходів до оцінювання ризику реалізації кібернетичних загроз сучасним СІС з урахуванням структурної уразливості таких систем.

Виклад основного матеріалу

Зобразимо складну систему у вигляді зваженого орієнтованого графа $G=(X,U)$ (рис. 1), де X — множина його вершин ($|X|=n$), що відповідають елементам системи, а U — множина зважених дуг $(|U|=n(n-1))$, які відображають взаємозв'язки між елементами системи і позначаються впорядкованою парою $u=(x_i,x_j)$, $x_i \neq x_j$, $i,j=\overline{1,n}$, що складається з початкової x_i і кінцевої x_j вершин.

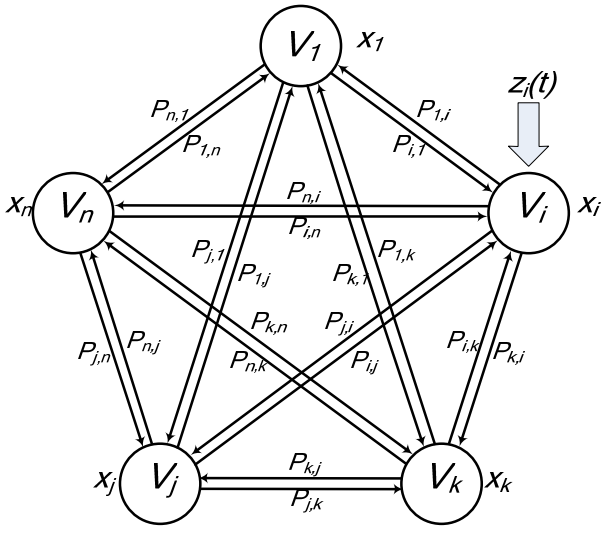

Рис. 1. Графова модель складної системи

Ступінь уразливості системи внаслідок виведення з ладу її i-го елемента можна оцінити коефіцієнтом структурної уразливості V_i, порядок розрахунку якого буде наведено нижче. Тому кожну вершину x_i графу G характеризуватимемо значенням V_i.

Нехай вага дуги (x_i,x_j) відображає ступінь залежності між елементами системи, яка вимірюється умовною ймовірністю $P_{i,j}$ виходу з ладу i-го елемента, якщо пошкоджено j-й елемент. Оцінки $P_{i,j}$ отримуються за результатами імітаційного моделювання шляхом почергового виведення з ладу одних елементів системи та реєстрування випадків порушення функціонування інших. У подальшому для спрощення позначень замість x_i можливе вживання V_i або індексу i, а замість (x_i,x_j) — $P_{i,j}$.

Позначимо $\vec{z}(t)=(z_1(t),z_2(t),...,z_n(t))$ вектор КЗ, координати якого набувають бінарних значень (0,1), що свідчить про наявність або відсутність КЗ i-му елементу системи на деякий момент часу t. Тоді L — множина елементів, для яких $z_i(t)=1$, відповідно $N \setminus L$ — множина елементів, для яких $z_i(t)=0$.

У термінах введених позначень задачу оцінювання ризику реалізації КЗ сформулюємо таким чином: за наявності КЗ, заданих вектором $\vec{z}(t)$, необхідно оцінити їх сукупний ризик для СІС, заданої зваженим орієнтованим графом $G=(X,U)$, вершини якого характеризуються коефіцієнтом структурної уразливості V_i, а дуги — умовною ймовірністю $P_{i,j}$.

Будь-яка КЗ може спрямовуватися на окремі елементи СІС, групи елементів системи або всю систему в цілому (впливу піддаються всі елементи). «Охоплення» загрозою елементів СІС характеризуватиме ступінь напруженості ситуації, що склалася навколо системи і загрожує їй негативними наслідками, та безпосередньо впливатиме на рівень ризику СІС. Для врахування його значення при розрахунку ризику реалізації КЗ використаємо вектор $\vec{z}(t)=(z_1(t),z_2(t),...,z_n(t))$.

