УДК 004.056, 004.75

В.Б. Дудикевич, Ю.Р. Гарасим
Національний університет "Львівська політехніка",
кафедра захисту інформації

ДОСЛІДЖЕННЯ ТА ВДОСКОНАЛЕННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ ОЦІНЮВАННЯ ЖИВУЧОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

Адаптовано методику оцінювання живучості на основі логіко-ймовірнісних моделей до системи захисту інформації корпоративної мережі зв'язку для визначення поведінки елементів і системи захисту загалом після впливу на неї дестабілізуючих факторів, вдосконалено та досліджено математичні моделі оцінювання живучості на основі логіко-ймовірнісних та потокової моделей.

Ключові слова: властивість живучості, оцінювання живучості, системи захисту інформації.

Survivability assessment method based on logical probabilistic models was adapted to enterprise communication network information security system for determining the behavior of the elements and security system in general after the destabilizing factors influence; survivability assessment mathematical models based on logical probabilistic and logic-flow models were improved and researched.

Key words: survivability, survivability assessment, information security system.

Вступ. Зважаючи на високу складність і комплексний характер проблеми аналізу та оцінювання живучості систем захисту інформації (СЗІ) корпоративних мереж зв'язку (КМЗ), логічно припустити, що оцінити ці показники лише на основі одного якого-небудь параметра доволі важко. Тому автори пропонують враховувати інтегральні багатофакторні (багатокритерійні) показники, що містять як кількісні, так і якісні характеристики, які можна використовувати для формального оцінювання її живучості.

1. Постановка завдання оцінювання живучості системи захисту інформації корпоративної мережі зв'язку. У загальному випадку постановка проблеми аналізу факторів властивості живучості [1–4] систем захисту КМЗ пов'язана з оцінюванням показників якості її функціонування (ПЯФ), яку необхідно здійснювати або протягом всього життєвого циклу цієї системи, або на достатньо тривалому відрізку цього циклу, найчастіше, – у фазі контрольованої деградації об'єкта дослідження. Визначимо якість функціонування СЗІ КМЗ множиною показників (факторів) $Q = \{q_1,...,q_2\}$, які знаходяться в межах встановлених значень експлуатаційних характеристик. Переважно ці значення задають в технічних вимогах (ТВ), що формулюють в технічному завданні (ТЗ) на цю систему. Введемо обмеження

$$q_j \geq q_j{}^{TB} \text{ або } q_j \leq q_j{}^{TB}, j = \overline{1,S}, \quad (1)$$

які формалізують умови відповідності ПЯФ цього об'єкта (СЗІ ЗКМЗ), що визначені у ТЗ технічним вимогам. У цьому випадку параметри $q_j{}^{TB}, j = \overline{1,S}$ є гранично допустимі значення відповідних ПЯФ системи. У найпростішій формі проблему забезпечення живучості сформулюємо

у вигляді задачі мінімізації вартості затрат, які необхідні для підтримки функціональних ПЯФ системи на необхідному рівні протягом заданого періоду часу, тобто у вигляді:

$$C = \sum_{i=1}^{\Omega} \sum_{j=1}^{S} c_{ij}(\Delta t_i) \to \min_{[0,T]}, \tag{2}$$

$$q_j^{\,*}(\Delta t_i) \geq q_j^{\,TB}, j = \overline{1,l} \text{ або } q_j^{\,*}(\Delta t_i) \leq q_j^{\,TB}, j = \overline{l+1,S}, \tag{3}$$

$T_{ПЛ} = \sum_{i=1}^{\Omega} \Delta t_i$, де $c_{ij}(\Delta t_i)$ – поточні експлуатаційні затрати на календарно-плановому відрізку $\Delta t_i \in [0, T_{ПЛ}], i = \overline{1,\Omega}$, при яких забезпечують рівень якості функціонування за j-м ПЯФ, що задовольняє ТВ; $q_j^{\,*}(\Delta t_i)$ – «найгірше» в розумінні виконання технічних вимог значення j-го ПЯФ на відрізку Δt_i. Зазначимо, що постановка завдання забезпечення живучості у вигляді (2), (3) справедлива в основному для сепарабельних функцій c_{ij}, коли вкладення в деякий тип ресурсу, що здійснюють для поліпшення одного з показників якості q_j, не впливають на інші ПЯФ, а також за умови адитивності інтегральної функції вартості C. Необхідно зазначити, що надійність і відмовостійкість – це показники поточні, ситуаційні, оперативні. А функціональна живучість – показник агрегований, довгостроковий, який характеризує зміну можливостей системи, яку досліджують протягом доволі тривалого часового відрізка (періоду деградації). Тому відповідні затрати, що спрямовані на забезпечення живучості СЗІ КМЗ, необхідно здійснювати рівномірно протягом всього планового періоду експлуатації, хоча на практиці цього не завжди дотримуються.

Кількісне оцінювання живучості СЗІ КМЗ з врахуванням її можливостей протистояти функціональній деградації здійснюватимемо на основі конкретних метрик, що характеризують втрату функціональності протягом деякого тимчасового періоду. При цьому можливими є різні методичні підходи до обчислення цих метрик, наприклад, через кількісне оцінювання відносної здатності системи до виконання критично важливих і відповідальних завдань, з врахуванням втрати нею частини початкових можливостей внаслідок деградації [2].

