УДК 004.056:654.026

DOI: 10.18372/2073-4751.78.18967

Сидоренко В.М., к.т.н.,
orcid.org/0000-0002-5910-0837,
e-mail: v.sydorenko@ukr.net,
Положенцев А.А.,
orcid.org/0000-0003-0139-0752,
e-mail: artem.polozhencev@gmail.com,
Сидоренко С.Ю.,
orcid.org/0000-0002-7170-123X,
e-mail: serh.sydorenko@gmail.com,
Скуратівський А.А.,
orcid.org/0009-0000-0566-2394,
e-mail: a.skurativskyi@gmail.com

МЕТОД ВИЗНАЧЕННЯ ПРІОРИТЕТІВ ІТ-ІНЦИДЕНТІВ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Національний авіаційний університет

Вступ

Забезпечення безпеки критичної інфраструктури (КІ) держави є одним із найважливіших напрямів сучасного управління. У світі, де інформаційні технології пронизують усі сфери діяльності, надійність та стійкість ІТ-систем стають основою національної безпеки. Об'єкти критичної інформаційної інфраструктури (ОКІІ) держави вимагають особливої уваги, оскільки їхня вразливість може призвести до масштабних негативних наслідків для економіки, громадської безпеки та стабільності держави.

Актуальність дослідження пріоритетів ІТ-інцидентів зумовлена зростанням кількості та складності загроз у світі, що потребують ефективних методів управління та реагування. ІТ-інциденти, що виникають на об'єктах критичної інформаційної інфраструктури, можуть мати різноманітні причини та наслідки, тому їх правильна класифікація та пріоритизація є необхідною умовою для забезпечення належного рівня захищеності та стійкості.

У даній статті пропонується метод визначення пріоритетів ІТ-інцидентів на об'єктах критичної інформаційної інфраструктури держави, що базується на інтеграції кращих світових практик у сфері управління ІТ-послугами та безпекою. Розроблений метод дозволяє систематично підходити до оцінки загроз, враховуючи їхній вплив на різні аспекти функціонування критичних об'єктів, а також розробляти ефективні стратегії для мінімізації ризиків.

З метою досягнення високого рівня надійності та стійкості ІТ-систем, у статті розглядаються ключові етапи розробленого методу, включаючи ідентифікацію та оцінку загроз, встановлення пріоритетів за допомогою методу попарних порівнянь (*AHP*), а також синтез локальних і глобальних пріоритетів для управління ІТ-безпекою. Описаний підхід дозволяє організаціям адаптувати існуючі методики до специфіки їхньої діяльності, забезпечуючи таким чином більш ефективне управління ризиками та збереження стабільності критичної інформаційної інфраструктури.

Аналіз останніх досліджень та публікацій

Незважаючи на важливість забезпечення ІТ-безпеки КІІ, станом на сьогодні немає достатньої кількості наукових досліджень, щодо розроблення та впровадження методів визначення пріоритетів ІТ-інцидентів, як на міжнародному, так і вітчизняному просторі. Тому, при проведені аналізу, авторами було досліджено підходи щодо управління інцидентами у різних сферах КІ.

У статті [1] представлено систематичний підхід до оцінки ризиків у телекомунікаційних системах, зокрема у внутрішньоплатіжних банківських системах. Основна мета дослідження полягає у побудові та аналізі моделі оцінки ризику реалізації загроз для телекомунікаційних систем, а також у розробці методики оцінки ризику загроз і ефективності засобів захисту даних. У роботі детально розглядається функціональний тип математичних моделей "чорного ящика", побудованих відповідно до методології *IDEF*0 з використанням *Case*-засобу *Bpwin*. Для оцінки економічного збитку при реалізації загроз використовується узагальнена картка експерта-аналітика, яка дозволяє визначити найбільш уразливі місця і оцінити ризики. Модель оцінки ризику враховує конфіденційність, цілісність та доступність даних. Запропонована методика дозволяє обґрунтувати вибір відповідних засобів захисту для критичних систем, включаючи банківські системи та системи управління залізничним транспортом.

У статті [2] розглядається проблема управління кіберризиками в інформаційних системах об'єктів критичної інфраструктури. Основна мета дослідження полягає у розробці методів і моделей оцінки та управління ризиками, зокрема векторної та інтегральної моделей ризику. Векторна модель ризику використовує набір параметрів для визначення рівня ризику, для якого присвоюється ваговий коефіцієнт, і загальний ризик розраховується як векторна сума параметрів з врахуванням їх вагових коефіцієнтів. Ця модель дозволяє ідентифікувати найбільш критичні компоненти ризику та легко візуалізувати і розуміти ризики на різних рівнях системи. Інтегральна модель ризику включає комплексний підхід до оцінки ризиків, враховуючи взаємозв'язки між різними параметрами. На практиці ці системи використовуються для моніторингу та управління кібербезпекою в різних секторах критичної інфраструктури, таких як енергетика, транспорт, охорона здоров'я. Результати дослідження показують, що запропоновані векторна та інтегральна моделі ризику є ефективними інструментами для оцінки та зниження кіберризиків, забезпечуючи надійний захист інформаційних систем критичної інфраструктури від кібервзагроз.

