УДК 004.9.005.95 https://doi.org/10.33099/2304-2745/2025-1-84/69-78

Кірпічніков Ю. А., кандидат технічних наук (0000-0001-6893-3569)
Рибидайло А. А., кандидат технічних наук, старший науковий співробітник (0000-0002-6156-469X)
Кондратенко Ю. В., доктор філософії (0000-0002-9575-5101)
Петрушен М. В. (0000-0002-7448-2765)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Модель оцінювання стійкості інформаційної інфраструктури в умовах відсічі збройної агресії

Резюме. На основі аналізу чинників, які впливають на забезпечення функціонування інформаційної інфраструктури, розроблено модель оцінювання стійкості інформаційної інфраструктури, яка має функціонувати в умовах збройної агресії. Обґрунтовано рекомендації стосовно модернізації існуючої інформаційної інфраструктури шляхом її нарощування з урахуванням визначених вимог щодо забезпечення стійкості.

Ключові слова: інформаційна інфраструктура; хмарні технології; стійкість інформаційної інфраструктури; інтеграл Сугено; хмарний провайдер.

Постановка проблеми. Інформаційну інфраструктуру (ІнфІ) Міністерства оборони (МО) України можна представити у вигляді мереже-центричної моделі [1, 2], основою якої є інформаційно-комунікаційна мережа. З метою уникнення несприятливих впливів збройної агресії з боку Російської Федерації (РФ) та інших загроз стосовно належного функціонування ІнфІ, її подальший розвиток проводиться із застосуванням підходу, який передбачає використання “хмарних технологій” для надання простого мережевого доступу за запитом до загального пулу ІТ-сервісів (інфраструктурних, базових та функціональних).

Побудова ІнфІ на основі хмарних технологій передбачає забезпечення її стійкості при виникненні несприятливих впливів на основі перерозподілу ресурсів інформаційно-комунікаційної мережі, використання механізмів резервування, реорганізації та реконфігурації окремих компонентів ІнфІ для обслуговування потоків запитів користувачів. Надання функціональних сервісів є головним призначенням функціонування ІнфІ. Стійкість ІнфІ розглядається як спроможність надання функціональних сервісів. У воєнних умовах це означає здатність ІнфІ підтримувати оперативні дії Збройних Сил (ЗС) України, протистояти ворогу та інтегруватися з партнерами, використовуючи переваги хмар (масштабованість, стійкість, мобільність).

Проблемним питанням реалізації зазначених технологічних рішень та розробки рекомендацій щодо зниження ризиків та загроз функціонуванню ІнфІ МО України є визначення критеріїв та методу оцінювання стійкості. У науковій практиці оцінка стійкості складних інфраструктурних об’єктів проводиться методами математичного моделювання [3, 4]. Виходячи з того, що забезпечення стійкості ІнфІ МО України є критично важливим для підвищення обороноздатності України, розроблення моделі оцінювання стійкості інформаційної інфраструктури в умовах відсічі збройної агресії є актуальною науковою задачею.

Аналіз останніх досліджень та публікацій. Питанням оцінювання характеристик функціонування ІнфІ присвячені праці [4–6], у яких висвітлюються методи забезпечення живучості інформаційно-комунікаційної мережі на основі перерозподілу ресурсів мережі, використання механізмів резервування, реорганізації та реконфігурації для обслуговування потоків вимог при виникненні несприятливих впливів. Розглянуті методи дають змогу оцінити стійкість інформаційно-комунікаційної мережі та підвищити час її життя. Проте чинників, які враховуються, недостатньо для комплексної оцінки стійкості та обґрунтування технологічних підходів для забезпечення функціонування інформаційної інфраструктури МО України в умовах збройної агресії.

Як показав аналіз, підходи щодо оцінки стійкості ІнфІ, та попередження усіх видів несприятливих впливів ще недостатньо розвинуті [7–11]. Результати наведених досліджень внесли певний внесок у теорію

забезпечення стійкості критичних інфраструктурних об'єктів та містять корисні рекомендації стосовно поліпшення їх стійкості до зовнішніх впливів. Проте існує низка чинників, які необхідно враховувати для комплексної оцінки стійкості ІнфІ та обґрунтування технологічних рішень для забезпечення її функціонування в умовах збройної агресії. Це являє собою важливу наукову задачу, яка потребує подальших досліджень.

Постановка задачі. У вербальній формі задачу можна сформулювати наступним чином: на основі аналізу можливих загроз щодо стійкого функціонування ІнфІ та поточних спроможностей ІнфІ стосовно надання необхідних користувачам сервісів потрібно розробити модель оцінювання стійкості ІнфІ та за результатами моделювання надати обґрунтовані рекомендації стосовно забезпечення належного функціонування ІнфІ МО України в умовах несприятливих впливів збройної агресії.

Метою статті є розробка моделі оцінювання стійкості інформаційної інфраструктури в умовах відсічі збройної агресії.

