DOI: 10.15587/2312-8372.2017.112495

РОЗРОБКА ПІДХОДУ ДО ПРОЕКТУВАННЯ, МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ КРИТИЧНОЇ ІТ-ІНФРАСТРУКТУРИ

Дорогий Я. Ю.

1. Вступ

На сьогоднішні створення критичних ІТ-інфраструктур є невід'ємною складовою розвитку ключових галузей, які є життєво необхідними для забезпечення безпеки та функціонування соціуму.

Існування критичної ІТ-інфраструктури тісно пов'язане з поняттям критичної інфраструктури – інфраструктури, що є критично важливою для держави, відмова або знищення якої може суттєво негативно вплинути на національну безпеку.

На цей час Україна тільки починає розробку таких глобальних комплексів управління, хоча деякі галузі вже мають розвинуті ІТ-інфраструктури, наприклад, диспетчерські системи управління транспортом, об'єктами енергетики.

Саме тому розроблення нових підходів, методів та алгоритмів створення, аналізу, моніторингу, забезпечення якості та надійності функціонування, безпечності критичних ІТ-інфраструктур є дуже актуальною проблемою.

2. Об`єкт дослідження та його технологічний аудит

Об'єктом дослідження є критична ІТ-інфраструктура.

У проекті закону [1] визначено, що критична ІТ-інфраструктура – це сукупність інформаційно-телекомунікаційних систем державного та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об'єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором, підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур і оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави. До критичних інфраструктур відносяться: фінансовий та енергетичний сектор держави, харчова промисловість, медицина, виробництво, транспортна система, водопостачання, державне управління та ін.

Критична ІТ-інфраструктура повинна:

– забезпечувати функціонування екологічно небезпечних та соціально значимих виробництв та технологічних процесів, порушення штатного режиму яких може призвести до надзвичайної ситуації техногенного характеру;

– виконувати функції інформаційної системи, порушення (зупинення) функціонування якої може призвести до негативних наслідків в політичній, економічній, соціальній, інформаційній, екологічній та інших галузях;

– забезпечувати надання значного об’єму інформаційних послуг, часткове або повне зупинення яких може призвести до значних негативних наслідків для національної безпеки в багатьох галузях.

Хоча кожна критична IT-інфраструктура зазвичай розглядається як окрема система, всі її системи сильно взаємопов'язані з різним рівнем взаємозалежності між ними. Як приклад, для роботи інформаційно-телекомунікаційної системи (ІТС) на рівні заявленої якості обслуговування потрібна безперебійна робота системи постачання електроенергії, в той час як якість роботи самої системи електропостачання залежить від стабільної роботи каналів передачі інформації ІТС. Ці двонаправлені відносини між системами критичної IT-інфраструктури підвищують їх загальну продуктивність, але в той же час збільшують її складність та чутливість до різного роду атак [2, 3].

Основна проблема в даній галузі – повна відсутність готових рішень, методологій, інструментарію, які б підійшли для моделювання, проектування та дослідження критичних IT-інфраструктур.

3. Мета та задачі дослідження

Метою даної роботи є розробка підходу до проектування, моделювання та дослідження критичної IT-інфраструктури.

Для досягнення поставленої мети необхідно виконати такі задачі:

1. Удосконалити існуючий математичний апарат відкритих гібридних автоматів для дослідження критичних IT-інфраструктур.
2. Побудувати спрощену модель критичної IT-інфраструктури та дослідити за її допомогою запропонований підхід.

4. Дослідження існуючих рішень проблеми

Моделювання взаємозалежності систем – це новий науковий напрямок, що включає кілька інноваційних підходів до моделювання. Існуючі моделі проаналізовані в працях [4, 5]. Серед найпопулярніших – це методи введення-виведення, агентне моделювання та мережеві підходи.

Методи введення-виведення ґрунтуються на теорії економічної рівності В. Леонтьєва і дозволяють оцінити цілісний рівень непрацездатності (відсоток несправності) інфраструктур шляхом використання коефіцієнтів залежності (коефіцієнтів Леонтьєва). Однак ці коефіцієнти важко правильно визначити, і тому, як правило, вони є наближенням більш високого рівня, виходячи з припущення про те, що взаємозалежність інфраструктур пов'язана з їхньою економічною взаємодією [6].

Методи агентного моделювання (АМ) розглядають критичні інфраструктури як гнучкі адаптивні системи (ГАС), тобто як комплекс взаємодіючих компонентів, стан яких може змінюватися в процесі навчання. Методи АМ використовують стратегію

проектування знизу-вгору і тому різні компоненти ІТ-інфраструктури представлені як автономні агенти з своїми атрибутами, поведінкою та правилами прийняття рішень, в той час як взаємозалежності між ними виникають при їх взаємодії [7, 8].

Мережеві підходи зазвичай припускають, що кожна інфраструктура складається з множини мережевих компонентів (як правило, представлених у вигляді вузлів), що утворюють мережу, і будь-які існуючі залежності представлені як відносини між вузлами, що належать до різних мереж [9]. Використання мережевих моделей для дослідження критичних взаємозалежних інфраструктур дає можливість досить легко виконати топологічний аналіз (тобто, якісно описати існуючі зв'язки для будь-якого набору компонентів). Недоліком даних моделей є досить мала кількість інформації для проведення функціонального аналізу. Зазвичай, такі моделі дають можливість дослідити лише спрощені гіпотези та отримати тільки базові характеристики мереж та повністю відсутня можливість дослідити складні ефекти, пов’язані з технологічними аспектами їх реалізації [10].

Також є ряд інших підходів до моделювання взаємозалежності систем критичних інфраструктур. Наприклад, в працях [11–13] представлені методи, побудовані на мережах Петрі, мережах стохастичної активності і байєсівських мережах.

На даний момент підходи, що представлені в літературі, використовуються для різних цілей, мають свої сильні і слабкі сторони, але як такий, єдиний підхід до вирішення проблеми відсутній. Крім того, труднощі, пов’язані з доступом до даних через їх конфіденційність та приватність, в поєднанні з тим, що структура критичної ІТ-інфраструктури стає різноманітнішою та складнішою, робить проблему перевірку взаємозалежності її компонентів та систем дуже нетривіальною проблемою. Отже, є потреба для подальшого розвитку підходів дослідження взаємозалежності компонентів, систем та цілих інфраструктур і тому тема роботи є перспективною.

5. Методи дослідження

Нехай критична ІТ-інфраструктура С представлена у вигляді сукупності систем і компонент Ω. Тоді, представимо нашу Ω у вигляді РВГА [14]:

$$\Omega = (D, S, S_0, I, O, Z, L, G, T, \tau, F, SP, P, R, V),$$

де D – скінченна множина дискретних станів системи (компоненти) критичної ІТ-інфраструктури Ω. Множина поділяється на наступні множини: D_{sf} – множину безпечних станів, D_{cr} – множину критичних станів та D_t – множину термінальних станів;

S – скінченна множина неперервних станів системи (компоненти) критичної ІТ-інфраструктури Ω. Множина поділяється на наступні множини: S_{sf} – множину безпечних станів, S_{cr} – множину критичних станів та S_t – множину термінальних станів;

$S_0 \subseteq SxD$ – скінченна множина початкових станів, $s_0 \in S_{sf}, d_0 \in D_{sf}$;

$I = \Xi \cup \Psi$ – скінченна множина входів, яка поділяється на: Ξ – множина внутрішніх входів (в рамках одного компонента), Ψ – множина зовнішніх входів (між компонентні входи);

O – скінченна множина вихідних станів.

