УДК 004.056, 004.75

Ю.Р. Гарасим[2], М.М. Рибій[1], В.А. Ромака[1]
[1]Національний університет "Львівська політехніка",
кафедра захисту інформації,
[2]ТзОВ "Спейс Ай Ті"

ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ ТА НЕПЕРЕРВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Запропоновано підхід до вирішення завдання забезпечення живучості та неперервності функціонування систем захисту інформації (СЗІ) у корпоративних мережах зв'язку (КМЗ). Детально проаналізовано процес відновлення функціонування СЗІ в КМЗ та визначено його параметри. Вирішено завдання визначення рівня залежності між режимами роботи СЗІ в КМЗ із застосуванням теорії складності обчислень. Обґрунтовано процес визначення економічної ефективності вибраної стратегії забезпечення живучості та неперервності функціонування СЗІ в КМЗ.

Ключові слова: властивість живучості, неперервність функціонування, системи захисту інформації, процес відновлення функціонування.

The paper consider enterprise communication network (ECN) information security system (ISS) survivability property and continuity functioning providing problem solving approach. Enterprise communication network ISS functioning recovery process analyzed in detail. Defined its parameters. Enterprise communication network ISS modes dependence degree definition problem solved using computational complexity theory. Enterprise communication network ISS survivability property and continuity functioning providing economic efficiency of chosen strategy determining process justified.

Key words: survivability property, continuity functioning, information security systems, functioning recovery process.

Вступ

Актуальність завдання забезпечення живучості та неперервності функціонування систем захисту інформації (СЗІ) в корпоративних мережах зв'язку (КМЗ), яке є основним бар'єром проти втрати конфіденційних даних, зумовлює необхідність поглибленого вивчення цього процесу та пошуку шляхів його регламентації/стандартизації. Тому автори запропонували підхід до забезпечення живучості та неперервності функціонування СЗІ, який базується на виправленні недоліків, які притаманні методам, методикам, алгоритмам забезпечення неперервності функціонування складних систем. Отже, отримано можливість детально описати та дослідити процес забезпечення живучості та неперервності функціонування СЗІ за умов невизначеності впливу чинників дестабілізації (ЧД), що є логічним продовженням роботи після проведення їх оцінки. Особливу увагу зосереджено на етапі відновлення функціонування СЗІ, аналіз якого дав змогу показати важливість правильної специфікації параметрів відновлення та врахувати залежність між режимами функціонування СЗІ за умови встановлення допустимих значень параметрів відновлення. Отже, вирішено завдання вибору економічно ефективного та оптимального забезпечення неперервності функціонування СЗІ.

1. Методика забезпечення неперервності функціонування СЗІ

Запропонована методика базується на вимогах трьох методик [1–3]. Вона призначена для ефективного та автоматизованого забезпечення процесу управління неперервністю функціонування СЗІ. Життєвий цикл СЗІ наведено на рис. 1, щоб проілюструвати процес забезпечення неперервності її роботи.