Крім наявного поля КЗ $\vec{z}(t)$, ризик визначатиметься величиною їх потенційного негативного впливу, яка також потребує вимірювання та оцінювання. Для цього застосуємо коефіцієнт структурної уразливості V_i, який відображає значущість i-го елемента для належного функціонування СІС загалом. Розрахунок V_i здійснюватимемо на підставі результатів імітаційного моделювання за таким виразом:

$$R_i=\frac{T_{sys}}{T_i}, \qquad (1)$$

де T_{sys} — час простою системи в результаті виведення з ладу її i-го елемента; T_i — час, на який виведено з ладу i-й елемент.

Однак коефіцієнт V_i має також враховувати множину специфічних параметрів *M*, якими прийнято вимірювати продуктивність X функціонування конкретної СІС. Тому у загальному випадку V_i є функцією від часу t і множини *M*:

$$R_i = f(t, m_1, m_2, ..., m_p),\ m_k \in M,\ k = \overline{1, p}. \quad (2)$$

Для прикладу розглянемо СІС, яка функціонує на базі IP-мережі.

Припустимо, що в момент часу t_1 виведено з ладу i-й комутуючий пристрій мережі, а в момент часу $t_1' > t_1$ зареєстровано зниження її загальної пропускної здатності $X(t) = X_0$ при $t \le t_1$ до $X(t) \le X_1$ при $t \ge t_1'$, де X_1 — критичне значення пропускної здатності, нижче якого мережа не забезпечує виконання СІС свого призначення (рис. 2).

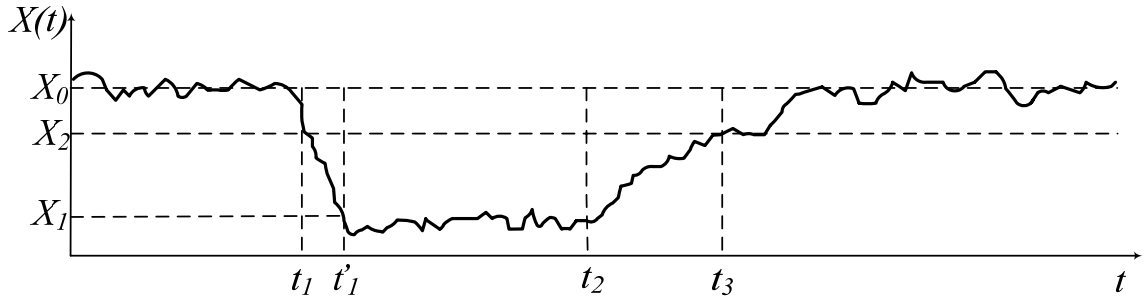

Рис. 2. До порядку розрахунку коефіцієнта структурної уразливості

Якщо в момент часу t_2 працездатність i-го комутуючого пристрою відновлено і відбувається зростання пропускної здатності до значення X_0: $X(t) \ge X_2$ при $t = t_3$ і $X(t) \to X_0$ при $t \ge t_3$, то можна стверджувати про відновлення працездатності всієї мережі після пошкодження її i-го елемента. Значення пропускної здатності $X(t) \ge X_2$ відображає спроможність мережі забезпечувати належне функціонування СІС.

Тоді коефіцієнт V_i розраховується як функція $f(t, X)$:

$$V_i = \frac{t_3 - t_1'}{t_1 - t_2}, \quad (3)$$

де t_1 — момент часу, з якого $X(t) \le X_1$; t_3 — момент часу, з якого $X(t) \ge X_2$.