Запис $(s,d) \in SxD$ описує зміну стану компоненти Ω, яка має:

- початковий стан $S_0 \subseteq SxD$;
- динаміку зміни станів, що описується вектором $\phi : SxDxI \to R^n$;
- функцію виходу $\varphi : SxDxI \to O$;
- множину дозволених станів та входів $Z \to 2^{SxI}$;
- $L \subseteq DxD$ – скінченну множину відміток переходів, що включає спеціальний символ †;
- множину умов $G : L \to 2^{SxI}$, що ініціюють перехід між дискретними станами;
- відношення скидання $T : LxSxS$, що скидає значення входу $s \in S$ перед кожним переходом;

τ – диспетчер часу;

F – розподіл втручань в роботу компонентів;

SP – набір специфікацій;

P – набір політик;

R – набір вимог безпеки;

V – набір вразливостей.

Перехід є детермінованим та відбувається за умовою G у випадку, коли $l \in L \setminus \{\dagger\}$, або ймовірнісним, у випадку, коли $l = \dagger$. В останньому випадку, значення стану формується випадково згідно розподілу F.

Взаємодіючими учасниками в такій моделі є:

- компоненти (телекомунікаційні, промислові і т. ін.);
- системи;
- інфраструктури;
- оператори систем критичної ІТ-інфраструктури;
- супротивники;
- середовище.

Їх логіка функціонування описується наборами специфікацій SP, політиками P та вимогами безпеки R.

Середовище контролює часові та просторові аспекти всіх подій в моделі та диспетчеризує всі зміни станів відповідно до τ, використовуючи для цього розподіли F. Розподіл дає можливість створювати стратегії виходу з ладу доступних компонентів та використовується для вирішення проблем одночасного виникнення подій в критичній ІТ-інфраструктурі та їх обробки.

Таку модель дуже зручно представити у вигляду направленого графу (рис. 1).

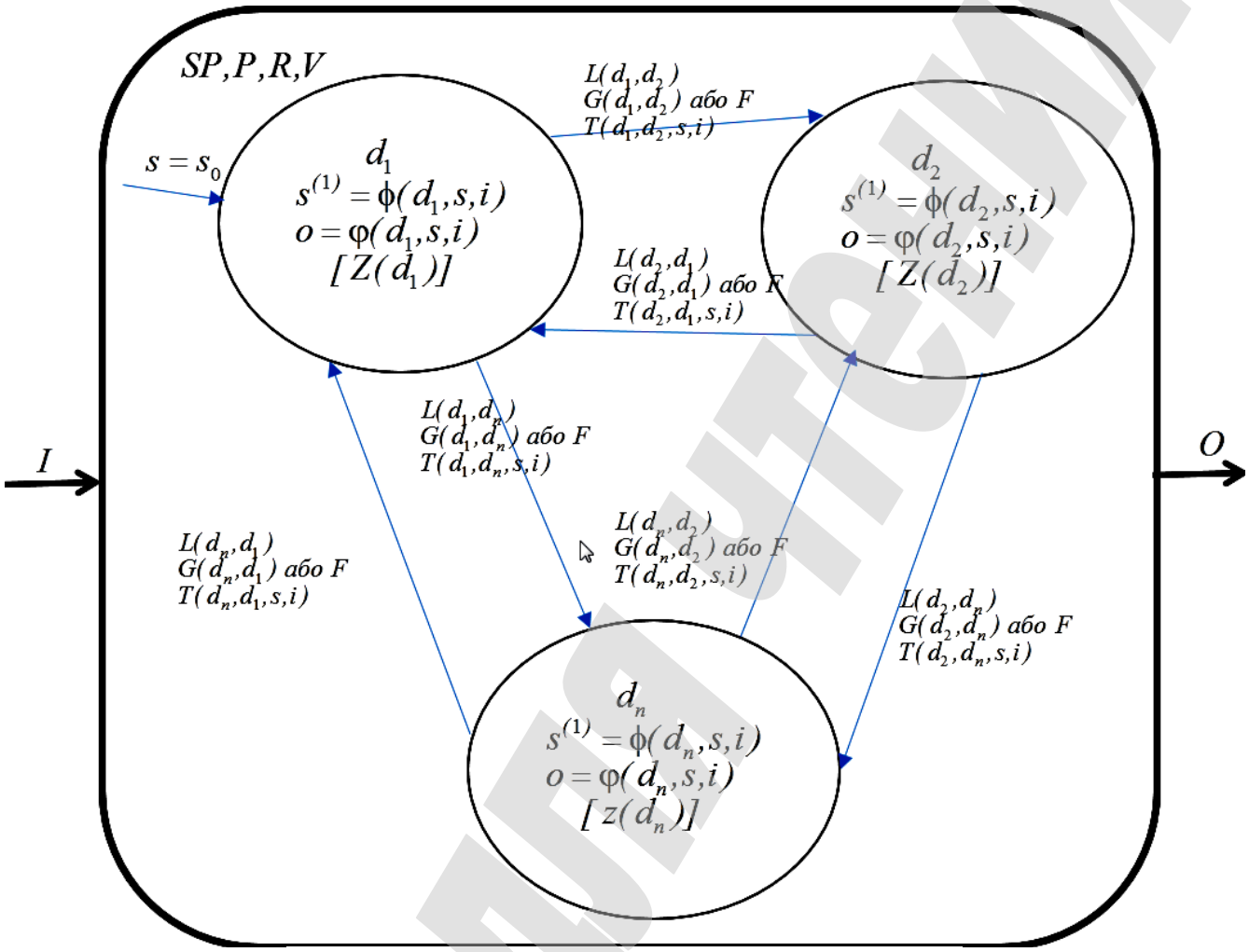

Рис. 1. Модель у вигляді направленого графу

Кожна вершина такого графу представляє собою дискретний стан $d \in D$. Ребра направленого графу представляють собою дискретні переходи між станами. Наприклад, ребро $(d_1,d_2) \in L$ починається в вершині $d_1 \in D$ і закінчується в вершині $d_2 \in D$. Кожний перехід відбувається при виконанні умови $G(d_1,d_2)$ або випадково, якщо $L(d_1,d_2) = \dagger$. В кінці переходу, при зміні значення неперервного стану, відбувається скидання відношення T.

Простий шлях (спрацювання РВГА) складається з послідовності інтервалів τ безперервної еволюції, що змінюються дискретними переходами. Виконання починається з деякого початкового стану $(d_0,s_0) \in S_0$. Модель залишається в дискретному стані d_i доки неперервний стан $s_i \in S$ та/або значення входу $i \in I$ мають допустимі значення Z. В той же час, значення виходу $o \in O$ визначається як $\varphi(s_i,d_i,i)$. Якщо $s_i \in S$ та/або значення входу $i \in I$ досягає умови переходу $G(d_i,d_j)$, то зміна стану відбувається миттєво, а значення безперервного стану визначається шляхом відношення T.