У статті [3] розглядаються математичні методи захисту критичної інфраструктури від небажаних інцидентів. Основна мета дослідження полягає у створенні шаблону для аналізу та покращення захисту та стійкості критичної інфраструктури. Оцінка інцидентів включає моделі ймовірності відмови компонентів системи та очікуваних втрат від таких відмов. Для кібербезпеки розглядаються методи оцінки вразливостей і часу реагування на інциденти. Метрики стійкості охоплюють індекс стійкості, що вимірює здатність системи до відновлення після збоїв, та цільовий час відновлення, що визначає максимально допустимий час простою системи. Застосування цих математичних методів дозволяє кількісно оцінювати інциденти, оцінювати ефективність заходів кібербезпеки та покращувати співпрацю між зацікавленими сторонами, що підтверджує практичну цінність розроблених методів для ефективного управління захистом критичної інфраструктури.

У статті [4] представлено модель індексу ризику для пріоритизації інцидентів безпеки. Модель оцінює індекс ризику для кожного інциденту на основі показників, отриманих з середовища активів та характеристик інцидентів. Основними факторами моделі є вплив на актив та ймовірність загроз і вразливостей, які додатково оцінюються за допомогою показників, таких як критичність, підтримуваність, замінність, надійність та контроль. Розподіл показників на основні та бажані дозволяє точно оцінювати інциденти та впроваджувати динамічні зміни індексу ризику для покращення процесу пріоритизації.

У статті [5] представлено розробку алгоритму, призначеного для пріоритизації кібервзагроз у системі кібербезпеки, враховуючи їх високу ймовірність реалізації. Основна мета дослідження полягає у створенні алгоритму, що включає ієрархічну

модель системи кібербезпеки з трьома рівнями: кібербезпека, загрози та ризики. У статті детально розглянуто метод аналізу ієрархій (*AHP*), який дозволяє оцінювати та порівнювати пріоритети загроз. Ключові кіберзагрози, такі як трояни, віруси та хробаки, мають найвищі пріоритети, що потребують зосереджених заходів для їх пом'якшення. Результати дослідження підтверджують практичну цінність розробленого методу, який допомагає систематично пріоритизувати загрози та ефективно керувати кібербезпекою.

Отже, в табл. 1 пропонується порівняти вище описані підходи, які можна застосувати для розробки методу визначення пріоритетів ІТ-інцидентів за наступними критеріями: простота використання (*EU*), фокус на критичну інфраструктуру (*CI*), об'єктивність (*OB*), можливість застосування для ІТ-інцидентів (*IT*).

Таблиця 1. Порівння підходів щодо пріоритизації ІТ-інцидентів

Підход/критерій	*EU*	*CI*	*OB*	*IT*
Метод оцінювання ризику реалізації загроз безпеки у телекомунікаційних системах	-	+	+	-
Метод оцінювання ризиків кібербезпеки інф. систем ОКІ	-	+	+	-
Методологія для ранжування кіберсценаріїв та критичних об'єктів	-	-	+	-
Метод індексу ризику (*RIM*)	-	-	+	+
Метод оцінки пріоритетів системи кібернетичної безпеки	+	+	+	-

Таким чином, з табл. 1 видно що метод, розроблений авторами у дослідженні [5] є кращим підходом на основі якого можна розробити метод визначення пріоритетів ІТ-інцидентів для забезпечення безпеки КІІ оскільки він є простим у використанні, завдяки чіткій ієрархічній моделі, яка робить процес оцінки інцидентів зрозумілим і доступним для користувачів, включає конкретні механізми для оцінки і пріоритизації загроз саме для ОКІІ, а використання методу аналізу ієрархій надає об'єктивність в оцінці загроз, оскільки дозволяє систематично і прозоро порівнювати та ранжувати загрози на основі встановлених критеріїв.

Мета цієї статті – розроблення і дослідження методу визначення пріоритетів ІТ-інцидентами на ОКІІ.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1. Проаналізувати існуючі підходи до визначення пріоритетів ІТ-інцидентів та визначення їх переваг та недоліків;

2. Розробити метод визначення пріоритетів ІТ-інцидентів на ОКІІ, базуючись на методі аналізу ієрархій (далі – MAI), для забезпечення надійності та стійкості функціонування КІІ.

3. Дослідити експериментально розроблений метод визначення пріоритетів ІТ-інцидентів на ОКІІ.

Метод визначення пріоритетів ІТ-інцидентів на ОКІІ держави

Розроблений метод складається з наступних етапів:

Етап 1. Визначення структури управління ІТ-інцидентами об'єкта критичної інформаційної інфраструктури.

На цьому етапі необхідно створити структуру для управління ІТ-інцидентами, що включає визначення ключових інцидентів та їх класифікацію наприклад, проблеми з фізичними пристроями, програмним забезпеченням, інциденти безпеки, тощо, а також створити відповідну ієрархічну модель.

Етап 2. Оцінка інцидентів та їхніх пріоритетів як на локальному, так і на глобальному рівнях в системі ІТ безпеки

На даному етапі необхідно оцінити пріоритетність кожного ІТ-інциденту, враховуючи його вплив на різні рівні (локальний та глобальний) ІТ-безпеки,

застосувавши метод попарних порівнянь (*AHP*) [6-7] для оцінки впливу кожного інциденту, обчислити локальні та глобальні пріоритети загроз, щоб визначити найбільш критичні для управління та мінімізації ризиків.