Викладення основного матеріалу. Надання функціональних сервісів ІнфІ МО України на основі хмарних технологій означає визначений рівень надійності, доступності та безпеки, з якими ІнфІ забезпечує виконання своїх завдань через хмарні сервіси. В даній статті наведені ознаки ІнфІ є складовими, що характеризують її стійкість в умовах відсічі збройної агресії. Отже поняття "***стійкість ІнфІ***" можна тлумачити як здатність системи задовольняти потреби користувачів (ЗС та МО України, інші органи сектору безпеки і оборони) у реальних умовах, зокрема під час війни з РФ, з урахуванням специфіки хмарних технологій. Розроблення моделі оцінювання стійкості ІнфІ в умовах відсічі збройної агресії (ведення бойових дій, збройного конфлікту) – це системний процес, який потребує врахування специфіки хмарних рішень, воєнних умов і потреб ЗС України. Модель має бути практичною, вимірюваною та орієнтованою на підвищення стійкості ІнфІ.

Пропонується наступний *методологічний підхід* до оцінювання стійкості ІнфІ:

на основі оцінки впливів на рівень стійкості ІнфІ при реалізації можливих загроз, з урахуванням синергетичного ефекту при їх одночасній дії та поточного складу ІнфІ, за допомогою обраного математичного апарату обґрунтувати рекомендації щодо поліпшення стійкості ІнфІ.

Для наочного сприйняття логіки процесу оцінювання стійкості ІнфІ на рис. 1 наведено порядок (етапи) вирішення поставленого завдання.

Рис. 1. Порядок оцінювання стійкості ІнфІ

Порядок передбачає виконання двох стадій – *розробка моделі* і *проведення моделювання*. Результатом першої стадії є структура моделі, другої – рекомендації щодо поліпшення стійкості ІнфІ МО України.

РОЗРОБКА МОДЕЛІ (перша стадія) – блоки 1-4 (рис. 1).

1. Визначення мети моделі. Метою розробки моделі є обґрунтування технологічних рішень стосовно нарощування ІнфІ для збільшення рівня стійкості ІнфІ в умовах відсічі збройної агресії.

2. Аналіз вимог до надання сервісів та стійкості ІнфІ. Основною вимогою до ІнфІ є її здатність працювати безперебійно в умовах війни, кібератак і фізичних загроз шляхом використання додаткового обладнання, створення резервних центрів обробки даних (ЦОД), а також застосування послуг хмарних провайдерів.

Функціонування ІнфІ, яка побудована з використанням хмарних технологій, включає ряд характеристик, що мають бути враховані при створенні моделі (Табл. 1).

Таблиця 1

Характеристики функціональних сервісів ІнфІ

№	ХАРАКТЕРИСТИКА	ТЛУМАЧЕННЯ
1	**Доступність (Availability)**	Означає, що сервіси ІнфІ завжди доступні для користувачів, навіть в умовах бойових дій чи кібератак. Хмарні технології забезпечують це через резервування даних і розподілену інфраструктуру
2	**Надійність (Reliability)**	Гарантія безперебійної роботи сервісів без збоїв чи втрати даних. Хмарні платформи дозволяють автоматичне відновлення після збоїв (*failover*). Дані не втрачаються при пошкодженні локального сервера
3	**Безпека (Security)**	Оцінка рівня безпеки хмарної інфраструктури та забезпечення захисту від зовнішніх загроз, витоків даних та несанкціонованого доступу. Хмарні рішення включають шифрування, ізоляцію даних і багаторівневий доступ
4	**Швидкість і продуктивність (Performance)**	Визначення швидкодії та продуктивності інформаційних сервісів включає оцінку часу відповіді, швидкість завантаження та обсяг обробки даних. Хмарні технології забезпечують масштабування обчислювальних ресурсів під навантаження
5	**Гнучкість і масштабованість (Scalability)**	Визначення здатності інфраструктури масштабуватися для забезпечення оптимальної продуктивності при збільшенні навантаження. Хмарні технології дозволяють додавати ресурси “на вимогу”
6	**Управління (Management)**	Зручність управління інфраструктурою через інтерфейси адміністрування та інші інструменти управління ресурсами при форс-мажорних обставинах

З Табл. 1 витікає, що, стійкість є комплексною характеристикою належного функціонування ІнфІ, яка включає доступність, надійність, продуктивність, безпеку, гнучкість надання сервісів та управління ІнфІ.

3. Визначення загроз. У Табл. 2 наведено основні загрози, які при їх реалізації можуть вплинути на характеристики функціональних сервісів ІнфІ в умовах збройної агресії.