2. Показники властивості живучості систем захисту інформації. Сьогодні в різних роботах [5–10] запропоновано багато різних показників живучості. Серед них є як ймовірнісні, так і детерміновані. Функціональну живучість СЗІ КМЗ визначатимемо за допомогою оцінювання її ПЯФ в умовах виникнення відмов у процесі експлуатації протягом всього життєвого циклу (ЖЦ). У такій постановці завдання якість виконання системою своїх апріорно заданих функцій оцінюватимемо за такими основними характеристиками: відповідність СЗІ КМЗ її цілям та завданням; показники продуктивності системи і окремих її функціональних елементів; функціональна готовність додатків і даних, яка пов'язана з показниками відгуку (часом реакції системи); якість обслуговування користувачів та додатків (QoS);

При проектуванні СЗІ КМЗ, які мають необхідний високий рівень функціональної живучості, спочатку слід визначити відповідні критерії для оцінювання різних системних якостей. Слід зазначити, що саме властивість живучості можна розглядати як найбільш об'єктивний і адекватний показник, що дає змогу оцінити всі аспекти структурно-функціональної надійності КМЗ, що знаходиться в постійно змінному зовнішньому середовищі і піддається перманентним модернізаціям з метою покращення ПЯФ. Дійсно, при дослідженні властивості живучості акцент здійснюватимемо не на одиничні збої і відмови, що викликають тимчасову непрацездатність системи, а на її здатність виконувати свої функції протягом тривалого періоду часу, бажано – протягом усього ЖЦ СЗІ КМЗ [5, 11]

Для оцінки живучості СЗІ КМЗ використаємо показники, які використовують під час оцінювання живучості складних систем (СС) за станом системи, що запропоновані в [12, 13]. Позначимо через A_n подію, що полягає в n-кратній появі дестабілізуючих факторів (ДФ), а через

F – функцію працездатності системи, яка набуває значення 1, якщо система працездатна, і – 0, якщо непрацездатна. Тоді умовний закон вразливості

$$Q(n) = P(F = 0/A_n), \tag{4}$$

якщо ймовірність втрати працездатності системи за умови n-кратного ДФ.

Виживаність системи при n-кратному ДФ

$$R_n = 1 - Q(n) = P(F = 1/A_n). \tag{5}$$

Запас живучості (d-живучість)

$$d = C - 1 \tag{6}$$

є критичною кількістю дефектів, зменшеною на одиницю. Дефект – це одиниця вимірювання збитку, який наносять системі ДФ. Це може бути один елемент, який видалений із системи в результаті ДФ, визначена номінальна захищеність чи конфіденційність в системі захисту, яка втрачається для абонентів внаслідок впливу ДФ тощо. Критичною називають мінімальну кількість дефектів, поява яких призводить до втрати працездатності.

Запас живучості (m-живучість)

$$m = \max_i m_i \tag{7}$$

є максимальною кількістю дефектів, яку ще може витримати система без втрати працездатності.

Середня кількість ДФ, що призводить до втрати працездатності

$$\overline{\omega} = \sum_{n=0}^{\infty} R(n) \tag{8}$$

є математичним сподіванням кількості ДФ, яке задається розподілом (4).

Середній запас живучості

$$\overline{d} = \overline{\omega} - 1. \tag{9}$$

Ця величина невід'ємна, оскільки $\overline{\omega} \geq 1$. Це випливає із (8), оскільки $R(0) = 1$. Показники (4), (5), (8) та (9) є ймовірнісними, (6) і (7) – детерміновані. До детермінованих показників відносять показник K_s^A, який запропонований в [14]. Нехай деяка система складається із n_s об'єктів, S – номер варіанта системи. При однократному дестабілізуючому впливі на i-й об'єкт виникає збиток величиною C_i^s. Об'єкти нумеруємо для кожного варіанта в порядку зменшення збитку $C_1^s > C_2^s > ... > C_{n_s}^s$. Встановимо порогове допустиме значення збитку A і припустимо, що при багатократному впливі ДФ піддаються різні об'єкти і в першу чергу об'єкти з найбільшим збитком. Причому збиток для системи загалом отримуємо додаванням збитків на окремих об'єктах. Тоді K_s^A визначаємо за формулою $K_s^A = \min(C_s \geq A)K_s, C_s = \sum_{i=1}^{K_s} C_i^s$, де K_s – кількість втрачених елементів у результаті ДФ в структурі S.

Нехай тепер система, яка має базову структуру S_0, виконує деяке завдання протягом часу t. У результаті ДФ в системі може виникнути нова структура S_i із множини працездатних структур $S^{П} = \{S_i, i = 1,..., N_p\}$ або непрацездатних структур $S^{НП} = \{S_i, i = N_p + 1,..., N\}$. Після n-кратного ДФ система з новою структурою повинна приступити до виконання встановленого завдання і виконати його за час t. Оцінюємо живучість за результатами виконання завдання за допомогою наступних показників.

Умовна функція живучості

$$G(t/S_i) = G_i(t) = P(t/S_i)/P(t/S_0) \tag{10}$$

є відношенням ймовірностей виконання завдання системою, які визначені для двох випадків: для базової та нової структури. При цьому не виключаємо, що для нової структури S_i завдання буде сформульоване по-іншому, ніж для S_0. Але при цьому повинна виконуватися умова $G_i(t) < 1$. За

наявності відновлення розглядатимемо і непрацездатні структури ($i > N_{П}$), оскільки і для них може бути $P(t/S_i) > 0$. За відсутності відновлення $P(t/S_i) = 0$ при $i > N_{П}$.

Функція виживаності системи при n-кратному впливі (подія A_n):

$$G(t/A_n) = G(t,n) = \sum_{k=1}^{N} P_n(k) G_k(t) \tag{11}$$

є усереднена за всіма можливими структурами функція живучості, $P_n(k)$ – ймовірність виникнення структури S_k після n-кратного впливу ДФ.