Етап 3. Проведення порівнянь елементів системи IT безпеки на різних рівнях для оцінки їх впливу та встановлення пріоритетів за допомогою методу попарних порівнянь (*AHP*).

Крок 3.1. Побудова матриць парних порівнянь

На цьому кроці необхідно сформувати матрицю парних порівнянь, яка дозволяє оцінити відносну важливість кожного критерію чи альтернативи в системі. Цей крок забезпечує структуру для проведення подальших розрахунків. Для цього створюємо матрицю A розміром $n \times n$, де кожен елемент a_{ij} представляє відношення важливості між критерієм i та критерієм j. Елементи матриці розташовані таким чином:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1i} \\ \vdots & \ddots & \vdots \\ a_{1j} & \cdots & a_{ij} \end{pmatrix} \quad (1)$$

де, A – матриця попарних порівнянь, a_{ij}– елементи матриці парних порівнянь.

Крок 3.2. Нормалізація матриць парних порівнянь

На цьому кроці необхідно провести нормалізацію матриць парних порівнянь, щоб забезпечити, що сума всіх елементів у кожному стовпці матриці дорівнює 1. Це дозволяє порівняти різні критерії та їхні ваги на основі єдиної шкали.

$$a'_{ij} = \frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} \quad (2)$$

де, a'_{ij}– нормалізований елемент матриці парних порівнянь, a_{ij} – початковий елемент матриці парних порівнянь.

Після нормалізації всіх елементів матриці отримуємо нормалізовану матрицю A':

$$A' = \begin{pmatrix} a'_{11} & \dots & a'_{1i} \\ \vdots & \ddots & \vdots \\ a'_{1j} & \cdots & a'_{ij} \end{pmatrix} \quad (3)$$

де, A' – нормалізована матриця попарних порівнянь, a'_{ij} – нормалізований елемент матриці парних порівнянь

Крок 3.3. Обчислення векторів ваг, та вектору Ax

На цьому кроці ми обчислюємо вектори ваг W для кожного критерію на основі нормалізованої матриці парних порівнянь A', що необхідно для визначення відносної важливості кожного критерію та для подальшого аналізу їхнього впливу на загальний результат.

$$W_i = \frac{1}{n} \sum_{j=1}^{n} a'_{ij} \quad (4)$$

де, W_i – вагового коефіцієнта для i-го критерію, a'_{ij} – нормалізований елемент матриці парних порівнянь, n – кількість критеріїв.

Для розрахунку вектору, який представляє відносну важливість кожного критерію і буде використаний для подальших розрахунків, скористаємось наступною формулою:

$$W = \begin{pmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{pmatrix} \quad (5)$$

де, W – це вектори ваг критеріїв порівняння.

Далі, для оцінки узгодженості матриці парних порівнянь і точності визначених вагових коефіцієнтів, що є критично важливим для прийняття обґрунтованих рішень у методі аналізу ієрархій, необхідно розрахувати вектор Ax:

$$Ax = A \times W \quad (6)$$

де, A – початкова матриця парних порівнянь, W – вектор ваг.

Отже, вектор Ax допомагає нам зрозуміти, як кожен критерій впливає на загальний результат, враховуючи відносну важливість кожного критерію.

Крок 3.4. Розрахунок індексу та коефіцієнту узгодженості

На цьому кроці необхідно розраховувати індекс узгодженості та коефіцієнт узгодженості для перевірки консистентності матриці парних порівнянь, що є важливим

кроком для оцінки надійності прийнятих рішень на основі вагових коефіцієнтів.

Для перевірки консистентності матриці парних порівнянь, що забезпечує логічну узгодженість і надійність визначених вагових коефіцієнтів, розрахуємо найбільше власне число:

$$\lambda \frac{1}{n} \sum_{i=1}^{n} \frac{(Ax)_i}{W_i}_{max} \quad (7)$$

де, λ_{max} – найбільше власне число, n – кількість критеріїв, Ax – елементи векторів, W_i – елементи вектора ваг.

Індекс узгодженості визначає, наскільки узгодженою є матриця парних порівнянь:

$$CI = \frac{\lambda_{max}}{n-1} \quad (8)$$

де, CI – індекс узгодженості, λ_{max} – найбільше власне число, n – кількість критеріїв.

$$CR = \frac{CI}{RI} \quad (9)$$

де, CR – коефіцієнт узгодженості, CI – індекс узгодженості, RI – випадковий індекс узгодженості, залежить від кількості критеріїв і визначається таблицею для відповідних значень n.

- Якщо $CR < 0.1$, – матриця парних порівнянь вважається узгодженою.
- Якщо $CR \geq 0.1$, це означає, що матриця має значні розбіжності і потребує перегляду парних порівнянь для досягнення кращої узгодженості.

Цей крок є критичним для забезпечення надійності та обґрунтованості прийнятих рішень, оскільки дозволяє виявити і усунути можливі невідповідності в матриці парних порівнянь.