Таблиця 2

Загрози функціонуванню інформаційної інфраструктури

№	ЗАГРОЗИ	НАСЛІДКИ ВПЛИВУ
1	**Фізичне пошкодження ІнфІ**	Фізичне пошкодження інформаційних мереж, комп'ютерів, серверів та інших пристроїв, які є складовими частинами ІнфІ
2	**Відключення від мережі**	Відключення від мережі операторів електронних комунікацій, хостинг-провайдерів та інших постачальників послуг, що може призвести до відключення частини ІнфІ
3	**Вразливість мережевої безпеки**	Зростання рівня кіберзагроз: кібератаки, хакерські атаки та віруси, що можуть порушити функціонування ІнфІ та зашкодити їй
4	**Втручання в управління**	Може включати: блокування доступу до деяких веб-сайтів та інших дій, що можуть обмежити доступ до інформації та вплинути на функціонування ІнфІ
5	**Недоступність ресурсів**	Відсутність електропостачання та доступу до Інтернету/Інтранету окремих складових ІнфІ може обмежити повноту її функціонування
6	**Недостатність кваліфікованих кадрів**	Відтік кваліфікованих ІТ-спеціалістів може призвести до нестачі кваліфікованих кадрів для підтримки ІнфІ

Врахування впливу, наведених у Табл. 2 загроз на характеристики функціональних сервісів ІнфІ дасть змогу оцінити інтегральну стійкість ІнфІ та врахувати наведені у Табл. 1 характеристики.

4. Визначення структури моделі та методу проведення розрахунків. Загальна структура розв’язання задачі оцінювання може бути подана у вигляді ієрархічної моделі (рис. 2).

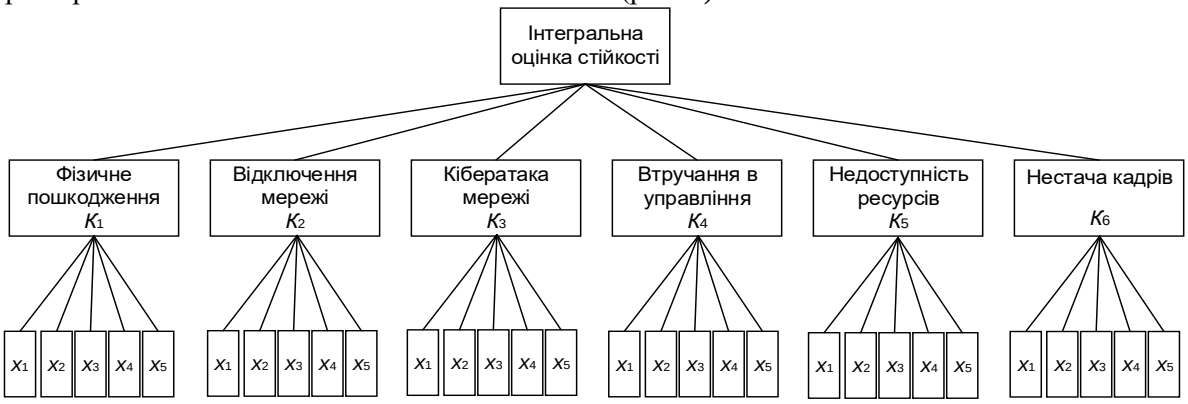

Рис. 2. Модель оцінювання стійкості ІнфІ

У моделі враховуються вплив на функціонування ІнфІ при реалізації загроз: фізичне пошкодження (K_1), пошкодження мережі (K_2), кібератака мережі (K_3), втручання в управління (K_4), недоступність ресурсів (K_5), нестача кадрів (K_6). Отже загрози можна представити множиною $K=\{K_i, i=\overline{1,6}\}$, де K_i – i-та загроза функціонуванню ІнфІ (див. Табл. 2).

Кожна загроза $K_i, i=\overline{1,6}$ може бути оцінена в шкалі лінгвістичних оцінок $X=\{x_j, j=\overline{1,5}\}$, де x_i – лінгвістична оцінка: x_1 – "критична"; x_2 – "суттєва"; x_3 – "середня"; x_4 – "нижче середнього"; x_5 – "не суттєва". Тобто за допомогою шкали X кожна загроза може бути оцінена шляхом опитування експертів.

Застосування інтегралу Сугено. Для визначення стійкості ІнфІ при реалізації загроз використовується оцінка на основі інтегралу Сугено (Sugeno) у вигляді:

$$E=(s)\int_K h(K)\circ\mu(\cdot)=\sup_{\alpha=[0,1]}\{\alpha\wedge\mu(H_\alpha\cap A_m)\}, \quad (1)$$

де $h(K): K\to[0,1]$ – експертні оцінки впливу загроз з множини K на функціонування ІнфІ в залежності від її складу;

$\wedge$ – операція min, $H_\alpha\subseteq K$ – підмножина загроз таких, що $H_\alpha=\{K_i, h(K_i)>\alpha\in[0,1]\}$;

$A_m\subseteq K$ – накопичувальна підмножина загроз;

m – індекс комбінації загроз, $m=\left[\overline{1,M}\right]$;

M – кількість комбінацій, яка визначається при проведенні розрахунків за визначеним сценарієм щодо складу ІнфІ;

$\mu(\cdot): 2^K\to[0,1]$ – нечітка міра Сугено важливості (критичності) загроз усіх підмножин 2^K множини K, яка відповідає λ-правилу:

$$\forall A\cap B=\varnothing,$$

$$\mu(A\cup B)=\mu(A)+\mu(B)+\lambda\cdot\mu(A)\cdot\mu(B), \quad (2)$$

де A і B - підмножини множини K, що не перетинаються;

$\lambda\in[-1,+\infty]$ – параметр міри, а міра $\mu(\cdot)$ - ідентифікується на основі експертних оцінок [12].