Безумовна функція живучості

$$G(t) = \sum_{n=1}^{\infty} P(A_n) G(t/A_n) = \sum_{k=1}^{N} P(S_k) G_k(t) \tag{12}$$

є усереднена за всіма можливими подіями A_n функція виживаності системи. Ймовірність $P(S_k)$ в формулі (12) визначаємо за формулою

$$P(S_k) = \sum_{n=1}^{\infty} P(A_n) P_n(k). \tag{13}$$

Показники (11) та (12) належать до класу адитивних і забезпечують згортку векторного показника $\{G_k(t), k = 1,...,N\}$ в скалярний. За відсутності точної інформації про ймовірності $P_n(k)$ і $P(S_k)$ їх замінюємо на вагові коефіцієнти a_k і β_k, які визначаємо експертним методом. Але, якщо і це здійснити складно – переходимо до мінімаксних показників.

Послідовність $G(t,n)$ є спадною функцією n і змінюється від 1 при $n = 0$ до 0 при $n \to \infty$. Тому середню кількість ДФ, яка призводить до невиконання завдання, визначаємо за формулою

$$\overline{\omega}(t) = \sum_{n=1}^{\infty} n\big(G(t,n-1) - G(t,n)\big) = \sum_{n=1}^{\infty} G(t,n). \tag{14}$$

При $t = 0$ або $\lambda_i = 0$ (елементи ідеально надійні) формули (11) і (14) переходять відповідно в (5) і (8). Насправді, при $t = 0$ функція $G_k(0) = 1$ для $k \le N_{П}$ і $G_k(0) = 1$ для $k > N_{П}$. Із (11) маємо $G(0/A_n) = \sum_{k=1}^{N_{П}} P_n(k) = R(n)$, а із (12) $G(0) = R = \sum_{n=1}^{\infty} P(A_n) R(n)$. Показники (10)–(14) можна узагальнити і на випадок розгалужених та багатополюсних структур. Для цього в (10) ймовірність виконання завдання замінюємо на деякий показник якості $E(S)$. Так, для системи з розгалуженою структурою функціонування в інтервалі часу t подамо функціоналом $E(t,S) = \varphi\big(P(t/S)\big)$, де $P(t/S) = \{P_m(t/S), m = 0,...,M\}$ розподіл кількості непрацездатних розгалужень у момент часу t за умови, що в початковий момент система мала структуру S. Тоді умовну функцію живучості визначаємо за формулою

$$G_i(t) = G(t/S_i) = E(t,S_i)/E(t,S_0). \tag{15}$$

При $M = 1$ отримаємо $E(t/S) = P(t/S)$, і формула (15) переходить в (10). Інші показники знаходимо за формулами (11)–(14). З метою аналізу властивості живучості та оцінювання рівня деградації СЗІ КМЗ пропонуємо використовувати інтегральний показник функціональної живучості Φ, який визначатимемо через середньозважену суму оцінок ПЯФ у такому вигляді: $\Phi = 1/S \sum_{j=1}^{S} z_j(k)$, де значення нормованих показників $z_j(k), j = \overline{1,S}$ обчислюємо як $z_j(k) = a_j \left(q_j{}^{*}(k) - q_j{}^{TB} \big/ q_j{}^{TB}\right)$, $j = \overline{1,l}$ для ТВ вигляду $q_j \ge q_j{}^{TB}$ або $z_j(k) = a_j \left(q_j{}^{TB} - q_j{}^{*}(k) \big/ q_j{}^{TB}\right)$, $j = \overline{l+1,S}$ для ТВ вигляду $q_j \le q_j{}^{TB}$

У цьому випадку a_j – ваговий коефіцієнт, що характеризує рівень значущості j-го ПЯФ для інтегрального оцінювання якості функціонування системи загалом; k – кількість накопичених відмов у системі за розглянутий період часу (зокрема з врахуванням відновлень). Очевидно, що якщо для всіх заданих ПЯФ у розглянутий період часу виконуються вимоги ТВ виду (1), то $\min_j z_j(k) \ge 0, j = \overline{1,S}$ і, отже, значення запропонованого інтегрального показника Φ буде не

нижчим за деяку критично нижню межу ПЯФ. Її конкретне значення задаватимемо спочатку при визначенні функціональних можливостей системи на певний період експлуатації, також як і початкове значення інтегрального показника Φ.

3. Математична модель оцінювання живучості системи захисту інформації за станом системи. Нехай існує двополюсна система захисту із N точкових елементів з довільними з'єднаннями між ними і функцією працездатності $F = f(X), X = \{x_1, x_2, ..., x_N\}$. Система піддається впливу потоку незалежних точкових ДФ з рівноймовірним ураженням кожного функціонального елемента СЗІ КМЗ при появі ДФ, тобто $\varphi_{kj} = 1/N, j = 1,...,N$. Вважатимемо також, що стійкість елементів дорівнює 0, а інтенсивність ДФ достатня для того, щоб гарантувати перехід у непрацездатний стан елемента, який потрапив в область дії ДФ. Оцінюєма живучість за показниками (5)–(9).

Виживаність системи при n-кратному ДФ подаємо у вигляді

$$R(n) = \sum\nolimits_{X \in X_1} P(X/A_n) = P(F = 1/A_n), \tag{16}$$

де X_1 – підмножина векторів X, що відповідають працездатним станам системи. Ймовірність $P(X/A_n)$ знаходимо за формулою:

$$P(X/A_n) = \sum\nolimits_{\bar{n} \in M_n} P(\bar{n}) P(X/\bar{n}), \tag{17}$$

де $\bar{n} = (n_1, n_2, ..., n_k)$ – вектор кількості ДФ, що належать k підсистемам, M_n – множина векторів, що задовольняють умову $n_1 + n_2 + ... + n_k = n$. Ймовірність

$$P(\bar{n}) = \left(n!/n_1!n_2!...n_k!\right) \cdot \gamma_1^{n_1} \gamma_2^{n_2} ... \gamma_k^{n_k}, \tag{18}$$

де γ_i – ймовірність того, що i-та підсистема входить в область дії ДФ. В окремих випадках тут може бути $k = N$.