На підставі отриманих значень V_i та заданого вектора КЗ $\vec{z}(t)$ визначимо ступінь ризику реалізації КЗ для СІС за виразом:

$$R' = \sum_{i=1}^{n} z_i(t) V_i. \quad (4)$$

Значення R' відображає інтегральну оцінку ризику для СІС як сукупність ризиків для окремих її елементів. Однак у складних системах у силу взаємозалежності їх складових має місце каскадний ефект поширення загрози [10], наслідки від якого можуть перевищувати шкоду від безпосереднього впливу на окремі елементи. Для врахування зазначеного ефекту скористаємося введеною характеристикою взаємозалежності елементів системи $P_{i,j}$. Тоді можливий ризик каскадного ефекту R'' від реалізації КЗ визначатиметься за формулою:

$$R'' = \sum_{j \in L} \sum_{i \in N \setminus L} P_{i,j} V_i,\ i \notin L. \quad (5)$$

При розрахунку умовної ймовірності $P_{i,j}$ до уваги беруться усі можливі маршрути поширення загрози, які являють собою набір послідовних і паралельних дуг. Тому для визначення $P_{i,j}$ слід дотримуватися таких правил:

- фрагмент графа, що складається з двох послідовних дуг $P_{i,k}$ і $P_{k,j}$, може бути замінено однією еквівалентною дугою, вага якої розраховується за теоремою множення ймовірностей:

$$P_{i,j} = P_{i,k} P_{k,j}; \quad (6)$$

- фрагмент графа, що складається з двох паралельних дуг $P_{i,j}'$ і $P_{i,j}''$, може бути замінено однією еквівалентною дугою, вага якої розраховується за теоремою додавання ймовірностей сумісних подій:

$$P_{i,j} = P_{i,j}' + P_{i,j}'' - P_{i,j}' P_{i,j}''. \quad (7)$$

Вирази (6) і (7) можуть бути поширені на будь-яку кількість послідовних чи паралельних дуг, що дозволяє розраховувати маршрути поширення КЗ довільної конфігурації. Врахування ризику каскадного ефекту поширення КЗ системою на підставі формули (5) дозволяє отримати інтегральну оцінку ризику для заданої СІС:

$$R = \sum_{i \in N} z_i(t) V_i + \sum_{i \in N} \sum_{i \in N \setminus L} P_{i,j} V_i . \qquad (8)$$

Для інтерпретації отриманого значення ризику слід визначити критерії, які характеризуватимуть ступінь такого ризику в лінгвістичному вираженні.

З цією метою виконаємо нормування R до максимально можливого рівня небезпеки $R_{\max}$, який характеризуватиметься наявністю загроз усім структурним елементам СІС ($z_i(t) = 1, \forall i \in N$):

$$R = \frac{R}{R_{\max}}, \quad R_{\max} = \sum_{i \in N} R_i . \qquad (9)$$

Нормоване значення може інтерпретуватися шляхом його порівняння з лінгвістичною шкалою оцінок, наведеною в табл. 1.

Таблиця 1

Лінгвістична шкала оцінок ризику реалізації КЗ

Значення нормованої інтегральної оцінки R_0 ризику реалізації КЗ	Лінгвістична категорія ризику реалізації КЗ
1–0,7	Високий
0,7–0,4	Середній
0,4–0,0	Низький

З урахуванням зазначеного оцінювання ризику реалізації КЗ пропонується здійснювати в такому порядку:

1. Побудова зваженого орієнтованого графа СІС.

1.1. Декомпозиція СІС на складові елементи та визначення коефіцієнтів структурної уразливості V_i для кожного з них за виразом (2).

1.2. Схематизація взаємозв'язків між елементами системи та визначення ступеня залежності між ними $P_{i,j}$ за результатами імітаційного моделювання.

2. Ідентифікація існуючих КЗ та представлення їх вектором загроз $\vec{z}(t) = (z_1(t), z_2(t), ..., z_n(t))$.

3. Розрахунок за виразом (4) величини ризику для СІС як сукупності ризиків для її елементів, що безпосередньо піддаються дії КЗ.

4. Розрахунок імовірності виведення з ладу елементів системи за усіма можливими маршрутами поширення КЗ за правилами (6) і (7).

5. Розрахунок величини ризику реалізації КЗ унаслідок виникнення каскадного ефекту поширення КЗ за виразом (5).

6. Отримання інтегральної оцінки ризику реалізації КЗ для СІС за виразом (8), його нормування за виразом (9) та інтерпретація за критеріями лінгвістичної шкали оцінок.