Вирішення задачі оцінки стійкості ІнфІ стосовно надання необхідних користувачам сервісів має врахувати можливість одночасної реалізації загроз (див. Табл. 2), тобто виникає необхідність оцінити рівень впливу на стійкість ІнфІ комбінації загроз. Для цього розглянемо підхід до визначення рівня сумарного впливу при одночасній реалізації загроз.

Застосування теорії нечітких мір. Використовується для слабко структурованих задач, коли думки експертів можуть коливатись та для врахування синергетичного ефекту при одночасній реалізації загроз.

При цьому застосовується нечітка міра для кожної загрози $\mu(K_1),...,\mu(K_6)$ і сукупності загроз – комбінації дії кількох загроз (наприклад, $\mu\{K_1,K_2\}$ або $\mu\{K_1,K_2,K_5\}$ тощо). Нечітка міра μ задає "вагу" або "важливість" кожної загрози та їхніх комбінацій у контексті впливу на ІнфІ.

При цьому застосовується інтегрована думка експертів, які є фахівцями щодо можливості реалізації загроз з врахуванням можливостей противника, наявного обладнання і дислокації елементів ІнфІ тощо. Експерти, на основі власного досвіду виставляють свої значення рівнів впливу $h(K_i)$ для визначеного сценарію, та міри окремої загрози $\mu(K_1),...,\mu(K_6)$, або сукупності загроз (наприклад, $\mu\{K_1,K_3\};\mu\{K_2,K_4,K_5\};\mu\{K_2,K_4,K_5,K_6\}$ тощо), які діють одночасно. Інтеграція оцінок експертів може бути здійснена за формулою (1).

Для отримання інтегральної оцінки стійкості ІнфІ за певними сценаріями, для кожного з них формується варіант впливу загроз та формалізується у вигляді функції $h(K_i): K\to[0,1]$, яка визначається експертним шляхом (пряме експертне оцінювання одним експертом) по шкалі:

$$X=\{1.0|x_1,\ 0.8|x_2,\ 0.5|x_3,\ 0.3|x_4,\ 0.1|x_5\} \quad (3).$$

ПРОВЕДЕННЯ МОДЕЛЮВАННЯ (друга стадія) – блоки 5-8 (див. рис. 1) – розробка і реалізація сценаріїв, інтерпретація результатів моделювання, обґрунтування рекомендацій стосовно збільшення стійкості ІнфІ МО України в умовах відсічі збройної агресії.

5. Розроблення сценарію. По-перше, проведемо оцінювання стійкості ІнфІ МО України для базового сценарію – два ЦОД, обидва розміщені в Україні.

Попереднє налаштування моделі. З точки зору експертів, враховуючи наявний склад ІнфІ, оцінки рівня впливу $h(K)$ по

шкалі (3) при реалізації загроз становлять (Табл. 3).

Таблиця 3

Оцінки рівня впливу загроз ІнфІ за базовим сценарієм

K_i	K_1	K_2	K_3	K_4	K_5	K_6
$h(K_i)$	1,0	0,5	0,8	0,3	0,5	0,1
Лінгвістична оцінка	критична	середня	суттєва	нижче середнього	середня	не суттєва

Нечітку міру $\mu(\cdot)$ важливості загроз можемо визначити одним із способів ідентифікації нечіткої міри на основі експертного опитування [12]. Враховуючи критичність для боєздатності ЗС України, частоту реалізації загроз, синергію загроз (наприклад, кібератака + недоступність ресурсів гірші разом), з використанням λ-правила (2) при $\lambda = -0,91$, отримуємо оцінки важливості загроз, як окремо (Табл. 4), так і в їх комбінаціях (Табл. 5).

Таблиця 4

Оцінки важливості загроз ІнфІ за базовим сценарієм

K_i	K_1	K_2	K_3	K_4	K_5	K_6
$\mu(K_i)$	0,6	0,3	0,5	0,2	0,5	0,1
Інтерпретація оцінки	Загроза дуже важлива	Загроза менш важлива	Загроза середня	Загроза менш важлива	Загроза середня	Загроза не суттєва

Таблиця 5

Оцінки важливості комбінації загроз ІнфІ за базовим сценарієм

A_m	K_1, K_2	K_1, K_3	K_3, K_5	K_1, K_2, K_3	K_1, K_2, K_3, K_5	K_1, K_2, K_3, K_4, K_5	$K_1, K_2, K_3, K_4, K_5, K_6$
$\mu(A_m)$	0,7	0,9	0,7	0,95	0,97	0,98	1,0
Інтерпретація оцінки	Загроза дуже важлива	Загроза дуже критична	Загроза дуже важлива	Загроза дуже критична	Синергія загроз	Суттєва синергія загроз	Критична синергія загроз

Зазначені оцінки отримані виходячи з логіки, що: *K1* (фізичне пошкодження) і *K3* (кібератака) мають більшу вагу через пряму загрозу для ІнфІ під час війни.