При рівноймовірному ураженні елементів формули (16)–(18) можна уточнити, представивши функцію працездатності у вигляді ортогональної диз'юнктивної нормальної (ОДНФ) форми $F = \bigcup_{i=1}^{m} Q_i$. Запишемо (16) у вигляді

$$R(n) = \sum\nolimits_{i=1}^{m} P(Q_i = 1/A_n). \tag{19}$$

Для імплікант, які містять $l_i = 0, 1, 2$ заперечення, запишемо формули в (19) у явному вигляді:

$$P(Q_i = 1/A_n) = (1 - s_i/N)^n, l_1 = 0, n \geq 1, \tag{20}$$

$$P(Q_i = 1/A_n) = \sum_{j=1}^{n} C_n^j (1 - s_i/N)^{n-j} \Big/ N^j, l_i = 1, n \geq 1, \qquad P(Q_i = 1/A_n) = \sum_{k=2}^{n} \sum_{j=1}^{k-1} C_n^j (1 - s_i/N)^{n-k} \Big/ N^{-n},$$

$l_i = 2, n \geq 2$, де s_i – кількість букв в імпліканті Q_i. Ці формули є окремим випадком (18) при $k = 2$ та різних значеннях n_1 і n_2. Для випадку рівноймовірного потрапляння елементів в область впливу ДФ можливий інший спосіб обчислення виживаності системи при n-кратному впливі. За базовою структурою S_0 визначаємо всі можливі працездатні структури $S_i, i = 1,..., N_p$. Тоді: $R(n) = \sum_{j=1}^{N_p} r_j(n) \Big/ N^n = r_n \Big/ N^n$, де $r_j(n)$ – кількість випадків, в яких виникає структура S_i при n-кратному ДФ. Цю кількість визначаємо за формулою $r_j(n) = \sum_{(k)} L_{nk} B_{kj}$, де L_{nk} – кількість перестановок із n елементів k типів, B_{kj} – кількість різних векторів X з k нулями, які приводять до структури S_i. Оскільки параметри d та m із формул (6) і (7) зазвичай невеликі, не складно знайти B_{kj} простим перебором векторів. Максимальна кількість векторів для дослідження

дорівнює mN, а практично вона значно менша. Числа L_{nk} – так звані числа Моргана. Вони пов'язані з числами Стірлінга другого роду співвідношенням

$$L_{nk} = k!S_{nk}, \tag{21}$$

де S_{nk} знаходять за допомогою рекурентного відношення $S_{nk} = S_{n-1,k-1} + kS_{n-1,k}; S_{nk} = S_{nk} = 0$ при $n < k; S_{nn} = 1$, але числа L_{nk} можна обчислити й безпосередньо за формулою: $L_{nk} = \sum_{i=1}^{k} C_k^i i^n (-1)^{k+i}$.

4. Математична модель оцінювання живучості системи захисту інформації за результатами виконання завдання. Нехай система з двополюсною структурою виконує завдання в інтервалі часу $(0,t)$. Для виконання цільової функції, яка поставлена СЗІ КМЗ, кожен її функціональний елемент повинен функціонувати відповідно до встановленого графіка і забезпечувати виконання протягом часу t заданого набору функцій. Ймовірність того, що i-й елемент виконує свою частину загального завдання, дорівнює $p_i(t)$. Зокрема, ця ймовірність може збігатися з ймовірністю безвідмовної роботи, функцією готовності, коефіцієнтом готовності, коефіцієнтом оперативної готовності. Але в загальному випадку $p_i(t)$ може бути ймовірністю виконання завдання із складним режимом роботи і складними обмеженнями на вид траєкторії функціонування. Під час оцінювання живучості вважатимемо, що усі ДФ завершилися на початок даного інтервалу часу $(0,t)$ і в початковий момент система приступає до виконання завдання, маючи одну з можливих працездатних структур. Припускаємо також, що процеси відновлення в системі спрямовані на підтримку працездатності структури, що збереглася, і не зачіпають елементи, що потрапили раніше в зону впливу ДФ. Це припущення не є примусовим і його можна зняти, якщо зберігається умова незалежності процесів функціонування елементів.

Оцінювання живучості СЗІ КМЗ здійснимо в такій послідовності. Після запису ФПЗ для базової структури визначаємо усі інші працездатні структури шляхом підстановки у ФПЗ векторів, в яких одна, потім дві, три і більше букв замінені нулями. Якщо при підстановці логічна функція не тотожно дорівнює нулю, тоді вона відповідає одній з працездатних структур. Максимальну кількість нулів, що вводиться у вектор при випробуваннях, визначаємо показником m-живучості. Одночасно при таких випробуваннях визначаємо коефіцієнти B_{kj}. Множенням на матрицю L знаходимо матрицю коефіцієнтів r_{ni}. Відношення r_{ni} / N^n гарантує ймовірність $P_n(i)$ того, що після n-кратного ДФ виникне структура $S_i, i = 1,..., N_p$. Для кожної із структур складаємо функцію працездатності і приводимо до форми переходу до часткового заміщення:

$$F^{(i)}(X) = x_n \left(V_{j=1}^{l} x_j f_j^{f^{(i)}(X)} \right), \tag{22}$$

де x_n – змінна, яка відповідає полюсу системи, x_j – неповторні елементи, $f^{(i)}(X)$ – функції алгебри логіки будь-якого виду. Від функції (22) переходимо до змішаної форми типу: $P\left(F^{(i)}(X) = 1\right) = p_n \left(1 - \prod_{j=1}^{l} q_j f^{(i)}(X)\right)$, де $p_n = P(x_n = 1), q_i = 1 - p_j = P(x_j = 0)$. Далі здійснюємо послідовне багатокрокове заміщення решти логічних змінних і отримуємо функції $P(t/S_i)$. Тоді визначаємо $G_i(t)$ і $G(t,n)$. Якщо вдається встановити ймовірність $P(A_n)$, тоді знаходимо і безумовну функцію живучості.