Етап 4. Синтез локальних і глобальних пріоритетів для системи ІТ-безпеки

На цьому етапі необхідно синтезувати локальні і глобальні пріоритети для системи ІТ-безпеки, що дозволить визначити загальну важливість кожного альтернативного рішення з урахуванням ваг критеріїв та їхніх пріоритетів.

Для кожного критерію C_i визначаємо локальні пріоритети альтернатив A_j. Локальний пріоритет альтернативи A_j за критерієм C_i позначається як $W_{Ci, Aj}$.

Глобальний пріоритет альтернативи A_j обчислюється як сума добутків ваг критеріїв на локальні пріоритети відповідних альтернатив. Формула для обчислення глобального пріоритету виглядає наступним чином:

$$G_{A_j} = \sum_{i=1}^{m} (W_{C_i} \times W_{C_i,A_j}) \quad (10)$$

де, G_{A_j} – глобальний пріоритет альтернативи A_j, W_{C_i} – вага критерію C_i, W_{C_i,A_j} – локальний пріоритет альтернативи A_j за критерієм C_i, m – кількість критеріїв.

Після обчислення глобальних пріоритетів для кожної альтернативи, ми отримуємо вектор глобальних пріоритетів, що дозволяє визначити загальну важливість кожної альтернативи у системі ІТ-безпеки та зробити обґрунтовані висновки щодо вибору найбільш пріоритетних альтернативних рішень для системи ІТ-безпеки. Альтернатива з найвищим глобальним пріоритетом має найбільшу важливість і повинна отримати пріоритет при реалізації.

Етап 5. Отримання результатів оцінки та коригування пріоритетів ІТ-безпеки

На цьому етапі необхідно обчислити остаточні результати оцінки пріоритетів для системи ІТ-безпеки та при необхідності коригуємо ці пріоритети. Це забезпечує точне і обґрунтоване визначення найважливіших аспектів для захисту критичної інформаційної інфраструктури.

$$\begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{n1} & a'_{n2} & \cdots & a'_{nn} \end{pmatrix} \times \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} a'_{11}w_1 + a'_{12}w_2 + \cdots + a'_{1n}w_n \\ a'_{21}w_1 + a'_{22}w_2 + \cdots + a'_{2n}w_n \\ \vdots \\ a'_{n1}w_1 + a'_{n2}w_2 + \cdots + a'_{nn}w_n \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{pmatrix} \quad (11)$$

де, a_{ij} – елемент матриці парних порівнянь, а i – номер рядка, j – номер стовпця, a'_{ij} – нормалізований елемент матриці парних порівнянь, w_1, w_2,… w_n – вагові коефіцієнти (пріоритети), що визначаються для кожного критерію, Y_1, Y_2,… Y_n – результати, отримані після множення нормалізованої матриці на вектор вагових коефіцієнтів.

Отримані результати Y_1, Y_2,… Y_n відображають відносну важливість кожного критерію або альтернативи в контексті ІТ-безпеки. Аналіз цих результатів дозволяє визначити, які аспекти потребують найбільшої уваги і ресурсів для забезпечення ефективного захисту.

На основі отриманих і скоригованих результатів приймаються рішення щодо пріоритетних напрямків захисту щодо ІТ-інцидентів. Це допомагає ефективно розподілити ресурси і зосередитися на найбільш критичних аспектах захисту критичної інформаційної інфраструктури.

Схема реалізації розробленого методу відображена на рис. 1:

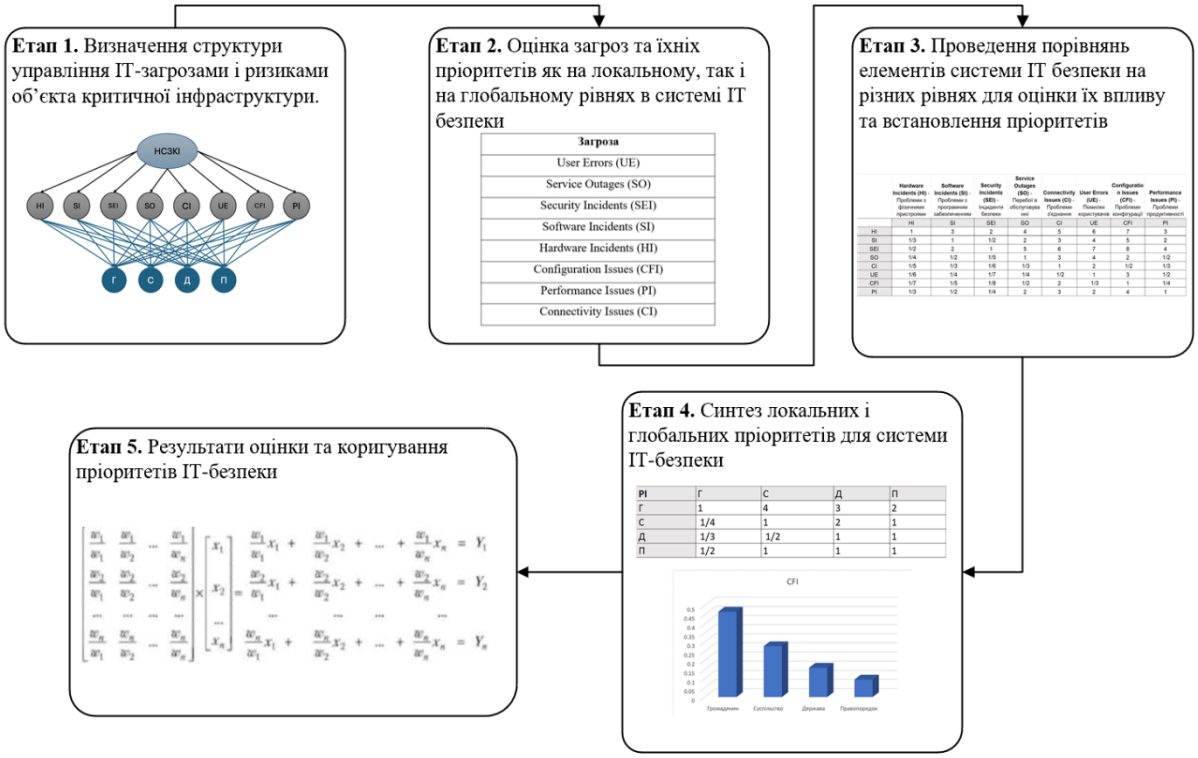


Рис. 1. Схема реалізації методу визначення пріоритетів ІТ-інцидентів

Експериментальне дослідження методу

Для експериментального дослідження розробленого методу, застосуємо його для сектору КІ «Інформаційні послуги», підсектору «засоби масової інформації», до якого відноситься, наприклад, надання послуг у сфері телебачення та радіомовлення [8-9].

Етап 1. У нашій моделі перший рівень ієрархії має одну мету: надійність та стійкість захисту КІІ (НСЗКІ). Значення її пріоритету приймається рівним одиниці.

Далі, для формування другого рівня ієрархії, пропонується, відповідно проведеного аналізу застосувати міжнародний стандарт *ITIL* [10].

Саме тому, другий рівень ієрархії включає різні види загроз, класифіковані за *ITIL*:

- проблеми з фізичними пристроями (*Hardware Incidents*);
- проблеми з програмним забезпеченням (*Software Incidents*);
- інциденти безпеки (*Security Incidents*);

- перебої в обслуговуванні (*Service Outages*);
- проблеми з'єднання (*Connectivity Issues*);
- помилки користувачів (*User Errors*);
- проблеми конфігурації (*Configuration Issues*);
- проблеми продуктивності (*Performance Issues*).

Пріоритети цих загроз розраховуються за допомогою матриці попарних порівнянь загроз щодо НСЗКІ у спосіб порівняння елементів другого рівня ієрархії відносно першого рівня.

Третій рівень ієрархії охоплює вплив на громадянина, суспільство, державу і правопорядок. Оцінка впливу загроз на ці три категорії також здійснюється за допомогою матриці попарних порівнянь, що дозволяє визначити пріоритети загроз для кожної категорії.

Отже, структуру управління ІТ-інцидентами на ОКІІ можна зобразити наступним чином (рис. 2).

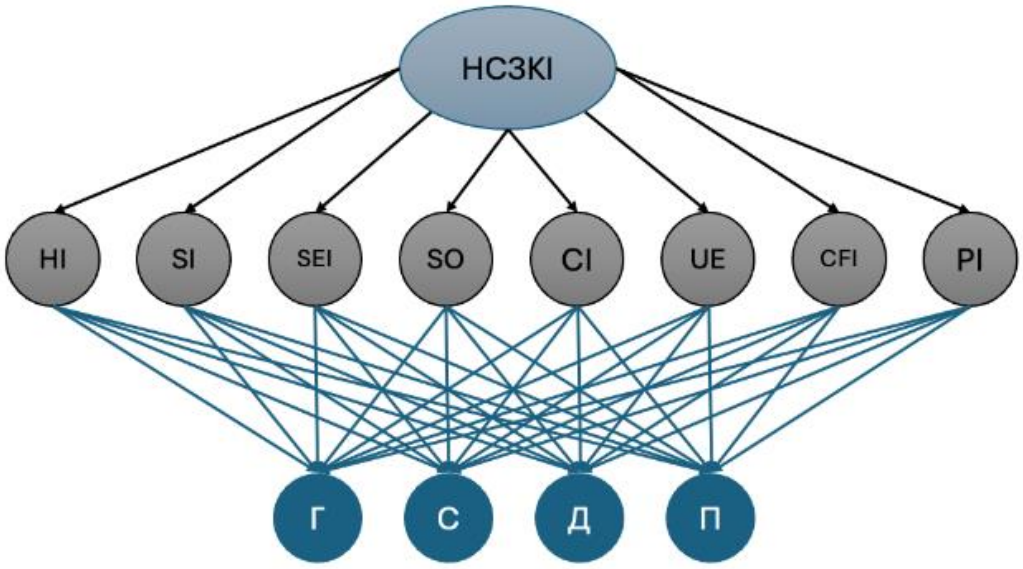


Рис. 2. Структура управління ІТ-інцидентами на ОКІІ

Етап 2. Оцінки в матриці Сааті виставлені на основі відносної важливості загроз для забезпечення надійності та стійкості критичної інформаційної інфраструктури (НСЗКІ). Вони враховують можливий вплив кожної загрози на загальний рівень безпеки та функціональність системи:

Етап 3. Відповідно до (1-9), побудуємо матрицю попарних порівнянь, яка, заснована на шкалі важливості Т. Сааті. Матриця має наступний вигляд (табл. 2):

Таблиця 2. Матриця попарних порівнянь ІТ-інцидентів на ОКІІ

	Hardware Incidents (HI) - Проблеми з фізичними пристроями	**Software Incidents (SI)** - Проблеми з програмним забезпеченням	**Security Incidents (SEI)** - Інциденти безпеки	**Service Outages (SO)** - Перебої в обслуговуванні	**Connectivity Issues (CI)** - Проблеми з'єднання	**User Errors (UE)** - Помилки користувачів	**Configuration Issues (CFI)** - Проблеми конфігурації	**Performance Issues (PI)** - Проблеми продуктивності
	HI	SI	SEI	SO	CI	UE	CFI	PI
HI	1	3	2	4	5	6	7	3
SI	1/3	1	1/2	2	3	4	5	2
SEI	1/2	2	1	5	6	7	8	4
SO	1/4	1/2	1/5	1	3	4	2	1/2
CI	1/5	1/3	1/6	1/3	1	2	1/2	1/3
UE	1/6	1/4	1/7	1/4	1/2	1	3	1/2
CFI	1/7	1/5	1/8	1/2	2	1/3	1	1/4
PI	1/3	1/2	1/4	2	3	2	4	1

Глобальні пріоритети показують відносну силу, величину та важливість кожного окремого елемента системи ІТ безпеки. На основі проведених розрахунків найбільший локальний пріоритет щодо ІТ безпеки в порівнянні з іншими загрозами має *User Errors* (*UE*) – 0,25. На другому місці *Service Outages* (*SO*) з глобальним пріоритетом 0,20. Третє місце займає *Security Incidents* (*SEI*) з глобальним пріоритетом 0,15.

Окрім цього, важливими є *Software Incidents* (*SI*) та *Hardware Incidents* (*HI*) з глобальними пріоритетами 0,12 та 0,10 відповідно. Проблеми з конфігурацією (*Configuration Issues, CFI*) також заслуговують на увагу з глобальним пріоритетом 0,08. Для решти загроз глобальні пріоритети наступні: *Performance Issues* (*PI*) – 0,06, *Connectivity Issues* (*CI*) – 0,04.

Отримані значення глобальних пріоритетів дозволяють визначити, які загрози є найбільш критичними для забезпечення надійності та стійкості критичної інформаційної інфраструктури. Зосередження уваги на найбільш пріоритетних загрозах допомагає ефективно управляти ІТ безпекою та мінімізувати ризики для громадянина, суспільства, держави та правопорядку (табл. 3).

Таблиця 3. Значення глобальних пріоритетів ІТ-інцидентів ОКІІ

Загроза	**Глобальний пріоритет**
UE	0,25
SO	0,20
SEI	0,15
SI	0,12
HI	0,10
CFI	0,08
PI	0,06
CI	0,04

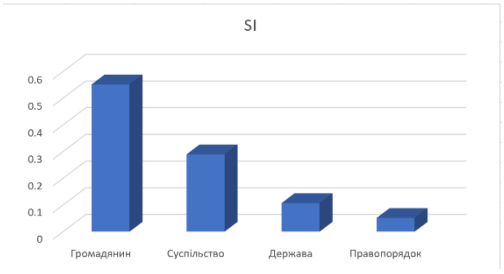
Таким чином, матриця парних порівнянь дозволяє визначити, які з загроз є найбільш критичними для забезпечення ІТ безпеки. Це допомагає зосередити ресурси та зусилля на найважливіших проблемах, мінімізуючи вплив потенційних загроз на систему.

Етап 4. Основним завданням цього етапу є визначення локальних пріоритетів ризиків об'єктів захисту через проміжний другий рівень – загрози за допомогою матриць попарних порівнянь щодо цих загроз, відповідно до (10). У такий спосіб за допомогою групи матриць парних порівнянь, для вище наведених загроз, послідовно формуємо множину локальних пріоритетів третього рівня щодо ризиків особи, суспільства та держави. Значення локальних пріоритетів ризиків об'єктів захисту щодо зазначених загроз наведені у табл. 4.