Кожну критичну IT-інфраструктуру можна представити як композицію різних РВГА. На рис. 2 представлена композиція двох РВГА.

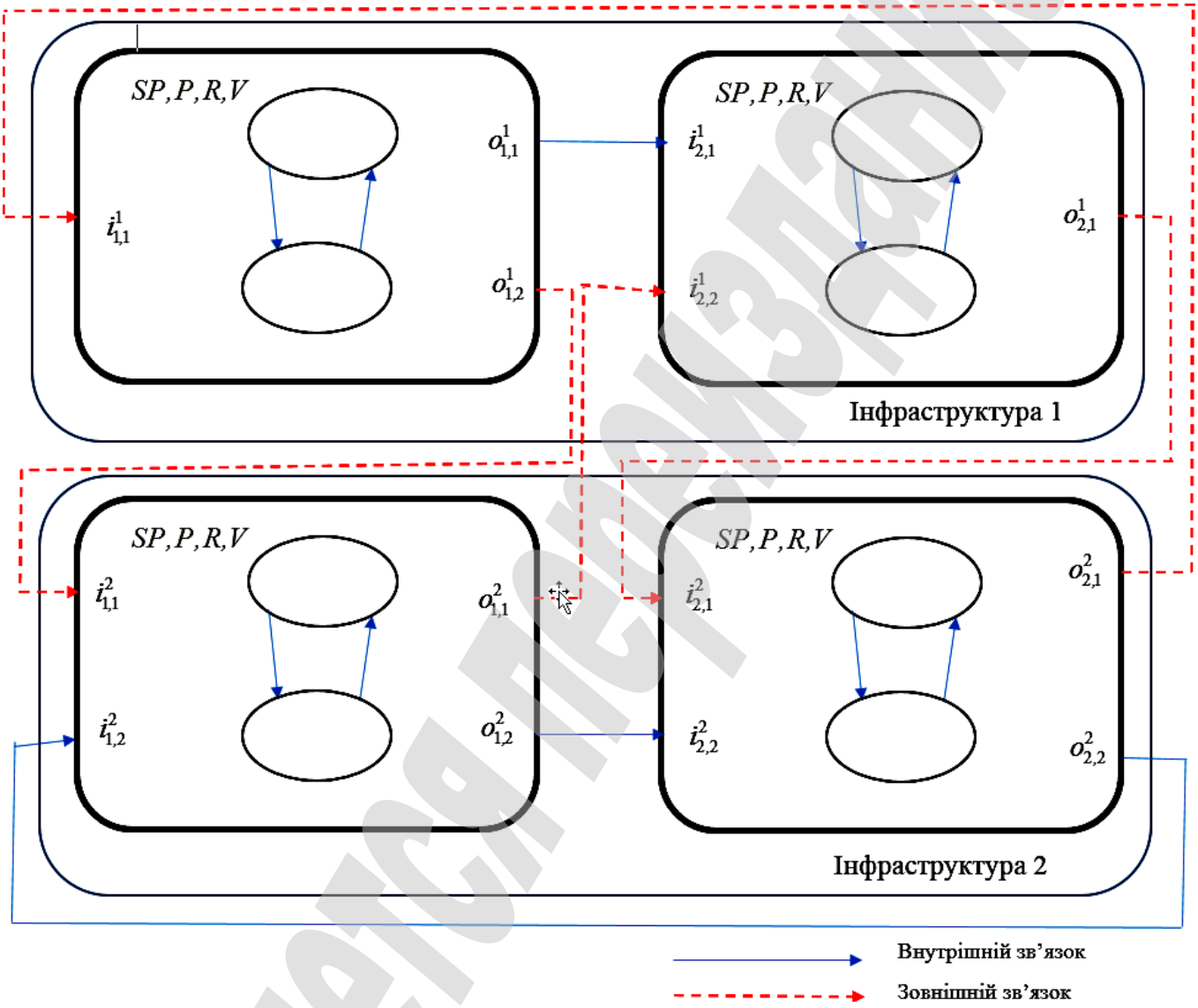

Рис. 2. Композиція автоматів

РВГА ІТС складається з композиції двох елементів:

– центру мережевих операцій (network operation center);

– мережі.

Опишемо модель центру мережевих операцій у термінах РВГА. Модель містить 5 дискретних станів:

– «Звичайний» – стан звичайної роботи центру мережевих операцій (ЦМО);

– «Безперебійне живлення» – стан роботи ЦМО на пристроях безперебійного живлення у випадку відсутності струму в електричній мережі;

– «Помилки охолодження» – стан роботи ЦМО у випадку аварій в системі охолодження обладнання;

– «Критичний» – стан роботи ЦМО у випадку одночасної відмови систем живлення та охолодження;

– «Аварія» – стан ЦМО, у якому подальша робота не можлива через відмови, що сталися.