5. Математична модель потокового оцінювання живучості системи захисту інформації. Потокова мережева інформаційна система [9] слугує математичною моделлю реальних розподілених СЗІ КМЗ, що поєднують безліч вузлів (структурних елементів (СЕ)). Для СЗІ КМЗ такого типу важливим є вирішення таких завдань, які пов'язані з прийняттям рішень щодо використання наявних

мережевих ресурсів, їх розподілом між СЕ, тобто з аналізом можливостей покращення роботи СЗІ КМЗ за рахунок раціонального перерозподілу інформаційних потоків. В умовах дефіциту ресурсів СЗІ КМЗ (у випадку успішної реалізації атаки зловмисниками) виникає погіршення якості зв'язку, яке полягає у відмовах в обслуговуванні, системних втратах, часових затримках, зниженні захищеності, конфіденційності, доступності, спостережуваності системи тощо.

Подамо СЗІ КМЗ у вигляді однорідних симетричних структур, де граф має форму решітки, в якій кожна вершина з'єднана з найближчими сусідніми. Вимоги користувачів до пропускної здатності ребер фізичного графу СЗІ КМЗ вважаємо відомими, проте це припущення не виконується при пошкодженні СЗІ КМЗ, тобто виникає проблема вибору оптимального розподілу потоків у випадку недопустимості СЗІ КМЗ. Тоді доводиться шукати рішення, яке використовує всі ресурси СЗІ КМЗ, поки вони можуть бути використані хоча б однією парою вузлів. Схожий розподіл потоків, який максимально забезпечує вимоги всіх тяжіючих пар, називатимемо нормативним. Він є таким розв'язком задачі розподілу потоків в СЗІ КМЗ, що не дає можливості одним тяжіючим парам покращити забезпеченість своїх вимог за рахунок інших, менш забезпечених, і крім того, використовує всі способи збільшення забезпеченості вимог тяжіючих пар за рахунок ресурсів СЗІ КМЗ. Критерій допустимості потокової СЗІ КМЗ задамо умовою $\Theta_0 \geq 0$, яке гарантує існування допустимого розподілу потоків, такого, що відповідний вектор мультипотоку буде не меншим за вектор заданих вимог.

У випадку неприпустимості СЗІ КМЗ $\Theta_0 < 0$ виникає складна проблема перерозподілу потоків у СЗІ КМЗ (оскільки розподілені СЗІ КМЗ завжди мають «вузькі місця» – ребра фізичного графу СЗІ КМЗ, пропускна здатність яких не дозволяє збільшувати потік вище певного значення), різних для різних тяжіючих пар. Нормативно розподілений потік дає змогу здійснити розподіл відповідно до рівня забезпеченості різних тяжіючих пар оптимальним чином.

Систему захисту інформації КМЗ у вигляді $S = (V, R, P)$ задамо множинами $V = \{v_1, v_2, ..., v_n\}$ – вузлів СЗІ КМЗ, $R = \{r_1, r_2, ..., r_e\} \subset V \times V$ – ребер фізичного графу СЗІ КМЗ G та $P = \{p_1, p_2, ..., p_m\} \subset V \times V$ – тяжіючих пар або ребер логічного графу СЗІ КМЗ $\overline{G}$. Наявні індекси множини позначимо: $N = \{1, ..., n\}$, $E = \{1, ..., e\}$, $M = \{1, ..., m\}$. Тоді $V = \{v_j\}_{j \in N}$, $R = \{r_k\}_{k \in E}$, $P = \{v_i\}_{i \in M}$. Нехай усі ребра не є орієнтовані, прямим напрямом потоку вважатимемо напрям від вершини з меншим номером до вершини з більшим. Кожне ребро r_k фізичного графу СЗІ КМЗ G будемо представляти орієнтованими дугами з номерами k та $k + l$ для прямого і зворотного напрямів. Для будь-якої вершини $v \in V$ позначимо через $S(v)$ множину індексів вихідних із неї дуг, а через $T(v)$ – множину індексів вхідних. Для кожної i-ї тяжіючої пари введемо позначення $p_i = (v_{s_i}, v_{t_i})$, де $s_i < t_i$ і вершину v_{s_i} називатимемо джерелом, а v_{t_i} – стоком i-го виду продукту. У випадку орієнтованого ребра логічного графу вершини джерело/стік визначаємо відповідно до орієнтування. Наведену структуру СЗІ КМЗ подамо за допомогою матриці інцидентності «дуги – вершини» фізичного графу СЗІ КМЗ G: $A = \{a_{k,j}\}$ розміром $(2e \times n)$ і матриці зв'язків логічного графу СЗІ КМЗ $\overline{G}$ $B = \{b_{i,j}\}$ розміром $(m \times n)$:

$$a_{k,j} = \begin{cases} 1, \textit{ якщо } k \in S(v_j); \\ -1, \textit{ якщо } k \in T(v_j); \\ 0, \textit{ в інших випадках}, \end{cases} \qquad b_{i,j} = \begin{cases} 1, \textit{ якщо } v_j = v_{s_i}; \\ -1, \textit{ якщо } v_j = v_{t_i}; \\ 0, \textit{ в інших випадках}. \end{cases}$$

Тобто однозначно задаємо значення z_i потоку між джерелом і стоком для кожної тяжіючої пари p_i залежно від розподілу f потоків за ребрами фізичного графу G. Введемо матричну змінну $f = \{f_{i,k}\}$ розміром $(m \times 2e)$. Кожен елемент $f_{i,k}$ позначає кількість потоку i-ї тяжіючої пари за ребром r_k в прямому напрямку для $k \in E$ або за ребром r_{k-l} у протилежному напрямку,

