

*В.Б. Дудикевич, доктор технічних наук, Ю.Р. Гарасим
(Національний університет «Львівська політехніка», Україна)*

ОЦІНКА ЖИВУЧОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ З МІСТКОВОЮ ТА ПОСЛІДОВНО-ПАРАЛЕЛЬНОЮ СТРУКТУРОЮ

В статті здійснено оцінку живучості типових систем захисту інформації в корпоративних мережах зв'язку з містковою та послідовно-паралельною структурою. Оцінювання здійснювалось за допомогою логіко-ймовірнісних математичних моделей за станом системи, за результатами виконання завдання та моделі потокової оцінки живучості засобами імітаційного моделювання.

Для формальної оцінки живучості [1] систем захисту інформації (СЗІ) в корпоративних мережах зв'язку (КМЗ) [2] враховуються інтегральні багатофакторні (багатокритерійні) показники, що містять як кількісні, так і якісні характеристики: виживаність системи при n -кратному впливі дестабілізуючих факторів (ДФ), d -живучість, m -живучість, середня кількість впливів ДФ, що призводить до втрати працездатності СЗІ в КМЗ, середній запас живучості, умовна функція живучості, функція виживаності системи при n -кратному впливі ДФ, безумовна функція живучості, ймовірність ураження конкретного структурного елементу (СЕ), кількість СЕ, що залишилися після впливу ДФ [3]. На основі вищенаведених показників формується критерій $Surv = \{R(n), m, d, \dots\}$ для вибору оптимальної структури СЗІ в КМЗ за властивістю живучості в умовах невизначеності впливу ДФ [4].

Результати імітаційного моделювання оцінки живучості для двох типових структур СЗІ в КМЗ подані нижче [5-7]. Моделювання здійснювалося в програмному середовищі Mathcad 14.

Оцінка живучості за станом системи. Для СЗІ в КМЗ з містковою структурою (рис. 1) результати оцінки живучості $R(n)$ при $n \leq 5$ за станом системи наведено на рис. 2.

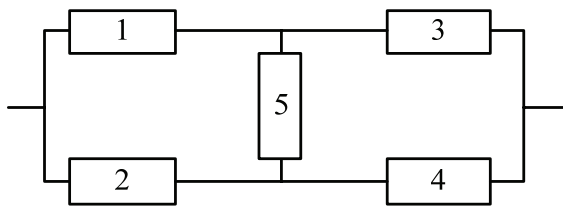


Рис. 1. Типова СЗІ в КМЗ з містковою структурою

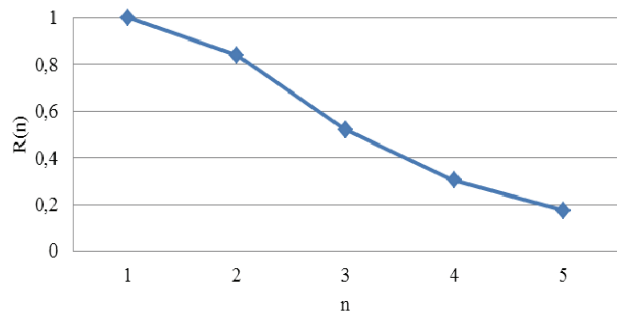


Рис. 2. Значення виживаності при n -кратному впливі ДФ для СЗІ в КМЗ з містковою структурою

Середній запас живучості $\bar{d} = 3.083$. Варто звернути увагу на те, що для даної структури $d = 2$, а $m = 3$. Відповідно, середній запас живучості більший за максимальну кількість СЕ, яка може бути видалена без втрати працездатності, більша за m -живучість. Цей ефект пояснимо тим, що деякі СЕ потрапляють в область впливу ДФ декілька разів.

Для СЗІ в КМЗ з послідовно-паралельною структурою (рис. 3) результати оцінки живучості за станом системи після n -кратного впливу ДФ наведено на рис. 4. Середній запас живучості $\bar{d} = 1.9524$. Це суттєво менше, ніж m -живучість (в цьому випадку $m = 4$).

Порівнюючи отримані результати оцінки живучості ($R(n)$) з випадком, коли уражені СЕ виключаються із області дії наступних ДФ при рівноймовірному ураженні працездатних СЕ, які залишилися ($R^*(n)$), бачимо, що $R(n)$ зменшується значно швидше, ніж в схемі неза-

лежних ДФ (при «пасивній стратегії»). Середня кількість ДФ, що призводить до втрати працездатності СЗІ в КМЗ – $\bar{\omega} = 2.547$. Це також менше, ніж в попередньому випадку.