6. Розрахунок сценарію. Наступним кроком після налаштування моделі є проведення розрахунків:

сортування оцінок по убуванню;

врахування нечітких мір (з Табл. 5);

формування накопичувальних підмножин $A_1 - A_6$;

інтегрування за допомогою інтегралу Сугено (1).

Розрахунок сценарію наведено у Табл. 6, а також у графічному вигляді на рис. 3.

Таблиця 6

Розрахунок стійкості ІнфІ за базовим сценарієм

K_i	A_m	$h(K_i)$	$\mu(A_m)$	$E' = \min\left[h(K_i), \mu(A_m)\right]$
K_1	$A_1 = \{K_1\}$	1,0	0,6	0,6
K_3	$A_2 = \{K_1, K_3\}$	0,8	0,9	0,8
K_2	$A_3 = \{K_1, K_3, K_2\}$	0,5	0,95	0,5
K_5	$A_4 = \{K_1, K_3, K_2, K_5\}$	0,5	0,97	0,5
K_4	$A_5 = \{K_1, K_3, K_2, K_5, K_4\}$	0,3	0,98	0,3
K_6	$A_6 = \{K_1, K_3, K_2, K_5, K_4 K_6\}$	0,1	1,0	0,1
$E = \sup\{\min[h(K_i), \mu(A_m)]\}$				0,8

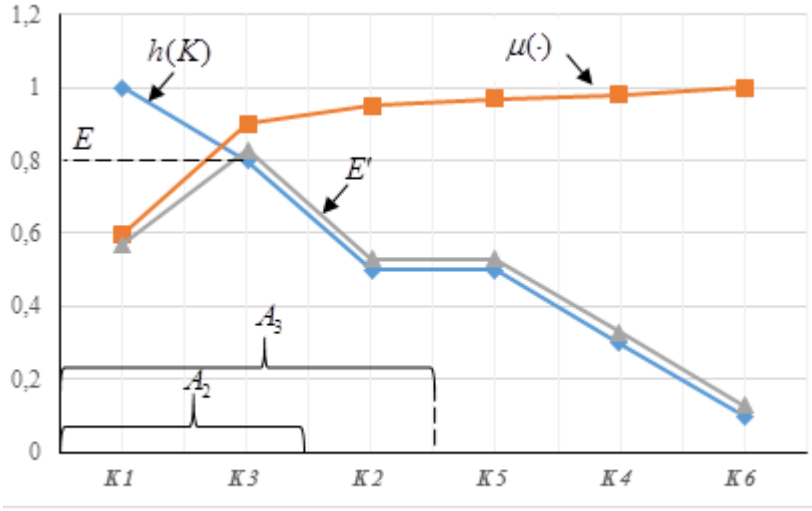

Рис. 3. Обчислення інтегралу Сугено

Отримана інтегральна оцінка $E=0,8\,(80\%)$ означає, що ризик щодо надання сервісів ІнфІ оцінюється на рівні 0,8 з урахуванням загроз. Це відображає суттєвий вплив кібератак K_3, але обмежується вагою комбінацій. Якщо E інтерпретувати як "ризик", то 0,8 – високий рівень уразливості, який потребує заходів.

У наведеному прикладі інтеграл Сугено $E=0,8\,(80\%)$ був розрахований для оцінки стійкості ІнфІ МО України з урахуванням впливу загроз. Його базова інтерпретація – це міра "вразливості" чи "ризику" для ІнфІ, де $E=0,8$ означає суттєвий рівень загрози, що обмежує можливість надання сервісів. Однак інтеграл Сугено через свою гнучкість дозволяє альтернативні інтерпретації, залежно від контексту задачі. Нижче розглянемо можливі інші інтерпретації E при оцінці стійкості ІнфІ.

6. Обговорення результатів моделювання. Модель оцінювання стійкості ІнфІ до визначених загроз може бути використана для вирішення наступних завдань:

оцінки можливості надання сервісів з урахуванням впливу загроз, які виникають при відсічі збройної агресії;

визначення рівня критичності складових ІнфІ з урахуванням їх ваги;

порогова оцінка стійкості ІнфІ;

ступінь готовності до протидії загрозам;

оцінка системного ризику з урахуванням взаємодії загроз;

обґрунтування пріоритетності заходів для підвищення стійкості ІнфІ.

Розглянемо альтернативні інтерпретації результатів моделювання у наведеному прикладі (базовий сценарій).