якщо $k > e$, $f_{i,k} \geq 0$. У транзитних вузлах виконуються умови нерозривності потоку, що призводить до відношення:

$$\sum_{k \in S(v)} f_{i,k} - \sum_{k \in T(v)} f_{i,k} = \begin{cases} z_i, \text{ якщо } v = v_{s_i}; \\ -z_i, \text{ якщо } v = v_{t_i}; \\ 0, \text{ в інших випадках}, \end{cases}$$

де $z_i \geq 0$ – величина вхідного потоку, що проходить через СЗІ КМЗ від джерела до стоку p_i при розподілі потоків f. В матричній формі отримаємо $Z = Z(f)$ систему рівнянь: $f_i A = z_i B, i \in M$, нижній індекс в матриці позначає відповідний вектор-рядок. Вектор $Z = Z(f) = (z_1, z_2, ..., z_m)$, що визначаємо вектором розподілу потоків f, є сукупністю потоків між усіма тяжіючими парами p_i і називається мультипотоком Z. Позначимо через $y_k = \sum_i \left(f_{i,k} + f_{i,(k+l)} \right)$ загальний потік через ребро r_k відповідно до розподілу потоків f. Кожному ребру r_k припишемо деяку кількість $C_k \geq 0$, яку називатимемо пропускною здатністю ребра r_k та яку вимірюватимемо в умовних одиницях потоку. Вектор $C = (c_1, c_2, ..., c_l)$ будемо вважати фіксованим та відомим. Вектор C задає наступні обмеження на розподіл потоків через СЗІ КМЗ: $\sum_{i=1}^{m} \left(f_{i,k} + f_{i,(k+l)} \right) \leq C_k$. Позначимо: $F(c)$ – множина можливих розподілів потоків f; $L(c)$ – множина можливих мультипотоків z; $X(c) = \{x\} = (f_1, f_2, ..., f_m, Z)$ – множина усіх можливих розподілів потоків f та мультипотоку Z. Нехай в потоковій СЗІ КМЗ заданий вектор d вимог або заявок тяжіючих пар p_i на величини потоків між джерелом та стоком, тобто всім ребрам p_i логічного графу приписані числа $d_i \geq 0$, які вимірюємо в умовних одиницях потоку, які необхідно пропустити через дане логічне ребро СЗІ КМЗ (так званому інформаційному напрямку). Якщо вектор d відомий, тоді ставиться задача про допустимість СЗІ КМЗ для наведеного вектора вимог, тобто виконання умови: $d \in L(c)$. Це визначає такий розподіл потоків $F(c)$, на якому досягаємо вектора вимог: $d \in Z(f)$, що формально розуміємо як $z = Z$. Відповідний розподіл потоків f, який допустимий для вектора d, позначимо $f[d]$. Зазначимо, що такий розподіл не єдиний. Вектор d може бути і невідомим точно, наприклад, задається лише множина його значень D, така як: $D = \left\{ d \middle| \sum_{i=1}^{m} d_i = d_0 \right\}$. Виникають дві різні постановки задачі про допустимість: гарантована – $D \subseteq L(c)$; слабка (допустимість хоча б одного вектора $d \in D$). При такій постановці задачі допустимим є лише якийсь один розподіл: $D \cap L(c) \neq 0$.

6. Дослідження моделей оцінювання живучості системи захисту інформації. Для наочності процесу оцінювання живучості системи захисту інформації дослідимо СЗІ КМЗ з різними структурами (місткова, з паралельно-послідовною структурою, із загальним структурним резервом з цілою кратністю) та наведемо результати у таблицях нижче.

6.1. Дослідження моделі оцінювання живучості системи захисту інформації за станом системи

Таблиця 1

Значення виживаності системи $R(n)$

при n-кратному впливі дестабілізуючих факторів для СЗІ з містковою структурою при $n \leq 5$

n	1	2	3	4	5	6	7
$R(n)$	1	0,84	0,52	0,3024	0,1744	0,1012	0,0592

Таблиця 2

Значення коефіцієнтів L_{nk} для СЗІ з містковою структурою

n	L_{nk}						
	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$
1	1	0	0	0	0	0	0
2	1	2	0	0	0	0	0
3	1	6	6	0	0	0	0
4	1	14	36	24	0	0	0
5	1	30	150	240	120	0	0
6	1	62	540	1560	1800	720	0
7	1	126	1806	8400	16800	15120	5040

Таблиця 3

Значення коефіцієнтів B_{ki} для дев'яти працездатних структур СЗІ, що отримують із базової структури шляхом видалення одного, двох або трьох функціональних елементів

k	B_{ki}								
	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$	$i=9$
1	1	1	1	1	1	0	0	0	0
2	0	0	0	0	0	3	3	1	1
3	0	0	0	0	0	1	1	0	0

Використовуючи формули (8) та (21), знайдемо середню кількість ДФ, яка призводить до втрати працездатності СЗІ КМЗ:

$$\omega = \sum_{n=0}^{\infty} R(n) = 1 + \sum_{n=0}^{\infty} \{2(0.6)^n + 2(0.4)^n - (0.2)^{n-1}\} = 4.083 .$$

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

Таблиця 4

Значення коефіцієнтів r_{ni}, які позначають кількість способів, якими при n-кратному ДФ можна перейти від базової структури S_0 до структури S_i

n	r_{ni}					r_n	N^n
	$i=1..5$	$i=6$	$i=7$	$i=8$	$i=9$		
1	1	0	0	0	0	5	5
2	1	6	6	2	2	21	25
3	1	24	24	6	6	65	125
4	1	78	78	14	14	189	625
5	1	240	240	30	30	545	3125
6	1	726	726	62	62	1581	15625
7	1	2184	2184	126	126	4625	78125

Середня кількість ДФ $\omega = 1 + \sum_{n=0}^{\infty} \{2(0.5)^n + 2(0.25)^n - 5(0.125)^n\} = 2.9524$. Середній запас живучості $\overline{d} = 1.9524$. Це значно менше, ніж m-живучість (у цьому випадку $m = 4$).