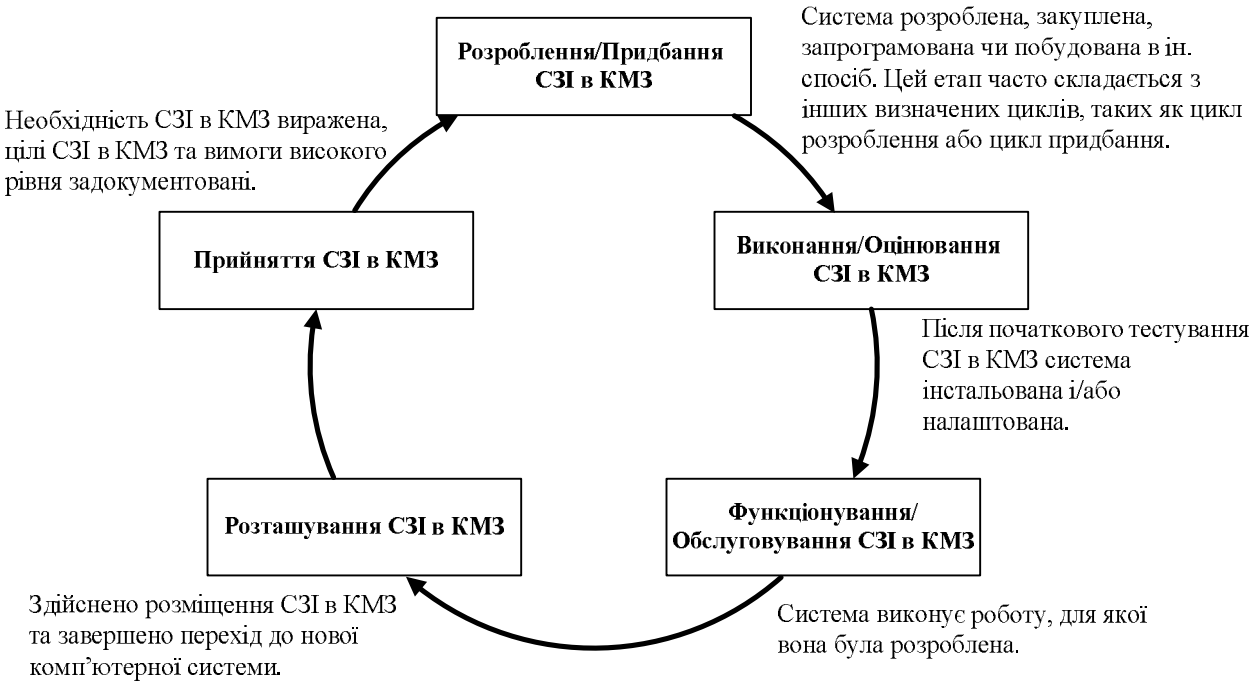

Рис. 1. Життєвий цикл СЗІ в КМЗ

На початковому етапі управління неперервністю функціонування СЗІ важливо усвідомити, як приймаються рішення щодо подолання кризових/аварійних ситуацій/подій та помилок у роботі СЗІ. На рис. 2 наведено схему отримання інформації та прийняття рішень за умови виникнення надзвичайних ситуацій, які можуть загрожувати неперервності функціонування СЗІ.

Розглянемо три основні етапи управління неперервністю функціонування СЗІ відповідно до запропонованої методики.

Етап І. Планування системи управління неперервністю функціонування СЗІ (СУНФ СЗІ).

Визначаємо область (межі) застосування і цілі СУНФ СЗІ з урахуванням: вимог до забезпечення неперервності функціонування СЗІ; загальних цілей та обов'язків організації; встановлених законодавчих, обов'язкових і договірних вимог; інтересів її ключових сторін.

Щоб забезпечити ефективність процесу управління неперервністю функціонування СЗІ та розуміння персоналом вимог забезпечення неперервності, на наступному кроці визначаємо політику СУНФ СЗІ. Ця політика описує загальні цілі організації за умови невизначеності впливу чинників дестабілізації (ЧД), а також встановлює організаційну структуру системи управління неперервністю функціонування СЗІ. Наголошуємо, що важливим є той факт, щоб політика СУНФ СЗІ була схвалена вищим керівництвом та доведена до відома всього персоналу організації [1]. Ключовими елементами політики СУНФ СЗІ є: сфера застосування та цілі політики; ролі та обов'язки; вимоги до необхідних ресурсів; вимоги до обізнаності та навчання персоналу; графіки тестування та технічного обслуговування системи захисту інформації в КМЗ [2].

Структура і функціонування процесу управління неперервністю функціонування СЗІ в КМЗ постійно вимагає фінансових, кадрових і планувальних ресурсів. Тому на цьому етапі визначаємо та забезпечуємо наявність ресурсів, необхідних для розроблення, впровадження функціонування та підтримки СУНФ СЗІ. Кількість ресурсів, необхідних для забезпечення неперервної роботи СЗІ, залежить, передовсім, не лише від розміру і типу організації та виду її діяльності, але також і від розташування, навколишнього середовища, клієнтів, технологій [3].

Акцентуємо, що забезпечення належного рівня компетентності персоналу в сфері управління неперервністю функціонування СЗІ є важливим фактором, який впливає на ефективність розробленої СУНФ СЗІ і забезпечується за допомогою: визначення рівня компетентності персоналу; аналізу потреб у навчанні персоналу, наділеного відповідальністю і повноваженнями в сфері управління неперервністю функціонування СЗІ; проведення навчання; забезпечення досягнення

персоналом необхідного рівня компетентності; реєстрації записів про освіту, навчання, навички, досвід та кваліфікацію персоналу [1].