Рівень критичності найслабшої ланки з урахуванням її ваги показує максимальний рівень впливу, який ІнфІ може витримати, враховуючи найслабшу загрозу в комбінації з її важливістю, тобто це "баланс" між найгіршим сценарієм і його значущістю. У прикладі $E=0,8$ досягнуто на комбінації $\{K_1,K_3\}$ та $\min(0,8;0,9)=0,8$, що вказує на кібератаку як ключовий фактор. У даній інтерпретації замість "загального ризику" увага сфокусована на конкретній загрозі, яка визначає межу стійкості. Це сигналізує, що захист від кібератак – є пріоритетним заходом.

Порогова оцінка стійкості системи – поріг, нижче якого стійкість залишається прийнятною, а вище - ІнфІ не витримує. У прикладі $E=0,8$ може означати, що при впливі загроз на рівні 80% і вище (суттєво/критично) ІнфІ втрачає функціональність, тобто це максимальний "допустимий" вплив, який ще не руйнує систему повністю. Отже інтерпретується як межа стійкості, а не ризик. Отже, якщо $E=0,8$ то при впливі $h(K_1)=1,0$ (критично) система виходить із ладу, але при $h(K_3)=0,8$ (суттєво) ще працює. Потрібно зміцнити стійкість до K_1 (фізичне пошкодження).

Ступінь готовності до протидії загрозам $\bar{E}=1-E$ – рівень підготовленості ІнфІ до нейтралізації загроз або ступінь готовності чи захищеності (обернений показник). Чим вище E тим нижча готовність

системи. При $\bar{E} = 0,2\,(20\%)$ ІнфІ готова лише на 20% протистояти комбінації загроз (наприклад, $K_1 + K_3$). Це означає, що 80% потенційного впливу залишаються неконтрольованими. Потрібні заходи (резервування, шифрування). Отже, увага акцентується на залишковій спроможності, а не на самому впливі.

Оцінка системного ризику з урахуванням взаємодії – міра системного ризику, яка враховує не лише окремі загрози, а й їхню взаємодію. У прикладі $E = 0,8$ досягнуто на $\{K_1, K_3\}$, де синергія фізичного пошкодження та кібератаки створює найбільшу загрозу. Отже, акцент робиться на синергії, а не лише на максимальному впливі.

Пріоритетність заходів для підвищення стійкості – показник, що вказує на загрозу, яку потрібно усунути першочергово для покращення стійкості. У прикладі $E = 0,8$, $h(K_3) = 0,8$ означає, що кібератака – ключовий фактор, який обмежує можливість надання сервісів. Отже розрахунок значення $E = 0,8$ використовується як інструмент для прийняття рішень, а не як оцінювання ризику.

У всіх інтерпретаціях формула інтеграла Сугено однакова, змінюється лише інтерпретація результату.

7. Обґрунтування рекомендацій. Розглянемо деталізацію інтерпретації інтеграла Сугено E у контексті складу ІнфІ МО України. При цьому потрібно реалізувати моделювання в сценаріях, коли нарощування потужності ІнфІ здійснюється шляхом надання одного або двох потенційних хмарних провайдерів, тобто варіюється склад ІнфІ.

Особливостями сучасного стану ІнфІ є: висока вразливість до фізичного пошкодження K_1 через бойові дії; обмежена масштабованість і резервування, що підвищує ризик від загрози K_5 (недоступність ресурсів); середній захист від кібератак K_3, який залежить від локальних засобів.

На сьогодні Україну активно підтримують три потенційні хмарні провайдери: локальний *UCloud* та міжнародні *Azure* і *AWS*, стислий опис характеристик яких наведено у Табл. 7.

Таблиця 7

Характеристики хмарних провайдерів

№	НАЗВА	ОПИС	ПЕРЕВАГИ	НЕДОЛІКИ
1	**UCloud (Україна)**	Містить п'ять дата-центрів (три в Польщі, один у Німеччині, один в Україні). Спеціалізується на надійному зберіганні та обробці даних, працює під час війни	Локальна присутність, розуміння контексту війни. Швидке розгортання для українських клієнтів. Захист від К1 завдяки дата-центрам за кордоном	Менша глобальна масштабованість порівняно з AWS/Azure. Обмежені ресурси для протидії складним кібератакам K_3
2	**Microsoft Azure**	Понад 200 хмарних сервісів, доступ у 116 зонах. Підтримав Україну, мігруючи 16 міністерств у хмару та надаючи $100 млн у 2022–2023 роках	Висока масштабованість і резервування K_5. Посилений захист від кібератак K_3 через Azure Security Center. Сумісність із НАТО (STANAG)	Залежність від зовнішньої інфраструктури (ризик K_2). Вищі ліцензійні витрати і витрати на інтеграцію
3	**Amazon Web Services (AWS)**	Лідер ринку (31% у 2024 році), мігрував 100 українських держреєстрів, надав $75 млн. у 2022 році. Використовує Snowball для фізичного перенесення даних	Глобальна інфраструктура, стійкість до К1 (дані за кордоном). Швидка реакція на кібератаки К3 як у випадку Spectre 2018. Підтримка JADC2 (аналог для ЗС України)	Складність інтеграції з локальними системами МО. Потенційні затримки через зовнішні мережі К2