Розрахунковий приклад

Нехай задано умовну СІС, що складається з шести елементів $(x_1 ... x_6)$, поєднаних у структуру, яка наведена на рис. 3.

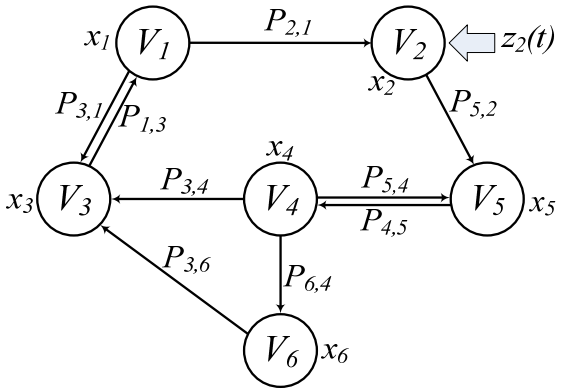

Рис. 3. Зважений орієнтований граф досліджуваної системи

Значення V_i вершин x_i та $P_{i,j}$ дуг (x_i, x_j) графа задано матрицею його зв'язності. При цьому на перетині i-го рядка і j-го стовпця вказано умовну ймовірність $P_{i,j}$ виведення з ладу i-го елемента системи в разі пошкодження її j-го елемента.

На перетині рядків і стовпців з однаковим номером розташовані коефіцієнти V_i відповідних елементів СІС. Відсутність взаємозв'язку між елементами системи позначається нульовими значеннями матриці (рис. 4).

На деякий момент часу $t = t_0$ виявлено загрозу 2-му елементу системи, тобто вектор КЗ має вигляд $\vec{z}(t_0) = (0,1,0,0,0,0)$. Тоді відповідно до запропонованого підходу $R' = z_2(t_0) V_2 = 0,4$.

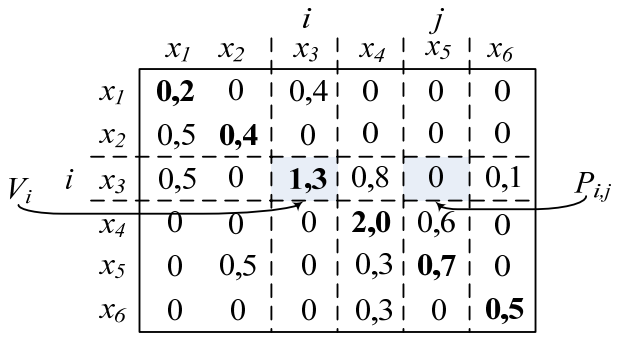

Рис. 4. Матриця суміжності графу досліджуваної системи

Згідно з п. 4 порядку оцінювання ризику визначимо всі можливі маршрути поширення виявленої КЗ та розрахуємо відповідні значення умовної ймовірності (табл. 2).

Ступінь ризику для СІС унаслідок виникнення каскадного ефекту поширення КЗ розрахуємо за виразом (5):

$$R'' = P_{1,2}V_1 + P_{3,2}V_3 + P_{4,2}V_4 + \\ + P_{5,2}V_5 + P_{6,2}V_6 = 1,34.$$

Відповідно інтегральна оцінка ризику реалізації КЗ для заданої СІС у ситуації, що склалася на момент часу $t = t_0$, згідно з виразом (8) становить

$$R = 0,4 + 1,34 = 1,73,$$

а її нормоване значення дорівнює $R = 0,26$, що за лінгвістичною шкалою оцінок відповідає низькому рівню ризику.