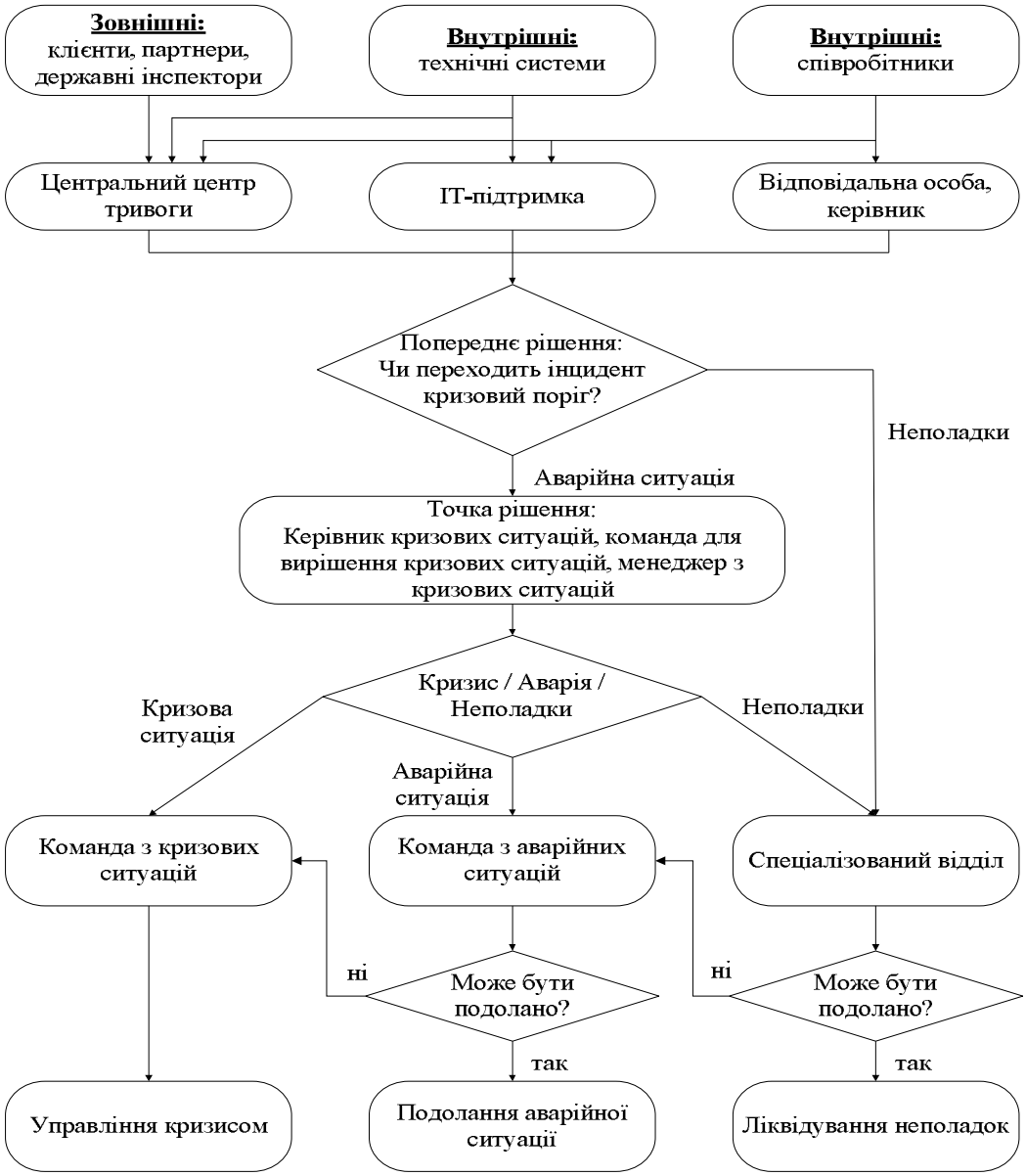

Рис. 2. Схема отримання інформації та прийняття рішень за умови впливу ЧД

Завершальним кроком першого етапу управління неперервністю функціонування СЗІ згідно з вдосконаленою методикою є розроблення плану неперервності функціонування СЗІ. Цей план є широким колом заходів, які спрямовані на підтримку і відновлення роботи СЗІ після впливу ЧД. Зазвичай це набір декількох планів, що забезпечують неперервність роботи СЗІ на основі багатофункціональної взаємодії між ними. Головним завданням є правильна побудова взаємозв'язків між різними видами планів для ефективного забезпечення неперервності функціонування СЗІ. Отже, розглядаємо такі основні категорії планів неперервності функціонування, що взаємодіють: планування неперервної роботи СЗІ під час виникнення аварійних ситуацій та після їх виникнення, планування відновлення роботи СЗІ після впливу ЧД, планування реагування на інциденти, які пов'язані із роботою СЗІ в КМЗ.