Постановка задачі. Розроблення рекомендацій щодо доцільності та варіантів нарощування складових інформаційної інфраструктури МО України (два ЦОД + потенційні хмарні провайдери) для підвищення стійкості ІнфІ та якості надання сервісів) з урахуванням загроз $K_1 - K_6$

Альтернативні сценарії наступні:

два ЦОД + *UCloud* – сценарій 1;

два ЦОД + *Azure* + *AWS* – сценарій 2.

Склад ІнфІ впливає на рівень впливу загроз $h(K)$ залежно від топології ІнфІ (ЦОД, хмари). Наприклад, $h(K_1)$ знижується з додаванням хмар за кордоном, $h(K_3)$ може

зрости через зовнішню залежність хмар. Важливість загроз $\mu(A_m)$ коригується залежно від уразливості компонентів. Для ЦОД значення $\mu(K_1)$ вище ніж для хмар, тоді як для хмар вище $\mu(K_3)$.

Розрахунки та інтерпретація.

Сценарій 1 (2 ЦОД+ *UCloud*). Оцінки рівня впливу загроз: $h(K_1)=0,8$ – рівень загрози зменшується за рахунок використання закордонних ЦОД хмарного провайдера; $h(K_3)=0,9$ – рівень зростає через можливість кібератаки мережі хмарного провайдера.

Сценарій 2 (2 ЦОД+ *Azure* + *AWS*). Оцінки рівня впливу загроз: $h(K_1)=0,6$ – рівень загрози зменшується за рахунок використання інфраструктури хмарних провайдерів

Результати оцінки впливу загроз за альтернативними сценаріями наведені в Табл. 8.

Таблиця 8

Оцінки рівня впливу загроз ІнфІ за альтернативними сценаріями

K_i	K_1	K_2	K_3	K_4	K_5	K_6
Сцен. 1 $h(K_i)$	0,8	0,5	0,9	0,3	0,3	0,1
Сцен. 2 $h(K_i)$	0,6	0,4	0,8	0,3	0,2	0,1

Обчислення інтегралу Сугено для двох сценаріїв наведено в Табл. 9.

Таблиця 9

Розрахунок стійкості ІнфІ за альтернативними сценаріями

K_i	A_m	Сцен.1 $h(K_i)$	Сцен.1 $\mu(A_m)$	Сцен.1 E'	Сцен. 2 $h(K_i)$	Сцен. 2 $\mu(A_m)$	Сцен. 2 E'
K_3	$A_1=\{K_3\}$	0,9	0,6	0,6	0,8	0,5	0,5
K_1	$A_2=\{K_3,K_1\}$	0,8	0,85	0,8	0,6	0,7	0,6
K_2	$A_3=\{K_3,K_1,K_2\}$	0,5	0,9	0,5	0,4	0,9	0,5
E				0,8			0,6
$\bar{E}=1-E$				0,2			0,4

UCloud знижує $h(K_1)$, але K_3 залишається проблемою через слабший кіберзахист порівняно з Azure/AWS (див. Табл. 3).

Azure + *AWS* підвищують готовність до 40%, знижуючи $h(K_1)$, і $h(K_5)$, але K_3 потребує додаткового захисту.

Результати моделювання дозволяють запропонувати рекомендації щодо використання хмарних провайдерів.

1. *UCloud* доцільно використовувати при потребі для швидкого резервування і інтегрування некритичних даних (логістика, архіви) за кордоном із мінімальними витратами. Проте, для основних систем резервування і інтегрування даних призводить до посилення ризику K_3 через слабший захист.

2. *Azure* може бути використано для систем із високими вимогами до кіберзахисту K_3 і сумісності з НАТО. Доцільно використати для основних бойових систем, скориставшись досвідом міграції держреєстрів.

3. *AWS* доцільно використовувати для глобального резервування та швидкої реакції на загрози K_1, K_3. При цьому для критичних даних можна застосувати фізичне перенесення через Snowball (досвід 2022 року).

Найбільш раціональним варіантом складу ІнфІ МО України є:

два ЦОД* + *Azure (основна хмара) **+ *AWS*** (резервування).

Така комбінація максимізує готовність (до 40% і вище з додатковим захистом), розподіляє ризики та відповідає стандартам НАТО.

Висновки. На основі розробленої моделі оцінювання стійкості ІнфІ стосовно можливості надання сервісів, яка побудована на основі хмарних технологій, обґрунтовані рекомендації щодо підвищення стійкості ІнфІ в умовах відсічі збройної агресії.