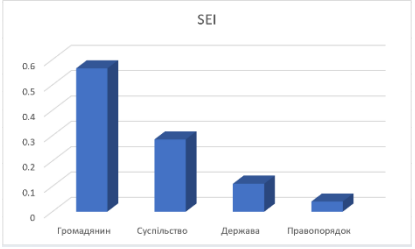
Таблиця 4. Значення локальних пріоритетів ІТ-інцидентів ОКІІ

Hardware Incidents (*HI*) – Проблеми з фізичними пристроями

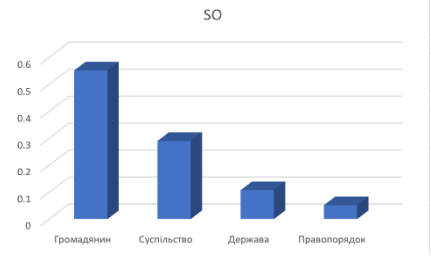
Software Incidents (*SI*) – Проблеми з програмним забезпеченням



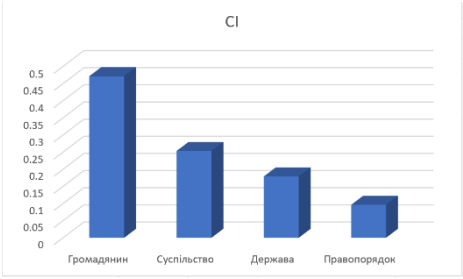
Security Incidents (*SEI*) – Інциденти безпеки



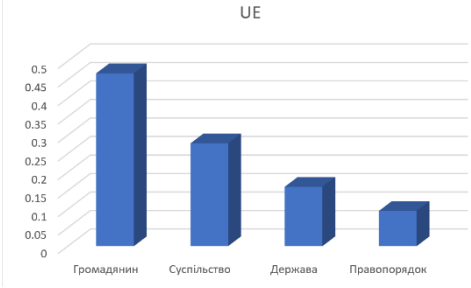
Service Outages (*SO*) – Перебої в обслуговуванні



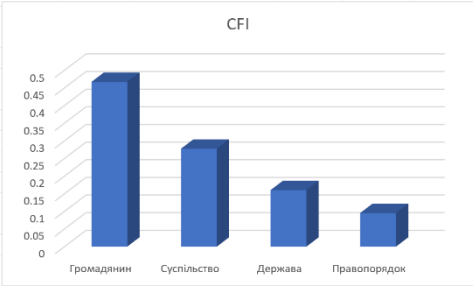
Connectivity Issues (*CI*) – Проблеми з'єднання



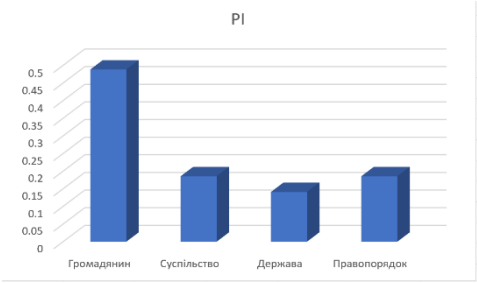
User Errors (*UE*) – Помилки користувачів



Configuration Issues (*CFI*) – Проблеми конфігурації



Performance Issues (*PI*) – Проблеми продуктивності



Етап 5. Разом з матрицями парних порівнянь ми отримали міри оцінок відхилення від узгодженості, які в узагальненому вигляді подані в табл. 5, відповідно до (11).

Таблиця 5. Міри оцінок відхилення від узгодженості

Рівні	**Пріоритети**	***n***	***λmax***	***CR***
1	НСЗКІ	8	8.57373	0.05812
2	*HI*	4	4.01452	0.005
2	*SI*	4	4,17244	0,05748
2	*SEI*	4	4,27255	0,09085
2	*SO*	4	4,17244	0,05748
2	*CI*	4	4,12326	0,04109
2	*UE*	4	4,03098	0,01033
2	*CFI*	4	4,03098	0,01033
2	*PI*	4	4,13199	0,04400

Отже, можна зробити висновок, що відповідно до проведеного експерименту, апаратні інциденти (*HI*) мають найвищий пріоритет для держави (0.483), що підкреслює необхідність підтримки фізичної інфраструктури, програмні інциденти (*SI*) та інциденти безпеки (*SEI*) є найбільш критичними для громадян (0.552 та 0.565 відповідно), що вимагає уваги до надійного програмного забезпечення і кібербезпеки, перебої в обслуговуванні (*SO*) суттєво впливають на громадян і суспільство, але менш впливають на державу і правопорядок, проблеми продуктивності (*PI*), помилки користувачів (*UE*) та проблеми конфігурації (*CFI*) мають значний вплив на громадян, потребуючи покращення IT-послуг і навчання користувачів.

Висновки

В результаті дослідження розв'язано наступні задачі:

1. Проаналізовано міжнародні стандарти та практики, такі як *ITIL*, *COBIT*, *ISO/IEC* 20000 та *NIST Cybersecurity Framework*. Було визначено переваги та недоліки кожного з підходів, що дозволило вибрати найбільш релевантні елементи для розробки власного методу. Аналіз показав, що станом на зараз немає достатньої кількості наукових праць, які зосереджуються на визначенні пріоритетів IT-інцидентів. Крім того, було встановлено, що міжнародний підхід *ITIL* має значні

переваги завдяки своїй структурованості, гнучкості та орієнтації на ІТ-послуги.

2. Розроблено метод, який базується на інтеграції кращих світових практик і використанні методу попарних порівнянь (*AHP*). Метод включає ідентифікацію та оцінку загроз, встановлення пріоритетів за допомогою *AHP*, а також синтез локальних і глобальних пріоритетів для ефективного управління ІТ-безпекою. Це дозволяє враховувати специфіку різних аспектів інформаційної безпеки, таких як вплив на громадян, суспільство, державу та правопорядок.