Етап ІІ. Аналіз ризиків.

Визначаємо, що аналіз ризиків передбачає три основні процеси: оцінювання ризиків, зниження ризиків та повторне оцінювання ризиків. Відповідно, метою аналізу ризиків є визначення

усіх можливих ризиків для врахування їх в процесі прийняття управлінських та стратегічних рішень та, за необхідності, розроблення відповідних стратегій і заходів захисту для зниження цих ризиків заздалегідь і підвищення живучості СЗІ [3].

Тому, відповідно до удосконаленої методики, першим кроком другого етапу є ідентифікація та оцінювання ризиків. Зазначимо, що існують різні методики оцінювання ризиків, зазначені в ISO\IEC 27005, NIST 300-80, BSI 100-3 тощо, але всі методики в загальному випадку містять такі елементи:

- визначення та ранжування чутливості та критичності системи, функціонування яких може порушуватись внаслідок реалізації загроз;
- ідентифікація загроз та вразливостей, які можуть пошкодити, вивести з ладу чи перервати на деякий час роботу системи і, тим самим, зумовити втрату, модифікацію чи витік конфіденційної інформації. Джерелами загроз у цьому випадку можуть бути як люди (зовнішні зловмисники, незадоволені співробітники), так і природні катаклізми (стихійні лиха). Оцінювання можливості реалізації загроз здійснюється на основі історичних відомостей, досвіду та компетентності аудитора;
- оцінювання потенційного збитку чи шкоди від реалізації перелічених загроз, зокрема витрат на відновлення функціонування СЗІ.

На етапі аналізу та оцінювання ризиків використано методику, наведену в табл. 1.

Таблиця 1

Методика оцінювання рівня ризику

		Вплив / Збиток			
		Низький	**Середній**	**Високий**	**Дуже високий**
Ймовірність	**Висока**	низький	середній	високий	дуже високий
	Середня	низький	середній	високий	високий
	Низька	низький	низький	середній	середній
	Відсутня	низький	низький	низький	низький

Після виконання перелічених вище кроків розробляємо звіт щодо аналізу ризиків. У цьому звіті подаємо не лише результати оцінювання ризиків, але й опис методики, яку використовували для їх оцінювання.

Етап ІІІ. Заходи забезпечення живучості та неперервності функціонування СЗІ в КМЗ.

На завершальному етапі забезпечення неперервності функціонування СЗІ передовсім вибирають заходи забезпечення неперервності функціонування. Такі заходи можуть передбачати як впровадження нових організаційних політик і процедур, так і технічні рішення захисту, наприклад, резервне копіювання даних, відновлення процесу функціонування, віддалене зберігання резервних копій даних, архівація даних, реплікація тощо.

Після цього особливу увагу приділяємо специфікації параметрів відновлення функціонування СЗІ, встановленню впливу залежностей між режимами роботи СЗІ в КМЗ на параметри відновлення та визначенню економічної ефективності вибраних заходів забезпечення неперервності. Розглянемо ці аспекти детальніше.

2. Специфікація параметрів відновлення функціонування СЗІ

Процес відновлення функціонування СЗІ розпочинається після того, як оцінено пошкодження та відмикання, працівників повідомлено і відповідні команди мобілізовано. Цей процес забезпечує відновлення можливостей системи, ремонт пошкоджень та приведення функціональних можливостей СЗІ в початковий або новий альтернативний стан.