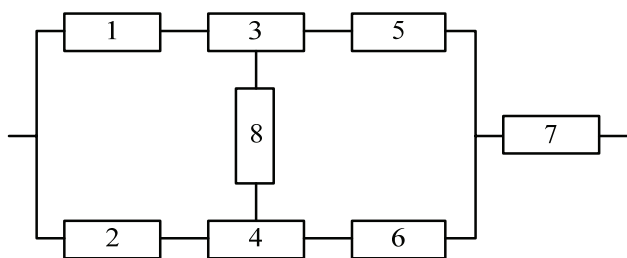


Рис. 3. Типова СЗІ в КМЗ з послідовно-паралельною структурою

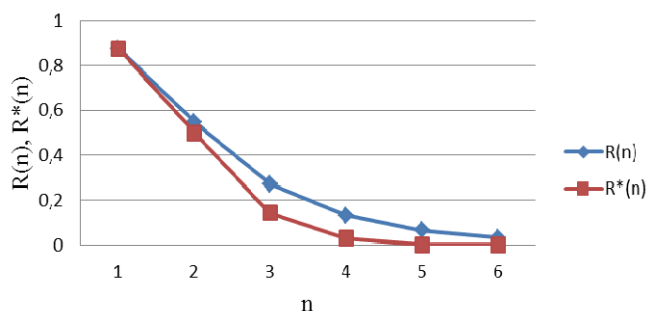


Рис. 4. Значення виживаності при n-кратному впливі ДФ для СЗІ з послідовно-паралельною структурою

Результати дослідження СЗІ в КМЗ із загальним структурним резервом з цілою кратністю (рис. 5) наведено на рис. 6, на якому показано зміну умовного закону вразливості $Q(n)$ із збільшенням кількості СЕ і кількості впливів ДФ.

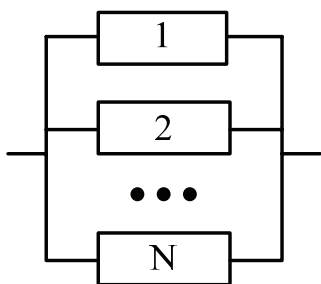


Рис. 5. Система СЗІ в КМЗ із загальним резервуванням з цілою кратністю

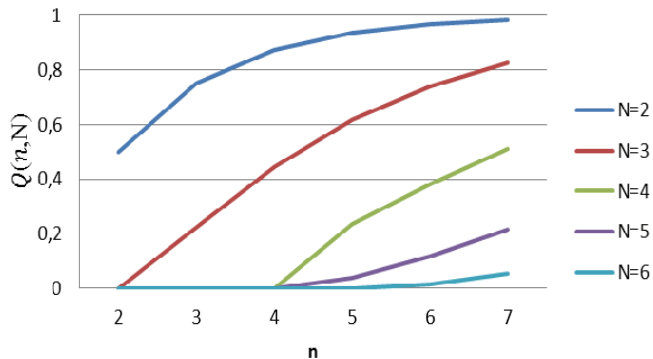


Рис. 6. Значення умовного закону вразливості при зміні кількості СЕ СЗІ в КМЗ і кількості ДФ

В цьому випадку при $n < N$ функція $Q(n) = 0$, оскільки для втрати працездатності СЗІ в КМЗ необхідно, щоб усі її СЕ були непрацездатні. При $n > N$ необхідно, щоб кожен СЕ попав в область впливу ДФ хоча б 1 раз. Кількість таких подій дорівнює кількості перестановок в n розрядах елементів N типів.

За результатами із рис. 6 видно, що при великій кількості резервних СЕ вразливість СЗІ в КМЗ є низькою навіть при надвеликій кількості впливу ДФ. Якщо кількість впливів ДФ дорівнює кількості СЕ, тоді вразливість СЗІ в КМЗ знижується відповідно до збільшення надлишковості досить помітно: більше ніж на порядок при збільшенні N від 2 до 5. Виживаність СЗІ в КМЗ не є дуже низькою, навіть якщо кількість впливів ДФ вдвічі перевищує кількість СЕ: 0.125 при $N = 2$ і 0.26 при $N = 3$. В окремому випадку, $\bar{\omega} = 3$ при $N = 2$, $\bar{\omega} = 5.5$ при $N = 3$. Середній запас живучості, відповідно, 2 і 4.5. Це суттєво більше, ніж m -живучість (в 2 і 2.25 рази).

Оцінка живучості за результатами виконання завдання. Для СЗІ в КМЗ з містковою структурою (рис. 1) результати оцінки живучості за результатами виконання завдання наведено на рис. 7. В цьому випадку можна зробити висновок, що показники живучості у всіх випадках менші, ніж показники безвідмовності. Необхідно зазначити і таку важливу властивість, що із збільшенням ймовірності виникнення відмов СЕ СЗІ в КМЗ q функція виживаності $G(t, n)$ зменшується, тобто відношення $G(t, n, q)/G(t, n, 0) < 1$ при всіх значеннях q та n , тобто малонадійна СЗІ в КМЗ більш вразлива при впливі ДФ, ніж високонадійна (рис. 8).