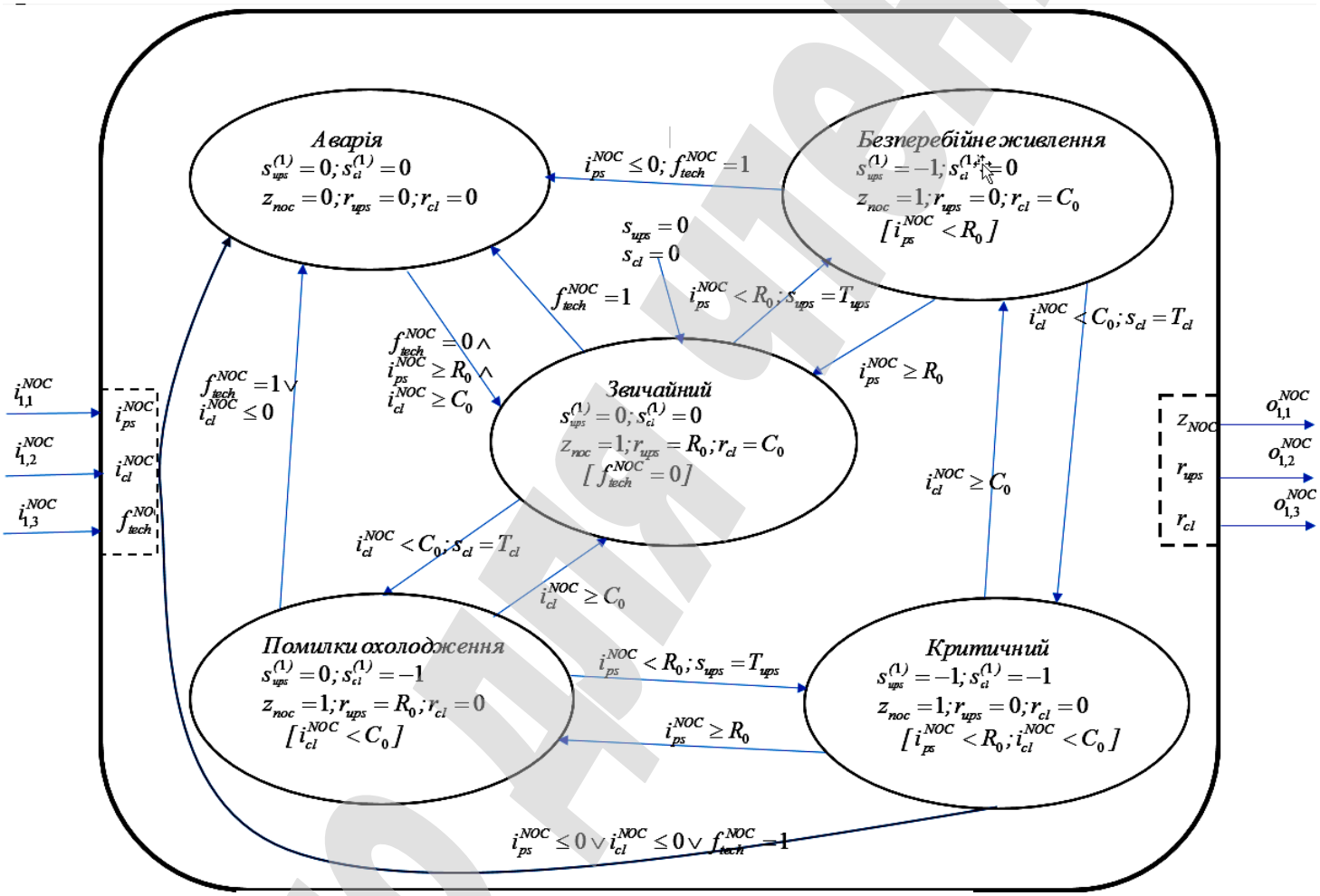

Рис. 3. Модель роботи центру мережевих операцій

Модель має наступні входи (рис. 3):

– i_{ps}^{NOC} – живлення ЦМО;

– i_{cl}^{NOC} – охолодження ЦМО;

– f_{tech}^{NOC} – наявність технічних відмов у ЦМО. Виникнення технічних відмов контролюється розподілом F або самою системою.

Перехід зі стану «Звичайний» в інші стани відбувається при наступних умовах:

– якщо виникла технічна відмова $f_{tech}^{NOC}=1$;

– якщо рівень постачання живлення впав нижче рівня потреби ЦМО $i_{ps}^{NOC}<R_0$;

– якщо рівень постачання хладогену впав нижче рівня потреби ЦМО $i_{cl}^{NOC}<R_0$.

У якості диспетчерів часу в системі виступають значення безперервних станів s_{ups} та s_{cl}. В разі відмови мережі електропостачання система безперебійного живлення може підтримувати роботу ЦМО $s_{ups} = T_{ups}$.

В разі відмови системи охолодження робота ЦМО підтримується ще деякий час, що дорівнює $s_{cl} = T_{cl}$.

Модель також має три виходи:

– статус роботи ЦМО z_{NOC} (z_{NOC} приймає 2 значення: 1 – ЦМО виконує свої функції, 0 – на ЦМО аварія);

– потреба ЦМО в електроживленні r_{ups};

– потреба ЦМО в охолодженні r_{cl}.

Розглянемо наступну модель – модель роботи мережі, що є варіантом моделі з [15]. Модель має три дискретні стани роботи (рис. 4):

– «Звичайний» – мережа працює у штатному режимі;

– «Відмова каналу передачі даних» – відмова одного або декілька каналів передачі даних;

– «Аварія» – мережа повністю відмовила.

Модель мережі має наступні входи:

– i_l^{NET} – мережа працює в штатному режимі, якщо немає відмов каналів передачі даних, тобто $i_l^{NET} = 0$;

– i_{noc}^{NET} – мережа працює у штатному режимі, якщо ЦМО також працює в штатному режимі, тобто $i_{noc}^{NET} = 1$;

– i_{ps}^{NET} – вхід, що отримує дані від системи електропостачання;

– i_{cl}^{NET} – вхід, що отримує дані від системи охолодження;

– i_{pct}^{NET} – вхід, що отримує дані про кількість вхідних пакетів, що потрапляють у мережу.

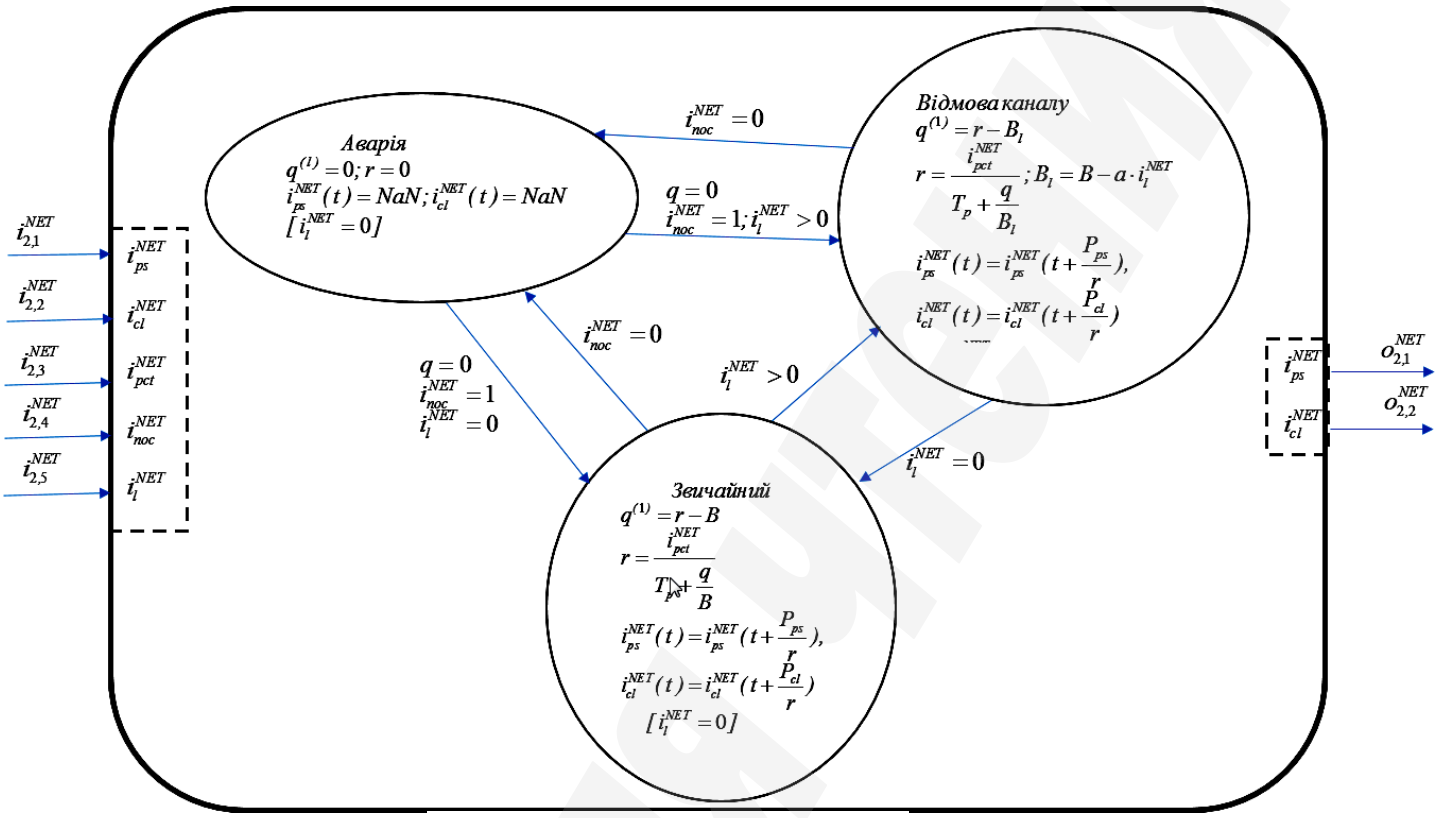

Рис. 4. Модель роботи мережі

Доки мережа працює у штатному режимі, швидкість передачі даних розраховується за формулою:

$$r = \frac{i_{pct}^{NET}}{T_p + \frac{q}{B}}, \tag{1}$$

де i_{ps}^{NET} – кількість пакетів, що входять в мережу; T_p – затримка розповсюдження; q – розмір черги; B – пропускна здатність мережі в пак/с.

Згідно з [14] розмір черги q описується наступним рівнянням динаміки:

$$q^{(1)} = r - B. \tag{2}$$

Дані від систем електропостачання та охолодження подаються в систему з затримкою:

$$i_{ps}^{NET}(t) = i_{ps}^{NET}\left(t + \frac{P_{ps}}{r}\right),$$
$$i_{cl}^{NET}(t) = i_{cl}^{NET}\left(t + \frac{P_{cl}}{r}\right), \quad (3)$$

де P_{ps}, P_{cl} – кількість пакетів, що приходять від конкретної системи.

Таким чином, чим більше трафік в мережі, тим більші затримки розповсюдження. У випадку відмови каналів передачі даних, пропускна здатність мережі зменшується за формулою:

$$B_l = B - a \cdot i_l^{NET}, \quad (4)$$

де a – кількість каналів передачі даних, що відмовили.

У випадку, коли ЦМО в неробочому стані, тобто $i_{noc}^{NET} = 0$, відбувається перехід до стану «Аварія» і на всіх виходах системи маємо значення NaN.

6. Результати дослідження

Для моделювання ЦМО побудована модель в пакеті Simulink/Stateflow (рис. 5). Вказана модель є дуже спрощеною, але достатньою для демонстрації запропонованого підходу для проектування та дослідження складних взаємозалежних систем за допомогою РВГА.

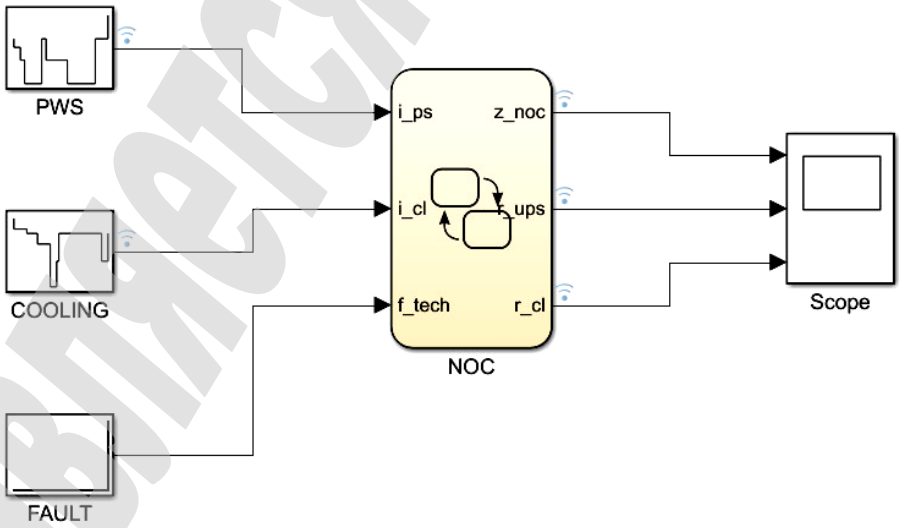

Рис. 5. Модель центру мережевих операцій в Simulink

Діаграма станів моделі ЦМО у StateFlow виглядає наступним чином (рис. 6).