Таблиця 5

Значення виживаності системи при n-кратному впливі дестабілізуючих факторів для СЗІ з паралельно-послідовною структурою

n	1	2	3	4	5	6
$R(n)$	7/8	35/64	139/512	539/4096	2107/32768	8315/262144
$R^*(n)$	7/8	1/2	8/56	1/35	0	0

Таблиця 6

Значення коефіцієнтів B_{ki} для СЗІ з паралельно-послідовною структурою

k	B_{ki}								
	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$	$i=9$
1	1	1	1	1	1	1	1	0	0
2	0	0	0	0	0	6	6	1	1
3	0	0	0	0	0	4	4	0	0
4	0	0	0	0	0	1	1	0	0

Таблиця 7

Значення r_{ni} для СЗІ з паралельно-послідовною структурою

n	r_{ni}					r_n	N^n
	$i=1..5$	$i=6$	$i=7$	$i=8$	$i=9$		
1	1	0	0	0	0	7	8
2	1	13	13	2	2	35	64
3	1	61	61	6	6	139	512
4	1	253	253	14	14	539	4096
5	1	1021	1021	30	30	2107	32768

Отже, результати у табл. 5 та 7 збігаються. Аналіз даних табл. 7 дає змогу встановити цікаву закономірність. Відношення r_{ni}/r_n виражає умовну ймовірність збереження структури S_i після n-кратного ДФ за умови, що система залишилась працездатною. Як видно із результатів обчислень (табл. 8), лише для одного типу структури (s_6 та s_7) умовна ймовірність зростає із збільшенням кількості ДФ і ця структура ненадлишкова і має найменшу кількість елементів. Вже при $n=5$ на частку структур s_6 та s_7 припадає 97% всіх випадків, коли система зберігає працездатність.

Таблиця 8

Відношення r_{ni}/r_n для СЗІ з паралельно-послідовною структурою

n	r_{ni}/r_n		
	$i=1..5$	$i=6,7$	$i=8.9$
1	0.1429	0.1429	0
2	0.0286	0.3714	0.0571
3	0.0072	0.4388	0.0432
4	0.0019	0.4694	0.0260
5	0.0005	0.4846	0.0142

Із даних (табл. 9) видно, що за великої кількості резервних елементів вразливість системи є низькою навіть за надвеликої кількості ДФ. Якщо кількість ДФ дорівнює кількості елементів, тоді

вразливість системи знижується відповідно до збільшення надлишковості доволі помітно: більше ніж на порядок при збільшенні N від 2 до 5 (діагональні елементи в табл. 9). Виживаність системи не є дуже низькою, навіть якщо кількість ДФ вдвічі перевищує кількість елементів: 0.125 при $N=2$ і 0.26 при $N=3$. В окремому випадку, $\overline{\omega}=3$ при $N=2$, $\overline{\omega}=5.5$ при $N=3$. Середній запас живучості, відповідно, 2 і 4.5. Це значно більше, ніж m-живучість (в 2 і 2.25 раза).

Таблиця 9

Результати обчислень умовного закону вразливості $Q(n)$ для СЗІ із загальним структурним резервом з цілою кратністю

n	$Q(n,N)$				
	$N=2$	$N=3$	$N=4$	$N=5$	$N=6$
2	0.5	0	0	0	0
3	0.75	0.2222	0	0	0
4	0.875	0.4444	0	0	0
5	0.9375	0.6173	0.2344	0.0384	0
6	0.9688	0.7407	0.3809	0.1152	0.0154
7	0.9844	0.8258	0.5127	0.2150	0.0540

6.2. Дослідження оцінювання живучості системи захисту інформації за результатами виконання завдання

Таблиця 10

Результати оцінювання живучості СЗІ з містковою структурою за результатами виконання завдання

q	$G(t,n)$					$P(t/S_0)$
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	
0.00	1.0000	0.8400	0.5200	0.3024	0.1744	1
0.02	0.9839	0.8082	0.4989	0.2900	0.1673	0.9992
0.05	0.9594	0.7653	0.4695	0.27272	0.1574	0.9948
0.10	0.9189	0.7003	0.4262	0.2474	0.1429	0.9785

Таблиця 11

Значення $G(t,n,q)/G(t,n,0)<1$ СЗІ з містковою структурою

q	$G(t,n,q)/G(t,n,0)$				
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$
0.02	0.9839	0.9621	0.9594	0.9590	0.9593
0.05	0.9594	0.9111	0.9029	0.9018	0.9025
0.10	0.9189	0.8337	0.8196	0.8181	0.8194

Із даних випливає, що показники живучості у всіх випадках менші, ніж показники безвідмовності. Необхідно зазначити і таку важливу властивість, що із збільшенням q функція виживаності зменшується, тобто відношення $G(t,n,q)/G(t,n,0)<1$ при всіх значеннях q та n, тобто малонадійна система більш вразлива при зовнішніх збуреннях, ніж високонадійна система (табл. 11). Причому із збільшенням q функція виживаності зменшується швидше, ніж спадає ймовірність виконання завдання. Отже, можна зробити висновок, що при одних і тих самих

вимогах до живучості і безвідмовності для забезпечення живучості вимагається висщй рівень надлишковості.