Причому, із збільшенням q функція виживаності зменшується швидше, ніж спадає ймовірність виконання завдання. Звідси можна також зробити висновок, що при одних і тих самих вимогах до властивості живучості і безвідмовності для забезпечення живучості вимагається більш високий рівень надлишковості.

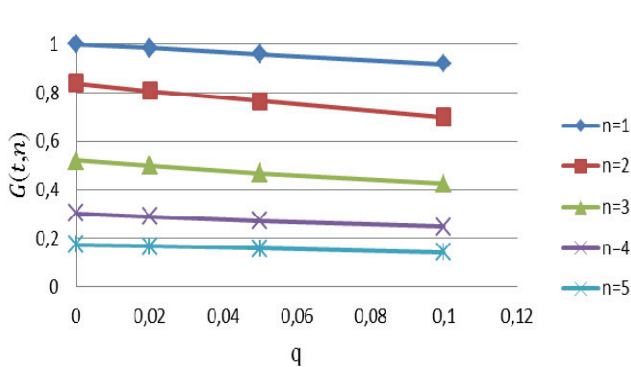


Рис. 7. Результати оцінки живучості СЗІ в КМЗ із містковою структурою за результатами виконання завдання

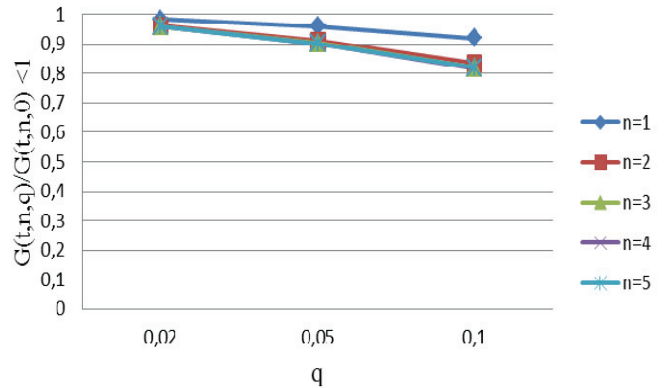


Рис. 8. Залежність функції виживаності СЗІ в КМЗ від ймовірності виникнення відмов СЕ

Для СЗІ в КМЗ з послідовно-паралельною структурою (рис. 3) результати оцінки живучості за результатами виконання завдання наведено на рис. 9.

Порівнюючи дані на рис. 8 і 10, бачимо, що у СЗІ в КМЗ, яка розглядається зниження живучості з погіршенням безвідмовності СЕ ще більш помітна, ніж у СЗІ в КМЗ з містковою структурою.

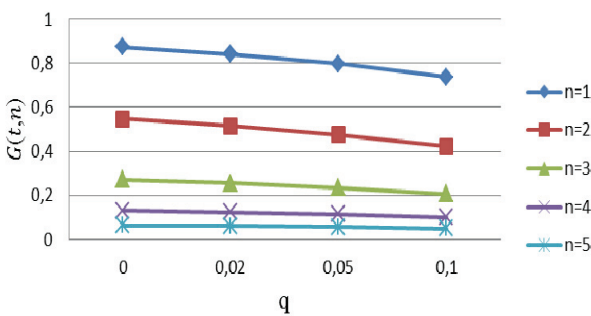


Рис. 9. Результати оцінки живучості СЗІ в КМЗ з послідовно-паралельною структурою за результатами виконання завдання

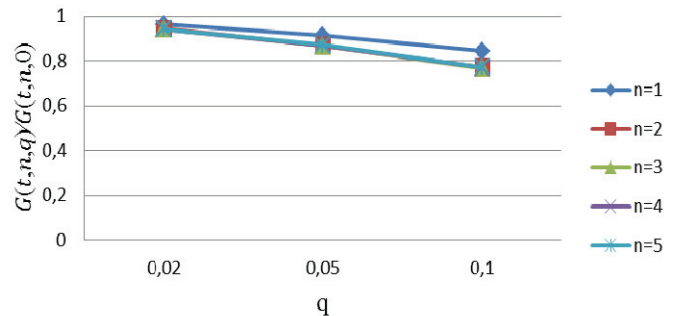


Рис. 10. Відносне зниження функції виживаності із зростанням ймовірності виникнення відмов СЕ СЗІ в КМЗ