Подальші дослідження доцільно зосередити на розробленні моделі оцінювання кіберзахищеності ІнфІ для обґрунтування відповідних рекомендацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. All that glisters: Is network-centric warfare really scientific? / D. Reid, G. Goodman, W. Johnson, R. Giffin // Defense & Security Analysis. 2005. № 21(4). P. 335–367. DOI: https://doi.org/10.1080/14751790520003454 03.
2. Wilson C. CRS Report for Congress. Network Centric Operations: Background and Oversight Issues for Congress. Washington, D.C : Library of Congress, 2007. 121 p.
3. Деякі аспекти живучості складних гарантоздатних комп'ютерних систем критичних умов застосування / В. Г. Сербін, А. І. Сухомлин // Математичні машини і системи. 2011. № 4. С. 183–191.
4. Аналіз методів підвищення живучості телекомунікаційних мереж / А. А. Зінченко, М. О. Масесов, І. О. Пантась // Сучасні інформаційні технології у сфері безпеки та оборони. 2021. № 2 (41). DOI: https://doi.org/10.33099/2311-7249/2021-41-2-5-10.
5. Мануілов Я.С. Використання технології "блокчейн" у телекомунікаціях. / Я. С. Мануілов // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – Том 32(71).– № 3. – DOI https://doi.org/10.32838/2663-5941/2021.3/20.
6. Грищенко И. В. Метод повышения живучести инфокоммуникационной сети // Холодильна техніка і технологія. 2013. № 6. (146). С. 66–70.
7 Метод обеспечения живучести телекоммуникационной сети на основе перераспределения ресурсов сети / Н. О. Князева, И. В. Грищенко, С. В. Шестопалов // Холодильная техника и технология. 2014. № 4 (150). С. 65–71.
8. Плахотнюк Р. В. Забезпечення стійкості критичної інфраструктури в Україні в умовах сучасних викликів // Економічний простір. 2024. № 195. С. 47–54. DOI: https://doi.org/10.30838/EP.195.47-54
7. Інформаційно-правові аспекти захисту критичної інфраструктури України / С. Г. Гордієнко, І. М. Доронін //. Інформація і Право. 2024. № 3 (50). С. 115–123. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311678.
8. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління / О.І. Яременко, Я.І. Страхніцький // Публічне управління та митне адміністрування. 2022. № 1. С. 76–82. URL: http://customs-admin.umsf.in.ua/archive/2022/1/13.
9. Boin A., McConnell A. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience // Journal of Contingencies and Crisis Management. 2007. Vol. 15, No. 1. P. 50–59. DOI: https://doi.org/10.1111/ j.1468-5973.2007.00504.x
10. Guidotti R., Chmielewski H., Unnikrishnan V., Gardoni P., McAllister T., van de Lindt J. Modeling the resilience of critical infrastructure: the role of network dependencies // Sustainable and Resilient Infrastructure. 2016. Vol. 1, No. 3–4. P.153–168. DOI: https://doi.org/10.1080/23789689.2016.1254999.
11. Sellevåg, Stig Rune. Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies // Security and Defence Quarterly. 2022. Vol. 39, No. 3. P. 6–20. DOI: https://doi.org/10.35467/sdq/146789.
12. Технологія аналізу воєнно-політичної обстановки / В. П. Бочарніков, С. В. Свєшніков, Р. І. Тимошенко, В. І. Павленко. Київ : НУОУ ім. Івана Черняховського, 2019. 384 с.

Стаття надійшла до редакційної колегії 17.04. 2025 року

Model for assessing the stability of information infrastructure in conditions of repelling armed aggression

Annotation

The construction of Information Infrastructure (InfI) based on cloud technologies envisions ensuring its resilience through the redistribution of communication and information network resources, the use of redundancy, reorganization, and reconfiguration mechanisms to service user request flows under adverse conditions.

The provision of functional services is the primary purpose of the functioning of the InfI of the Ministry of Defense of Ukraine. The quality of the functional services provided by the InfI of the Ministry of Defense of Ukraine based on cloud technologies – as a comprehensive characteristic of the proper functioning of the InfI – encompasses availability, reliability, performance, security, flexibility, and cost-efficiency. Under wartime conditions, this means the system's ability to support the operational activities of the Armed Forces of Ukraine, resist enemy actions, and integrate with partners by leveraging cloud advantages such as scalability, resilience, and mobility.

The development of a model for assessing the resilience of the InfI and the quality of service delivery using cloud technologies is a systematic process that requires consideration of the specifics of cloud solutions, wartime conditions, and the needs of the Armed Forces of Ukraine.

Based on the analysis of factors influencing the functioning of the information infrastructure, a model for assessing the resilience of the information infrastructure designed to operate under armed

aggression conditions has been developed. Recommendations have been substantiated regarding the modernization of the existing information infrastructure of the Ministry of Defense of Ukraine through its expansion, taking into account defined requirements – minimizing costs, ensuring resilience, and achieving interoperability with NATO.

Keywords: information infrastructure; cloud technologies; information infrastructure resilience; Sugeno integral; cloud provider.