Розглядаючи процес відновлення функціонування СЗІ, автори визначили такі параметри відновлення, які графічно наведено на рис. 3:

- максимально допустимий період недоступності (МДПН) СЗІ – це максимальний проміжок часу, протягом якого СЗІ можуть бути недоступними внаслідок впливу ЧД, перш ніж виникне можливість негативних наслідків, таких як: руйнування, модифікація чи витік конфіденційних даних [4];
- цільовий час відновлення (ЦЧВ) СЗІ – це проміжок часу, протягом якого функціонування СЗІ повинне бути відновлене з метою уникнення негативних наслідків, які пов'язані із втратою даних. Показник ЦЧВ повинен бути меншим, аніж МДПН [3];
- час відновлення (ЧВ) – складається з часу до виявлення надзвичайних ситуацій, часу реакції (час між виявленням надзвичайної ситуації та початком застосування відновлювальних заходів) та фактичного часу, необхідного для відновлення процесу. Показник ЧВ може бути більшим, ніж МДПН, у такому випадку безпека активів та даних буде під загрозою [3];
- максимально допустимий період аварійного режиму (МДПАР) або максимально допустимий час відновлення (МДЧВ). Останній є сумою ЧВ і МДПАР [3];
- час для повернення в нормальний режим роботи з аварійних режимів є частиною часу аварійного режиму і також повинен бути взятий до уваги під час планування [3];
- після того, як режим нормального функціонування СЗІ відновлений, може бути необхідним виконання деяких післяаварійних режимів роботи і час, необхідний для цієї роботи, є частиною часу нормального функціонування [3].