Таблиця 2

Розрахунок умовної ймовірності $P_{i,2}$

Номер вершини	Варіанти маршруту поширення КЗ	$P_{i,2}$	
		Для послідовних дуг	Для паралельних дуг
1	2→5→4→6→3→1	$P'_{1,2} = P_{5,2}P_{4,5}P_{6,4}P_{3,6}P_{1,3}$	$P_{1,2} = P'_{1,2} + P''_{1,2} - P'_{1,2}P''_{1,2}$
	2→5→4→3→1	$P''_{1,2} = P_{5,2}P_{4,5}P_{3,4}P_{1,3}$	
3	2→5→4→3	$P'_{3,2} = P_{5,2}P_{4,5}P_{3,4}$	$P_{3,2} = P'_{3,2} + P''_{3,2} - P'_{3,2}P''_{3,2}$
	2→5→4→6→3	$P''_{3,2} = P_{5,2}P_{4,5}P_{6,4}P_{3,6}$	
4	2→5→4	$P_{4,2} = P_{5,2}P_{4,5}$	
5	2→5	$P_{5,2}$	
6	2→5→4→6	$P_{6,2} = P_{5,2}P_{4,5}P_{6,4}$	

Висновки

Таким чином, набув подальшого розвитку підхід до оцінювання ризику реалізації КЗ для СІС за рахунок урахування структурної уразливості таких систем, який дозволяє: визначати значущість структурних елементів системи та взаємозв'язків між ними; моделювати поширення КЗ структурою складних систем; отримувати комплексну оцінку ризику для СІС з погляду їх структурної зв'язності.

На відміну від відомих, запропонований підхід як вхідні дані використовує результати імітаційного моделювання і не потребує обробки значних обсягів статистичних даних або врахування суб'єктивних оцінок експертів.

Наведені результати чисельного моделювання підтверджують його дієвість.

Разом з тим, розв'язання модельних прикладів показало, що обчислювальна складність оцінювання ризику значно зростає зі збільшенням кількості структурних елементів СІС. Тому подальші дослідження слід спрямувати в напрямку розробки алгоритмів зниження обчислювальної складності розрахунків.

ЛІТЕРАТУРА

1. *Большая* Советская Энциклопедия. — М. : СЭ, 1973. — Т. 12. — С. 214.

2. *Даник Ю. Г.* Визначення сутності та змісту кібернетичної загрози / Ю. Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць ЖВІ НАУ. — Житомир, 2012. — С. 5–14.

3. *Буйко К. В.* Подходы к оценке уровня промышленной безопасности в организациях, эксплуатирующих опасные производственные объекты / К. В. Буйко, Ю. В. Пантюхова // Безопасность труда в промышленности. — 2010. — № 10 — С. 42–46.

4. *Гаршин А. Ю.* Методика оценки уровня опасности морской критической инфраструктуры / А. Ю. Гаршин, О. В. Иванченко, Е. Н. Мащенко // Системи озброєння і військова техніка. — 2010. — № 3 (23) — С. 107–109.

5. *Нечунаев В. М.* Оценка рисков информационной безопасности корпоративной информационной системы / В. М. Нечунаев // Доклады ТУСУРа. — Томск, 2009.— № 1 (19). — Ч. 2. — С. 51–53.

6. *Корченко А. Г.* Анализ и определение понятия риска для его интерпретации в области информационной безопасности / А. Г. Корченко, Е. В. Иванченко, С. В. Казмирчук // Науково-технічний журнал «Захист інформації». — 2010. — №3. — С. 1–5.

7. *Cyber* Threat Metrics [Text]. Sandia Report / Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, Jason Frye. Sandia National Laboratories, Sandia Corporation. — Albuquerque. — 2012. — 39 p.

8. *Song Jae-Gu.* A cyber security risk assessment for the design of I&C systems in nuclear power plants /Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee, Kee-Choon Kwon, Dong-Young Lee // Nuclear Engineering And Technology. — 2012. — Vol. 44, No. 8. — P. 919–928.

9. *Hughes J. 2013.* Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity / J. Hughes, G. Cybenko // Technology Innovation Management Review. — 2013.— P. 15–24.

10. *Кондратьев А.* Современные тенденции в исследовании критической инфраструктуры в зарубежных странах / А. Кондратьев // Зарубежное военное обозрение. — 2012. — №1. — С. 19–30.

Стаття надійшла до редакції 23.01.2014