Потокова модель оцінки живучості. Аналізуючи СЗІ в КМЗ, яка задана графом з великою кількістю вершин (що зумовлює актуальність та доцільність застосування саме потокової моделі оцінки живучості) так, щоб із вершини, яка обрана випадковим чином можна було встановити зв'язок після атаки зловмисника (впливу ДФ) з 90% ($\beta = 0.9$) неуражених вершин, вважаючи, що ребра графа невразливі, а вершини піддаються знищенню. Щільність атак складає 100 атак/хв. Ймовірність ураження конкретної вершини $\Delta/D = 0.05/1 = 0.05$, $k_s = 1$.

$$\beta = 1 - \exp\left\{-d \sum_{k=0}^{k_s-1} \frac{5^k}{k!} e^{-5\beta}\right\}; \quad d \sum_{k=0}^{k_s-1} \frac{5^k}{k!} \geq e^5 \frac{-\ln 0.1}{0.9} = 380.$$

Таким чином, граф, що містить 380 вершин може витримати одну атаку, після якої можна встановити зв'язок з 90% вершинами, які залишилися після атаки. Обчислимо кількість вершин, що залишилися:

$$\sum_{k=0}^{k_s-1} g_k^l(\eta) = e^{-0.05} \frac{0.05 \cdot 100}{1} = 0.034.$$

Таким чином, від початкових 380 вершин залишиться лише 3% – 12 вершин. Загальний потік знизиться більше ніж в 30 разів, система захисту інформації стане недопустимою, тобто СЗІ в КМЗ буде знищена.

Висновки

Отримала подальший розвиток математична модель оцінки живучості СЗІ в КМЗ за станом системи, що дає можливість оцінити виживаність системи при n -кратному впливі ДФ та використовувати точкову, статичну модель системи без врахування стійкості СЕ і вторинних наслідків після впливу ДФ. Результати дослідження математичної моделі показали що при великій кількості резервних СЕ вразливість СЗІ в КМЗ є низькою навіть при надвеликій кількості впливів ДФ.

Отримала подальший розвиток математична модель оцінки живучості СЗІ в КМЗ за результатами виконання завдання, що дає можливість виявити усі працездатні структури системи після n -кратного впливу ДФ, а також використовувати точкову, статичну модель системи без врахування стійкості елементів і вторинних наслідків після впливу ДФ. Дослідження математичної моделі показало, що в СЗІ в КМЗ зниження властивості живучості з погіршенням безвідмовності елементів є більшим, ніж в системі з містковою структурою.

Отримала подальший розвиток математична модель потокової оцінки живучості СЗІ, яку доцільно використовувати для розподілених КМЗ, що вирішує проблему перерозподілу потоків після впливу ДФ. Дослідження моделі потокової оцінки живучості дозволило визначити можливість (кількісно) встановлення зв'язку між СЕ СЗІ в КМЗ при однократному впливі ДФ, а також визначити кількість СЕ, які залишаться після впливу ДФ.

Список літератури

1. Дудикевич В. Б. Системи захисту інформації, що мають властивість живучості. Основні поняття / В. Б. Дудикевич, Ю. Р. Гарасим // Науково-технічний журнал «Сучасний захист інформації», спеціальний випуск. – 2010. – № 4. – С. 6-13.
2. Дудикевич В. Б. Стійкість та живучість систем захисту інформації в корпоративних мережах зв'язку / В. Б. Дудикевич, Ю. Р. Гарасим // Матеріали Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія». – Вінниця, 2010. – С. 193-194.
3. Dudykevych V. Survivable security Systems Analysis / V. Dudykevych, I. Garasym // Computer science and information technologies: Materials of the VIth International scientific and technical conference CSIT 2010. – Lviv : Publishing House Vezha&Co, 2010. – pp. 108-110.
4. Гарасим Ю. Р. Метод вибору варіанту системи захисту інформації за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів / Ю. Р. Гарасим // Збірник тез міжнародної наукової конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні аспекти кібернетики». – Київ, 2011. – С. 74-76.
5. Гарасим Ю. Розробка моделі оцінки живучості для систем захисту інформації / Ю. Гарасим // Комп'ютерні науки та інженерія: Матеріали IV Міжнародної конференції молодих вчених CSE-2010. – Львів : Видавництво Львівської політехніки, 2010. – С. 320-321.
6. Garasym I. Information security system survivability assessment method based on logical-probabilistic models / I. Garasym // Proceedings of the XIth International Conference CADSM 2011. – Polyana, Svalyava (Zakarpattya), Ukraine, 2011. – pp. 160-161.
7. Дудикевич В. Б. Моделі оцінки живучості систем захисту інформації / В. Б. Дудикевич, Ю. Р. Гарасим // «Обчислювальні методи і системи перетворення інформації»: зб. праць наук. техн. конф., Львів, 7-8 жовтня 2010 р. – Львів : ФМІ НАНУ, 2010. – С. 104-107.