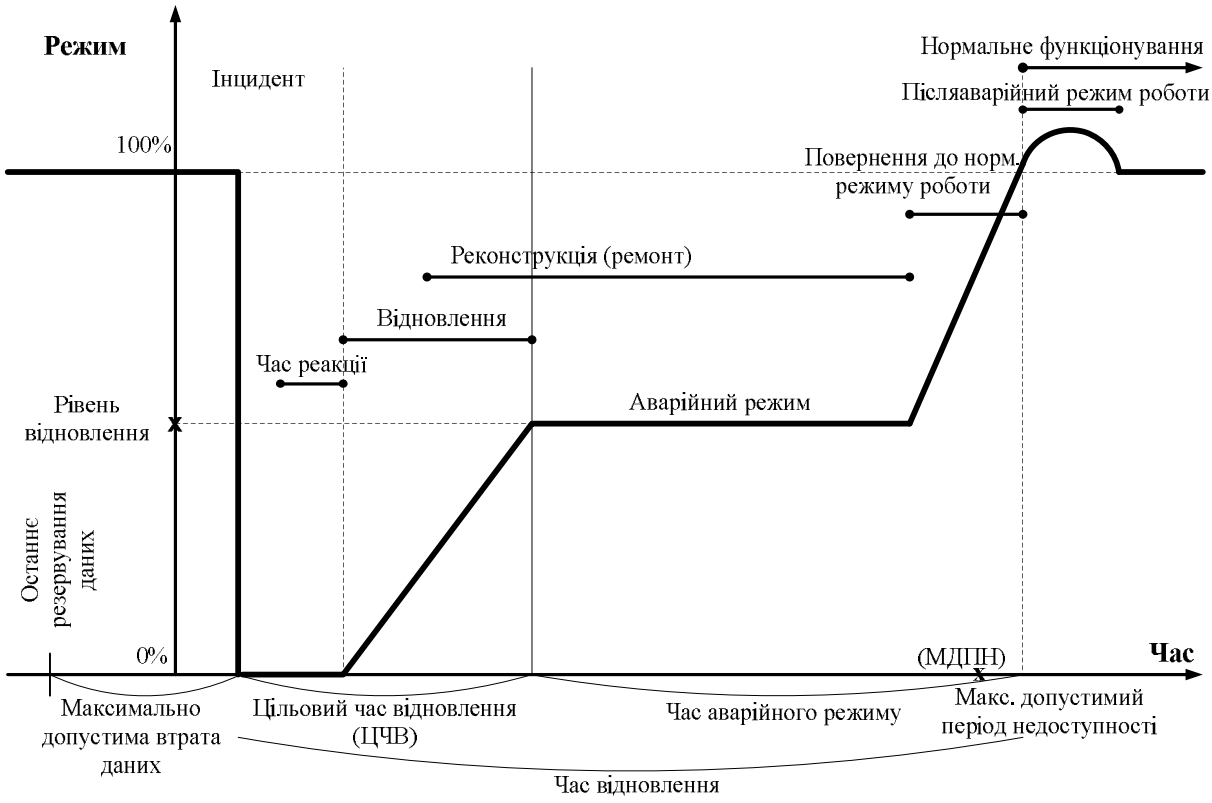

Рис. 3. Параметри процесу відновлення функціонування СЗІ в КМЗ

3. Вплив залежності між режимами функціонування СЗІ на параметри відновлення

Залежність між режимами функціонування СЗІ може зумовити необхідність адаптування часу відновлення функціонування окремих СЗІ. Рівень корекції часу відновлення функціонування відповідної СЗІ залежить від рівня залежності між СЗІ. Це означає, що чим вища залежність, тим більший розмір компенсації за час відновлення. Тому необхідно не лише розрізняти «незалежні» і «залежні» режими функціонування СЗІ, але й визначити ієрархічну модель залежностей [3]. Тобто перед авторами постало завдання визначення рівня залежності між режимами функціонування СЗІ із застосуванням теорії складності обчислень.

Отже, в загальному випадку, якщо ми маємо завдання $x \in \{0,1\}^*$ і хочемо отримати для нього вирішення $y \in \{0,1\}^*$, яке є взаємозалежним з x, то завдання пошуку рішення характеризується відношенням

$$R \subseteq \{0,1\}^* \times \{0,1\}^*, \tag{1}$$

де $(x, y) \in R$ тоді й тільки тоді, коли y є прийнятним рішенням для x [5].

У нашому випадку як завдання x ми розглядаємо пошук рівня залежності між режимами функціонування СЗІ в КМЗ, а y буде її рішенням в тому випадку, якщо воно існує. Якщо вирішення завдання немає $y \in R(x)$, $R(x)$ – порожня множина.

Отже, пошук рівня залежності між режимами функціонування СЗІ в КМЗ розглядається як неорієнтований граф

$$G = (V, E), \tag{2}$$

який зображено на рис. 4, для якого V є множиною вершин графа, що є множиною СЗІ в КМЗ

$$V \to \{S_1, S_2, \mathbf{K}, S_n\}, \tag{3}$$

а E – ребрами графа, які становлять множину коефіцієнтів залежностей між режимами функціонування СЗІ в КМЗ

$$E \to \{1,2,3,4\}. \tag{4}$$

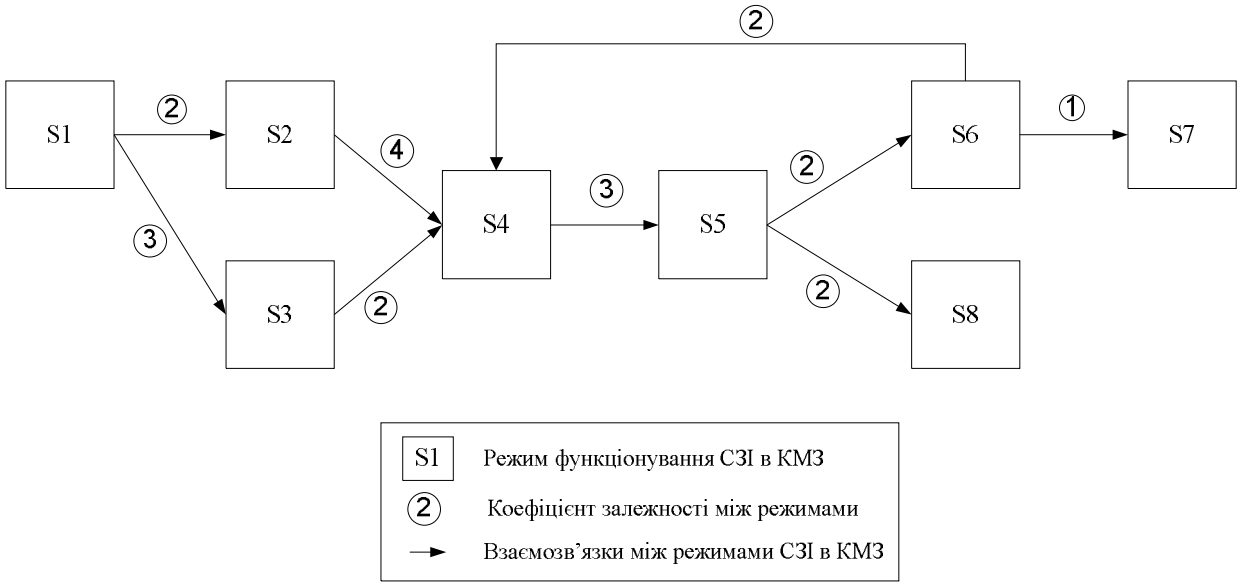

Рис. 4. Граф залежності між режимами функціонування СЗІ в КМЗ

Авторами запропонована така шкала оцінювання залежності, яка визначає значення коефіцієнтів множини E: «1» – низький рівень залежності між режимами функціонування СЗІ в КМЗ, «2» – середній рівень залежності, «3» – високий рівень залежності, «4» – дуже високий рівень залежності.