Таблиця 12

Результати оцінювання живучості СЗІ з паралельно-послідовною структурою за результатами виконання завдання

q	$G(t,n)$					$P(t/S_0)$
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	
0.00	0.8750	0.5469	0.2715	0.1316	0.0643	1
0.02	0.8418	0.5158	0.2556	0.1240	0.0606	0.9773
0.05	0.7980	0.4758	0.2352	0.1143	0.0560	0.9334
0.10	0.7376	0.4229	0.2084	0.1013	0.0497	0.8445

Таблиця 13

Відносне зниження функції виживаності із зростанням q

q	$G(t,n,q)/G(t,n,0)$				
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$
0.02	0.9621	0.9450	0.9414	0.9422	0.9425
0.05	0.9120	0.8700	0.8663	0.8685	0.8709
0.10	0.8430	0.7733	0.7676	0.7698	0.7729

Порівнюючи дані табл. 13 і 11, бачимо, що в системі захисту, яка розглядається, зниження живучості з погіршенням безвідмовності елементів ще більш помітне, ніж в системі з містковою структурою.

6.3. Дослідження потокової моделі оцінювання живучості системи захисту інформації. Задамо систему захисту інформації графом з великою кількістю вершин (що зумовлює актуальність та доцільність застосування саме потокової моделі оцінювання живучості) так, щоб із вершини, яка обрана випадково можна було встановити зв'язок після атаки зловмисника (впливу ДФ) з 90% ($\beta = 0.9$) неуражених вершин. При цьому вважатимемо, що ребра графу невразливі, а вершини піддаються знищенню. Щільність атак становить 100 атак/хв. Ймовірність ураження конкретної вершини $\Delta/D = 0.05/1 = 0.05, k_s = 1$.

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

Отже, 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: $\sum_{k=1}^{k_s-1} g_k^l(\eta) = e^{-0.05}((0.05*100)/1) = 0.034$. Від початкових 380 вершин залишиться лише 3% – 12 вершин. Загальний потік знизиться більше ніж в 30 разів, система захисту інформації стане недопустимою, тобто СЗІ КМЗ буде знищена.

Висновки. Визначено показники живучості, які на практиці можна використовувати для формального оцінювання живучості систем захисту інформації КМЗ. Отримала подальший розвиток математична модель оцінювання живучості СЗІ КМЗ за станом системи, що дає можливість оцінити виживаність системи при n-кратному впливі ДФ та використовувати точкову, статичну модель системи без врахування стійкості елементів і вторинних наслідків після ДФ. Результати дослідження математичної моделі показали, що при великій кількості резервних елементів вразливість СЗІ є низькою навіть при надвеликій кількості ДФ. Отримала подальший розвиток математична модель оцінювання живучості СЗІ 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 ДФ. Результати дослідження математичної моделі показали, що в СЗІ зниження властивості живучості з погіршенням безвідмовності елементів є більшим, ніж в системі з містковою структурою. Отримала подальший розвиток математична модель потокового оцінювання живучості СЗІ, яку доцільно використовувати для розподілених КМЗ, що вирішує проблему перерозподілу потоків після впливу ДФ. Дослідження потокової моделі оцінювання живучості дало змогу визначити можливість (кількісно) встановлення зв'язку між ФЕ СЗІ КМЗ при однократному впливі ДФ, а також визначити кількість ФЕ, які залишаться після впливу ДФ.

1. Mead N. R. Survivable Network Analysis Method / N. R. Mead, R. J. Ellison, R. C. Linger, T. Longstaff, J. McHugh. – CMU/SEI-2000-TR-013. – 2000. – 61 p. 2. Wutz D. Application of the Survivable Network Analysis Method to Secure My Office System / D. Wutz / SANS Institute InfoSec. – 2001. – 1–12 p. 3. US Patent Application Publication. Multi-variate network survivability analysis / Vanko Vankov, Vinod Jeyachandran, Pradeep K. Singh, Alain J. Cohen, SHobana Narayanaswamy. – Pub. No.: US 2008/0040088 A1. – Feb. 14.2008. – 1–9 p. 4. Christie A. M. Network Survivability Analysis Using Easel / A. M. Christie. – CMU/SEI-2002-TR-039. – 2002. – 71 p. 5. Зиновьев П. А. Анализ факторов и механизмов живучести в корпоративных информационных системах / П. А. Зиновьев // Исслед. по информ., Отечество. – Казань, 2007. – С. 3–30. 6. Павский В. А. Вычисление показателей живучести распределенных систем и осуществимости решения задач / В. А. Павский, К. В. Павский, В. Г. Хорошеский // Искуственный интелект. – 2006. – № 4. – С. 28–34. 7. Павский В. А. Расчет показателей живучести распределенных вычислительных систем / В. А. Павский, С. А. Иванова. – 2007. – С. 1–4. 8. Черкесов Г. Н. Методы и модели оценки живучести сложных систем / Г. Н. Черкесов. – М., 1987. – 38 с. 9. Громов Ю. Ю. Синтез и анализ живучести сетевых систем / Ю. Ю. Громов, В. О. Драчев, К. А. Набатов, О. Г. Иванова. – М. : «Издательство машиностроение – 1». – 2007. – 88 с. 10. Neumann P. G. Practical architectures for survivable systems and networks / P. G. Neumann. – SRI International, 2000. – 227 p. 11. Мінін А. В. Критерії і моделі оцінки живучості комп'ютерної системи / А. В. Мінін, М. Ф. Смирний // Інформаційна безпека. – 2009. – № 2 (2). – С. 115–119. 12. Горшков В. В. Логико-вероятностный метод расчета живучести сложных систем / В. В. Горшков. – Кибернетика АН УССР, 1982. – № 1. – С. 104-107. 13. Рябинин И. А. Надежность и эффективность структуры сложных технических систем / И. А. Рябинин, Ю. Н. Парфенов // В кн. : Основные вопросы теории и практики надежности. – Минск : Наука и техника, 1982. – С 25–40. 14. Руденко Б. Н. Надежность систем энергетики / Б. Н. Руденко, И. Н. Ушаков. – М. : Наука, 1986. – 252 с.