3. Експериментально перевірено розроблений метод на реальних даних. Отримані результати підтвердили практичну цінність методу, що дозволяє систематично пріоритизувати загрози та ефективно керувати ІТ-безпекою. Було встановлено, що апаратні інциденти мають найвищий пріоритет для держави, тоді як програмні інциденти та інциденти безпеки є найбільш критичними для громадян. Це підкреслює необхідність підтримки фізичної інфраструктури та посиленої уваги до розробки надійного програмного забезпечення для забезпечення ІТ-безпеки.

Література

1. Король О. Г., Огурцова К. В., Євсеєв С. П. Оцінка ризику реалізації загроз безпеки у телекомунікаційних системах. Автоматика, телемеханіка, зв'язок. *Збірник наукових праць ДонІЗТ*. 2013. № 36. С. 55–63.

2. Mokhor V. V., Honchar S.F. Evaluation of risks of cyber security of information systems of objects of critical infrastructure. *Electronic modeling*. Vol. 41, no. 6. P. 65–76. DOI: 10.15407/emodel.41.06.065

3. Jablanski D. Method for Determining the State of Protection of Critical Information Infrastructure Objects from IT Risks. Наукові дослідження з кібербезпеки. URL: https://www.researchcybersecurity.com/ state-protection-method/ (дата звернення: 01.06.2024).

4. Anuar N. et al. A risk index model for security incident prioritization. *9th Australian Information Security Management Conference* : proceedings, Perth, WA, Australia, 05–07 December 2011 / 2011. P. 25–39.

5. Качинський А. Б., Варичева Д. І., Свириденко С. В. Ефективне управління ІТ-інцидентами в критичній інформаційній інфраструктурі. *Інформація і право*. 2016. № 2(17). С. 114–126.

6. Nosal K., Solecka K. Application of AHP method for multi-criteria evaluation of variants of the integration of urban public transport. *Transportation Research Procedia*. 2014. Vol. 3. P. 269–278. DOI: 10.1016/ j.trpro.2014.10.006.

7. Saaty T. L. Decision making with the analytic hierarchy process. *International Journal of Services Sciences*. 2008. Vol. 1(1). P. 83–98. DOI: 10.1504/ijssci.2008.017590.

8. Закон України про критичну інфраструктуру. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/ show/1882-20#Text (дата звернення: 01.06.2024).

9. Кабінет Міністрів України. Деякі питання об'єктів критичної інфраструктури: Постанова від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/ show/1109-2020-%D0%BF#Text (дата звернення: 01.06.2024).

10. ITIL Foundation: ITIL 4 Edition. ITIL 4 Best Practice. URL: https://www.axelos.com/certifications/itil-certifications/itil-foundation (date of access: 01.06.2024).

Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А.

МЕТОД ВИЗНАЧЕННЯ ПРІОРИТЕТІВ ІТ-ІНЦИДЕНТІВ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Стаття присвячена розробці методу визначення пріоритетів ІТ-інцидентів на об'єктах критичної інформаційної інфраструктури держави. У дослідженні розглянуто основні підходи до класифікації та управління ІТ-інцидентами, такі як ITIL,

COBIT, ISO/IEC 20000 та NIST Cybersecurity Framework. Запропонований метод базується на використанні методу попарних порівнянь (AHP) для оцінки та пріоритизації загроз, враховуючи їхній вплив на різні рівні функціонування критичних об'єктів. Стаття детально описує етапи розробки методу, включаючи ідентифікацію загроз, встановлення локальних і глобальних пріоритетів, а також синтез отриманих результатів для ефективного управління IT-безпекою. Запропонований підхід дозволяє раціонально розподіляти ресурси, забезпечуючи надійність та стійкість критичної інформаційної інфраструктури. Експериментальні дослідження підтверджують практичну цінність методу, що робить його корисним інструментом для підвищення рівня захищеності та ефективного реагування на IT-інциденти в умовах сучасних викликів забезпечення IT-безпеки.

***Ключові слова**: критична інфраструктура; критична інформаційна інфраструктура; об'єкти критичної інформаційної інфраструктури; IT-інциденти; ITIL; пріоритизація IT-інцидентів.*

Sydorenko V.M., Polozhentsev A.A., Sydorenko S.Y., Skurativskyi A.A.

A METHOD FOR PRIORITIZING IT INCIDENTS AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES OF THE STATE

The article is devoted to the development of a method for prioritizing IT incidents at critical information infrastructure facilities of the state. The study considers the main approaches to classifying and managing IT incidents, such as ITIL, COBIT, ISO/IEC 20000 and NIST Cybersecurity Framework. The proposed method is based on the use of the pairwise comparison method (AHP) to assess and prioritize threats, taking into account their impact on different levels of critical facilities. The article describes in detail the stages of method development, including threat identification, local and global prioritization, and synthesis of the results obtained for effective IT security management. The proposed approach allows rational allocation of resources, ensuring the reliability and resilience of critical information infrastructure. Experimental studies confirm the practical value of the method, which makes it a useful tool for increasing the level of security and effective response to IT incidents in the face of modern threats to IT-security.

***Keywords**: critical infrastructure; critical information infrastructure; critical information infrastructure facilities; IT incidents; ITIL; IT incident prioritization.*