Звідси, для кожного рівня залежності відповідно до запропонованої шкали оцінювання встановлено значення цільового часу відновлення, поданого у вигляді множини

$$RTO \to \{168,96,48,24\}. \tag{5}$$

Вирішення завдання визначення рівня залежності між режимами функціонування СЗІ в КМЗ подамо у вигляді алгоритму:

$$R(x) = \{y \mid \forall E_n.E, |E| = n, \quad \exists R_k.RTO : |RTO| = k, (k = n) \wedge (R_k = R_k \frac{E_n}{10})\}. \tag{6}$$

Алгоритм є можливим для виконання в тому випадку, якщо він виконується протягом деякого поліноміального часу $p(n)$ з довжиною алгоритму n.

Оскільки

$$|x| \sim O(n^2) \Rightarrow |x| \sim n^2 \text{ і } |y| \sim O(n), \quad (7)$$

виконується умова:

$$|y| \le p(|x|), \quad (8)$$

Отже, на основі (8) отримано алгоритм вирішення проблеми визначення рівня залежності між процесами СЗІ в КМЗ, який є поліноміально обмеженим і який можливо виконати.

4. Визначення економічної ефективності заходів забезпечення неперервності функціонування

Наголошуємо на тому, що одним з найважливіших факторів правильного й ефективного управління неперервністю функціонування СЗІ є забезпечення неперервності за прийнятною ціною. Аналіз витрат на план забезпечення неперервності функціонування СЗІ і збережених коштів, внаслідок реалізації плану неперервності за умови впливу ЧД, можна використати для визначення правильності та ефективності вибраної стратегії неперервності функціонування СЗІ та відновлюваних заходів і засобів. Оскільки неможливо врахувати всі фактори впливу через динамічну зміну умов зовнішнього середовища та невизначеність впливу ЧД, аналіз вартості забезпечення неперервності функціонування СЗІ здійснюємо за допомогою прагматичного підходу. Цей підхід поділено на етапи [3].

Визначення збитків внаслідок впливу ЧД. Визначаємо потенційні збитки від дії ЧД. Враховуємо той факт, що чим швидше СЗІ відновить свою роботу після впливу ЧД, тим збиток для організації буде меншим.

Визначення вартості стратегії забезпечення неперервності функціонування СЗІ. На цьому етапі визначаємо вартість заходів та засобів забезпечення неперервності функціонування СЗІ. Окрім витрат на придбання необхідних засобів та послуг, у ці витрати входять поточні витрати для постійного технічного обслуговування, підготовки кадрів, лізингові витрати тощо.

Аналіз збитків та витрат. Після визначення збитків від реалізації ЧД та вартості стратегії неперервності функціонування СЗІ результати попередніх двох етапів підсумовуємо, щоб використати як допомогу під час ухвалення рішення. Підсумок оформляємо у вигляді звіту.

Наведемо приклад розрахунку економічної ефективності різного роду стратегій для забезпечення неперервності функціонування СЗІ, який подано в табл. 2.

Таблиця 2

Аналіз економічної ефективності стратегій забезпечення неперервності функціонування СЗІ

СЗІ, МДПН = 10 днів	Цільовий час відновлення	Вартість відновлення	Збиток до відновлення	Надійність / Граничні умови / Обмеження
S1: «Гаряче резервування». Повний набір резервного обладнання для функціонування.	< 6 год	5 млн. дол.	Низький	Дуже високі
S2: «Тепле резервування». Повна альтернативна база, але меншої потужності, відновлення з резервних копій.	6–24 год	3 млн. дол.	Низький – середній	Високі
S3: «Холодне резервування». Деяке обладнання для використання в надзвичайних ситуаціях, встановлення програмного забезпечення і додатків, відновлення даних з резервної копії.	2–10 днів	1 – 1,2 млн. дол.	Середній – високий	макс. ЦЧВ 10 днів відповідає МДПН

Нижче, на рис. 4, наведено приклади фінансової ефективності стратегій неперервності функціонування СЗІ різного роду (Ws1,…, Ws4) з графічним відображенням взаємозалежності величини вартості відновлення та збитків внаслідок реалізації ЧД.