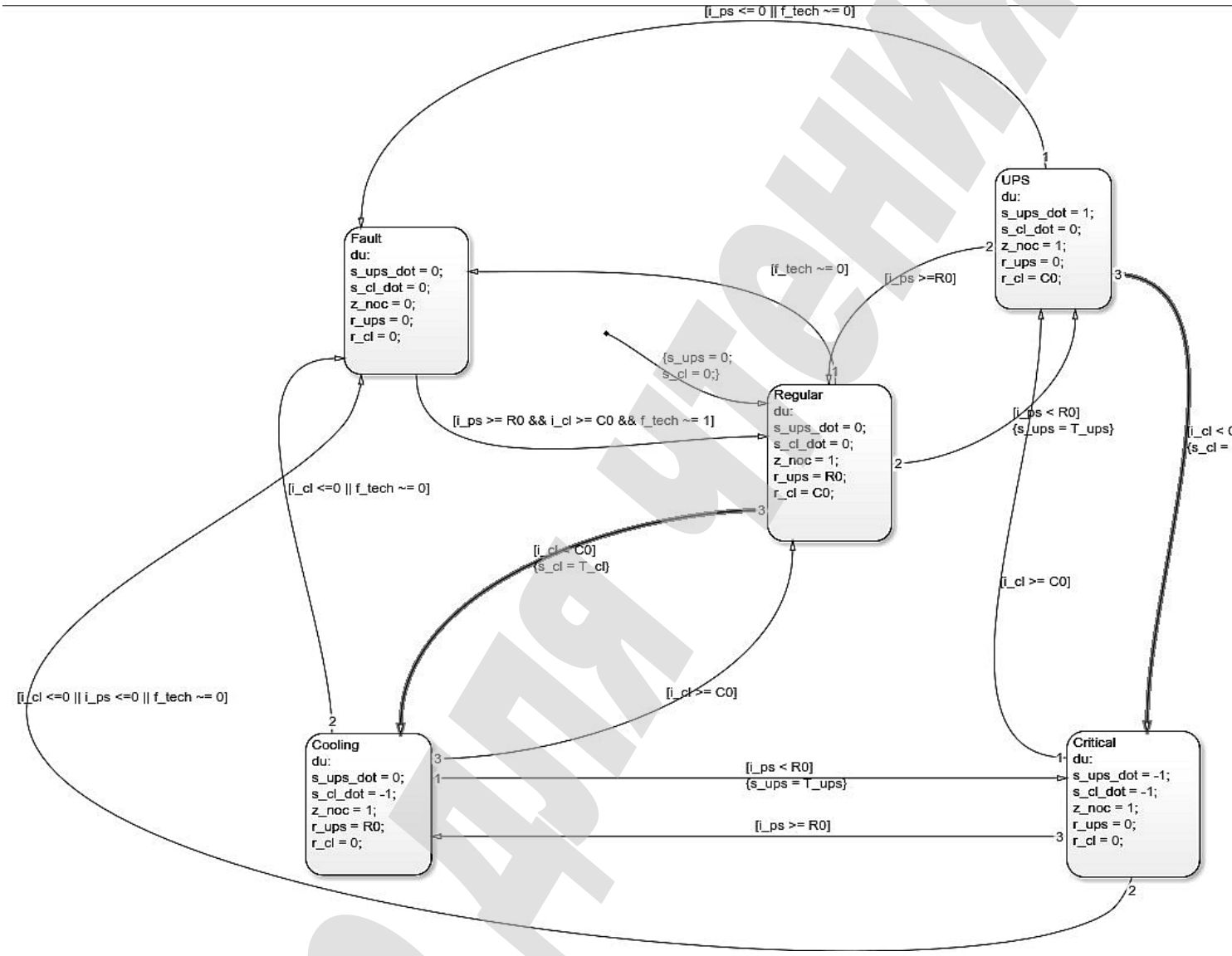

Рис. 6. Модель центру мережевих операцій в Stateflow

Для моделі встановлені наступні значення параметрів:

– $T_{ups} = 20$ с – час, який ЦМО може працювати на джерелах безперебійного живлення;

– $T_{cl} = 10$ с – час, який ЦМО може працювати без системи охолодження;

– $R_0 = 3000$ Вт·час – мінімальний рівень електроенергії, потрібний для роботи ЦМО;

– $C_0 = 2000$ BTU/час – мінімальний рівень потужності охолодження, потрібний для роботи ЦМО.

На часових діаграмах представлені значення параметрів, що подаються на входи побудованої моделі (рис. 7–9).

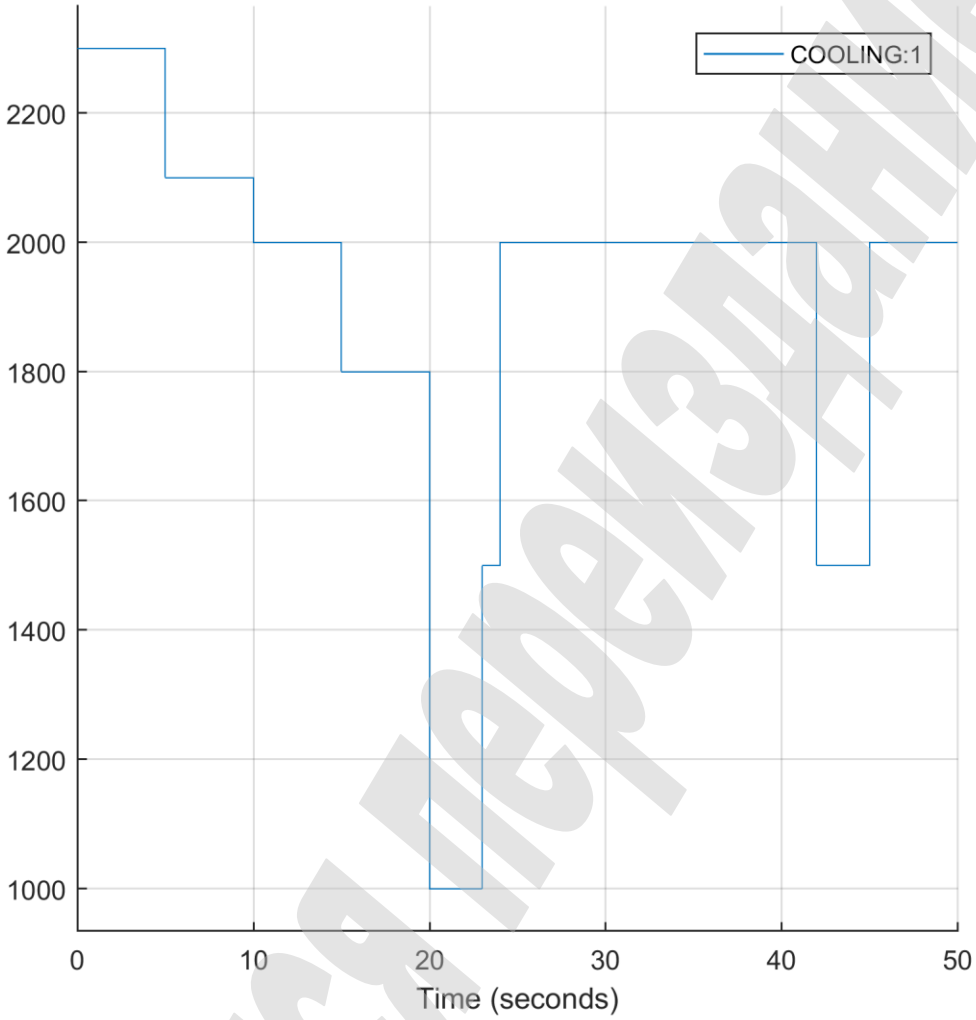

Рис. 7. Діаграма потужності охолодження на вході центру мережевих операцій

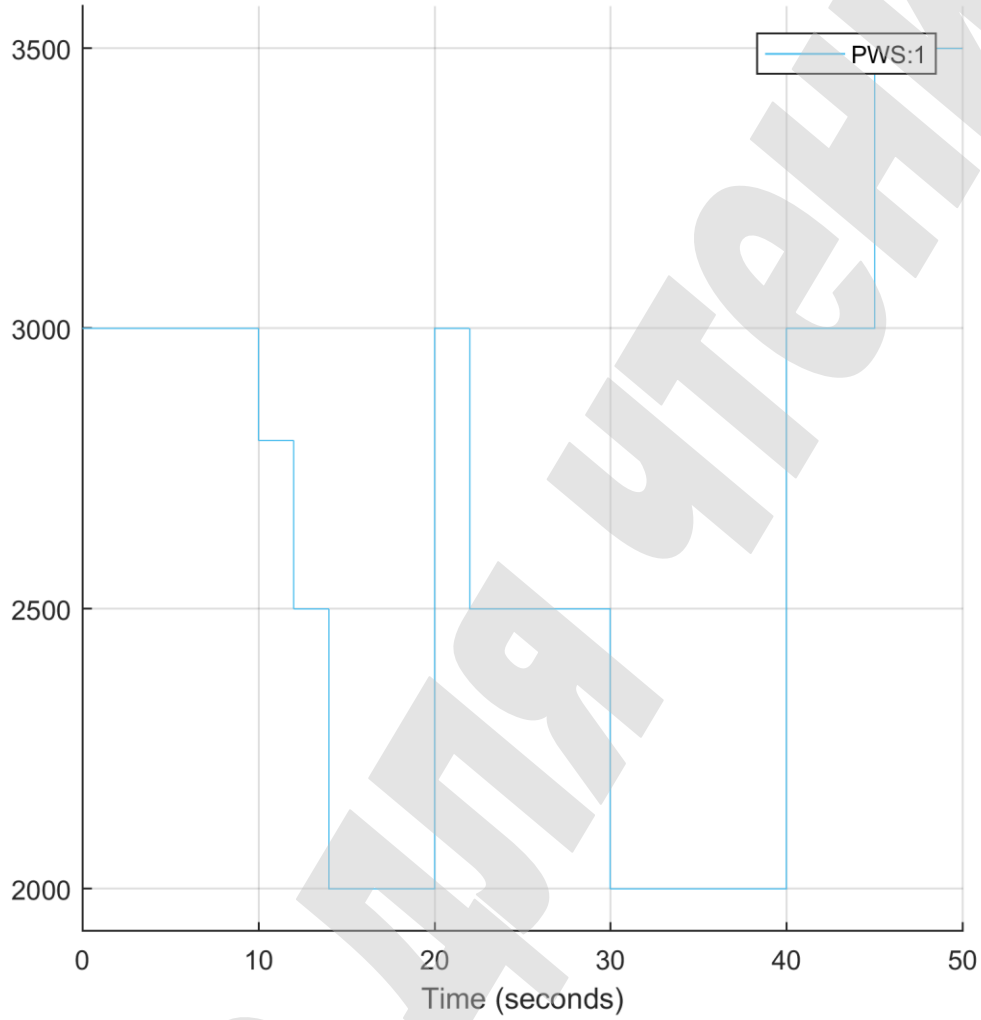

Рис. 8. Діаграма наявності електроенергії на вході центру мережевих операцій

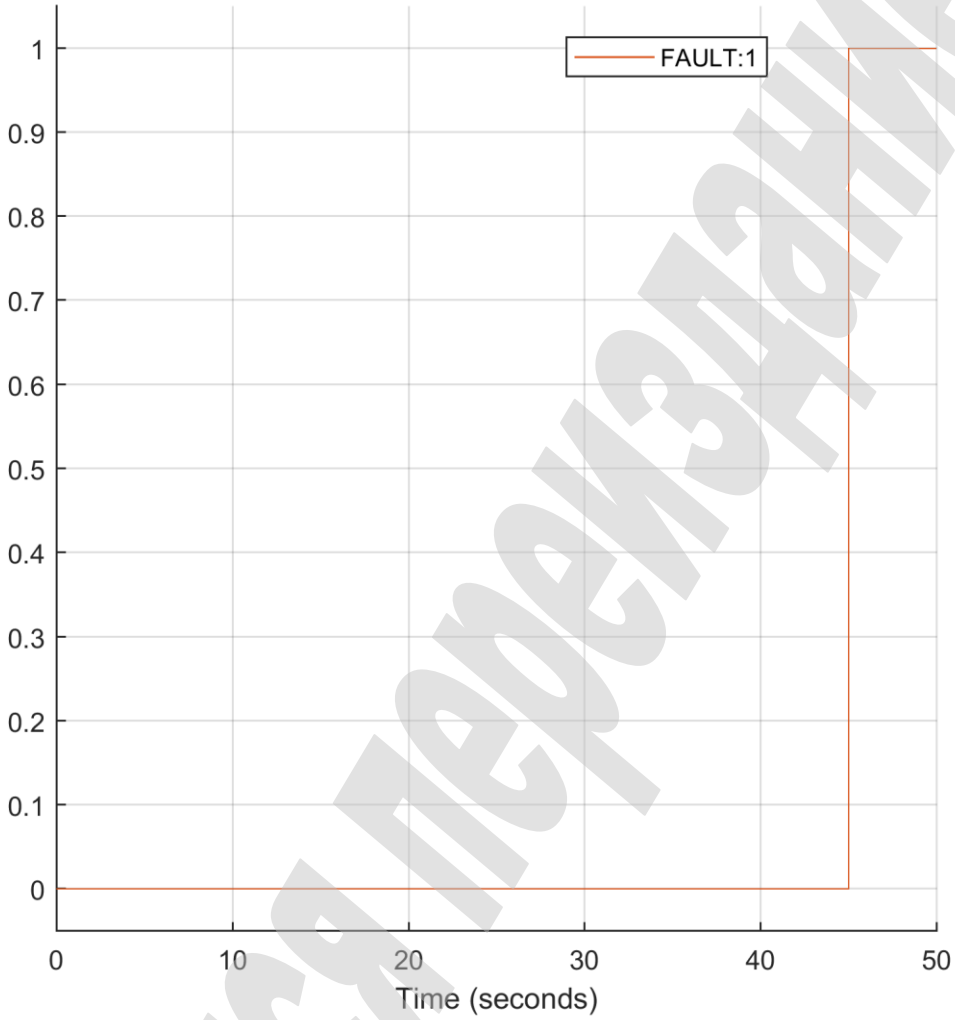

Рис. 9. Діаграма розподілу виникнення технічних відмов на вході центру мережевих операцій

Часові діаграми виходів моделі ЦМО представлені на рис. 10.

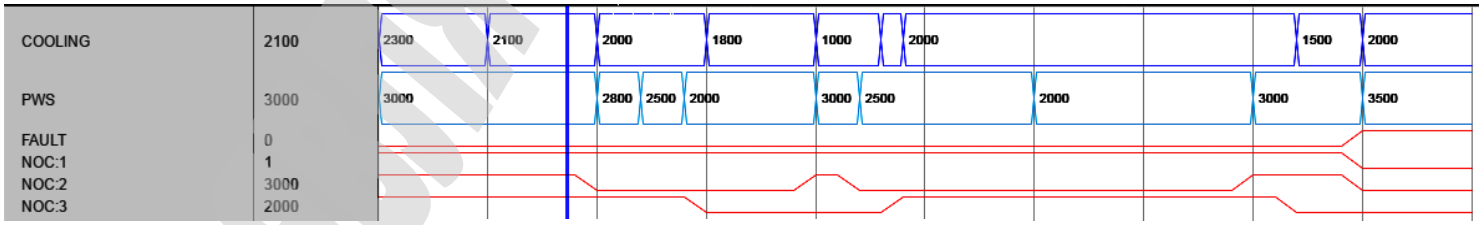

Рис. 10. Часові діаграми виходів

Діаграма на рис. 10 вказує на те, що ЦМО працює у заданому режимі, проходить відповідні стани в залежності від вхідних параметрів, які надходять від інших підсистем моделі.

7. SWOT-аналіз результатів дослідження

Strengths. При роботі з критичними IT-інфраструктурами, масштабованість є однією з проблем, з якою стикаються всі методи, які використовуються для моделювання взаємозалежності. Запропонований підхід є водночас модульним та масштабованим в тому сенсі, що має достатню гнучкість у виборі та використанні як високоточних, так і простих моделей для критичної IT-інфраструктури. Модульність досягається за рахунок використання композиції елементів, тоді як масштабованість представлена у двох формах: масштабованість при побудові моделі (топологія і функціональність) критичної IT-інфраструктури та масштабованість з точки зору обчислювальної потужності, необхідної для запуску моделей. З точки зору моделювання, пропонований підхід дозволяє створювати композиції моделей, які можна далі використовувати як компоненти вищого рівня, які в свою чергу, можуть бути використані для створення компонентів ще вищого рівня тощо. Таким чином, підхід дозволяє накопичувати портфоліо компонентів для багаторазового використання. Наприклад, електричну підстанцію можна представити як набір кількох генераторів. Таким чином, можна побудувати модель одного генератора, а потім повторно її використати для створення моделі електричної підстанції. А якщо додати ще в цей набір вузли безперебійного живлення, то отримаємо модель електричної інфраструктури як частини більш складної критичної IT-інфраструктури. З точки зору необхідної обчислювальної потужності для запуску моделі підхід надає ту ж саму можливість формування необхідного рівня абстракції.