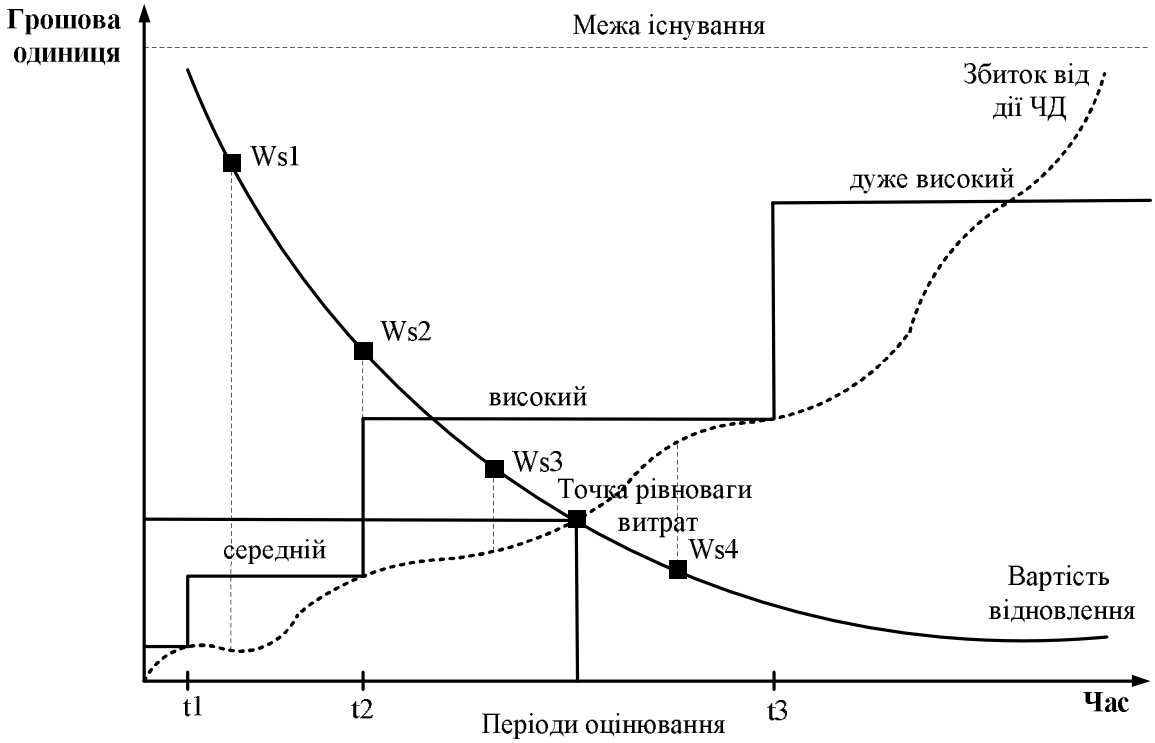

Рис. 5. Результуючі вартість відновлення функціонування СЗІ та збиток від реалізації ЧД

Висновки

Удосконалено методику забезпечення неперервності функціонування СЗІ, що дало змогу проаналізувати та описати процес забезпечення неперервності функціонування СЗІ за умов невизначеності впливу ЧД. Детально розглянуто процес відновлення функціонування СЗІ, здійснено специфікацію параметрів відновлення з метою забезпечення оперативного та ефективного процесу відновлення роботи СЗІ. Значну увагу приділено наявності залежності між режимами функціонування СЗІ та вирішено завдання визначення рівня залежності між режимами роботи СЗІ за допомогою застосування теорії складності обчислень. Це дало змогу ефективніше та економічно обґрунтовано забезпечити живучість та неперервність функціонування систем захисту інформації.

1. BS 25999-1:2006 Business continuity management. Specification. 2. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems. 3. BSI-Standard 100-4: Business Continuity Management. 4. Maximum tolerable period of disruption [Електронний ресурс] режим доступу: http://en.wikipedia.org/wiki/ Maximum_Tolerable_Period_of_Disruption. 5. Papadimitriou Christos H. Computational Complexity / H. C. Papadimitriou – QA267.7.P.36. – 1995. – 540 pp.