Підхід побудований на використанні розширених відкритих гібридних автоматів (РВГА) і надає всі необхідні інструменти для побудови, планування, дослідження, управління, оцінювання тощо критичних IT-інфраструктур.

Weaknesses. На даному етапі розробки підходу єдиною вадою є наявність дуже спрощених моделей підсистем та компонент критичної IT-інфраструктури.

Opportunities. У майбутньому планується використати запропонований підхід для розробки моделей з різними рівнями абстракції для різних компонентів та підсистем критичної IT-інфраструктури, з кінцевою метою у вигляді створення бібліотеки моделей, яка дозволить вибирати та легко використовувати їх для різних досліджень. Також, майбутньою метою є дослідження шляхів генерації сценаріїв побудови композицій з метою створення великих та надвеликих моделей.

Запропонований підхід та бібліотека моделей для Simulink/Stateflow надасть можливість дослідникам проводити моделювання будь-яких взаємозв’язків між системами, компонентами критичної IT-інфраструктури.

Threats. На даний момент важко передбачити негативні ризики розробленого підходу. Але можна точно сказати, що ніяких додаткових витрат розробник критичної IT-інфраструктури, що буде використовувати пропонований підхід та розроблену в майбутньому бібліотеку моделей нести не буде.

8. Висновки

1. Удосконалений існуючий математичний апарат відкритих гібридних автоматів з метою дослідження критичних IT-інфраструктур. До звичайного відкритого гібридного апарату введені додаткові елементи, що значно розширюють його функціональність. Множина міток переходів $L \subseteq DxD$ дозволяє формувати розмічені транзитивні системи компонент та систем критичної IT-інфраструктури для подальшого їх дослідження на предмет досяжності та безпечності станів. Розподіл F дозволяє додати ймовірнісний характер в поведінку елементів, а набори SP, P, R, V – надати компонентам та системам критичної IT-інфраструктури якісні характеристики.

2. Побудовані спрощені модель деяких компонент критичної IT-інфраструктури та досліджено за їх допомогою можливість використовувати запропонований підхід. Цей підхід дозволяє створювати композиції моделей на основі взаємозалежностей, які існують між ними, об'єднуючи їх у більш складні моделі, і таким чином, утворювати наступні рівні абстракції моделей. На простих моделях перевірена працездатність запропонованого підходу – створені декілька моделей в пакеті Matlab, досліджена їх робота, отримані очікувані результати.

Література

1. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zabezpechennia kibernetychnoi bezpeky Ukrainy [Electronic resource]: Draft Law No. 11125 from August 31, 2012 // Official web portal of the Verkhovna Rada of Ukraine. – Available at: \www/URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=44208
2. Rinaldi, S. M. Identifying, understanding, and analyzing critical infrastructure interdependencies [Text] / S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly // IEEE Control Systems Magazine. – 2001. – Vol. 21, No. 6. – P. 11–25. doi:10.1109/37.969131
3. Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems [Text] / M. Ouyang // Reliability Engineering & System Safety. – 2014. – Vol. 121. – P. 43–60. doi:10.1016/j.ress.2013.06.040
4. Satumtira, G. Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research [Text] / G. Satumtira, L. Duenas-Osorio // Sustainable and Resilient Critical Infrastructure Systems. – Berlin, Heidelberg: Springer, 2010. – P. 1–51. doi:10.1007/978-3-642-11405-2_1
5. Hasan, S. Modeling infrastructure system interdependencies and socioeconomic impacts of failure in extreme events: emerging R&D challenges [Text] / S. Hasan, G. Foliente // Natural Hazards. – 2015. – Vol. 78, No. 3. – P. 2143–2168. doi:10.1007/s11069-015-1814-7
6. Oliva, G. Fuzzy dynamic input–output inoperability model [Text] / G. Oliva, S. Panzieri, R. Setola // International Journal of Critical Infrastructure Protection. – 2011. – Vol. 4, No. 3–4. – P. 165–175. doi:10.1016/j.ijcip.2011.09.003

7. Kaegi, M. Analyzing maintenance strategies by agent-based simulations: A feasibility study [Text] / M. Kaegi, R. Mock, W. Kroger // Reliability Engineering & System Safety. – 2009. – Vol. 94, No. 9. – P. 1416–1421. doi:10.1016/j.ress.2009.02.002

8. Rolik, A. I. Kontseptsiia upravleniia korporativnoi IT-infrastrukturoi [Text] / A. I. Rolik // Visnyk NTUU «KPI». Informatics, operation and computer science. – 2012. – Vol. 56. – P. 31–55.

9. Svendsen, N. K. Graph Models of Critical Infrastructure Interdependencies [Text] / N. K. Svendsen, S. D. Wolthusen // Inter-Domain Management. – Berlin, Heidelberg: Springer, 2007. – P. 208–211. doi:10.1007/978-3-540-72986-0_27

10. Wang, S. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies [Text] / S. Wang, L. Hong, M. Ouyang, J. Zhang, X. Chen // Safety Science. – 2013. – Vol. 51, No. 1. – P. 328–337. doi:10.1016/j.ssci.2012.07.003

11. Gursesli, O. Modeling infrastructure interdependencies using Petri nets [Text] / O. Gursesli, A. A. Desrochers // SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme – System Security and Assurance (Cat. No.03CH37483). – IEEE, 2003. – P. 1506–1512. doi:10.1109/icsmc.2003.1244625

12. Beccuti, M. Quantification of dependencies between electrical and information infrastructures [Text] / M. Beccuti, G. Franceschinis, S. Donatelli, S. Chiaradonna, F. Di Giandomenico, P. Lollini, G. Dondossola, F. Garrone // International Journal of Critical Infrastructure Protection. – 2012. – Vol. 5, No. 1. – P. 14–27. doi:10.1016/j.ijcip.2012.01.003

13. Di Giorgio, A. A Bayesian Network-Based Approach to the Critical Infrastructure Interdependencies Analysis [Text] / A. Di Giorgio, F. Liberati // IEEE Systems Journal. – 2012. – Vol. 6, No. 3. – P. 510–519. doi:10.1109/jsyst.2012.2190695

14. Dorogyy, Ya. Yu. TS-sumisna arkhitektura krytychnoi IT-infrastruktury [Text] / Ya. Yu. Dorogyy // Visnyk NTUU «KPI». Informatics, operation and computer science. – 2016. – Vol. 65.

15. Lee, J. Modeling Communication Networks With Hybrid Systems [Text] / J. Lee, S. Bohacek, J. P. Hespanha, K. Obraczka // IEEE/ACM Transactions on Networking. – 2007. – Vol. 15, No. 3. – P. 630–643. doi:10.1109/tnet.2007.893090