DOI: 10.18372/2310-5461.62.18687
УДК 004.5:004.891

В. М. Сидоренко, канд. техн. наук, доцент
Національний авіаційний університет
orcid.org/0000-0002-5910-0837
e-mail: v.sydorenko@ukr.net;

А. А. Положенцев
Національний авіаційний університет
orcid.org/0000-0003-0139-0752
e-mail: artem.polozhencev@gmail.com

МЕТОД УПРАВЛІННЯ ІТ-ЗАГРОЗАМИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Вступ

У сучасному світі цифрових технологій захист критичної інфраструктури (КІ) є одним із найважливіших завдань для організацій та держави. Зростання кількості кіберзагроз, пов'язаних із розвитком інформаційних технологій, підвищує необхідність впровадження надійних заходів безпеки. Критична інформаційна інфраструктура (КІІ) включає в себе системи та мережі, які є життєво важливими для функціонування суспільства у сферах енергетики, транспорту, фінансів, зв'язку та охорони здоров'я. Вихід з ладу або компрометація таких компонентів можуть мати серйозні наслідки для національної безпеки, економіки та суспільного добробуту. Для ефективного захисту КІІ необхідно правильно ідентифікувати, оцінити та управляти ІТ-загрозами, особливо в умовах обмежених ресурсів захисту. Все це, свідчить про наявність важливого наукового завдання щодо розробки та впровадження ефективного методу управління ІТ-інцидентами на об'єктах КІІ (ОКІІ).

Постановка проблеми

Незважаючи на важливість забезпечення ІТ-безпеки КІІ, станом на сьогодні немає достатньої кількості наукових досліджень, щодо розроблення та впровадження методів управління ІТ-загрозами, як на міжнародному, так і вітчизняному просторі (рис. 1). Проте, при проведені аналізу, авторами було досліджено підходи щодо управління загрозами у різних сферах КІ.

Рис. 1. Процес управління ІТ-інцидентами [1]

У дослідженні [2] автори розробили алгоритм оцінки загроз кібербезпеки для систем управління навчанням (LMS). Поєднавши модель STRIDE з багатокритеріальним методом підтримки прийняття рішень TODIM та додавши нечіткі множини, вони оцінили платформи LMS, а саме Moodle,
Atutor та Ilias. У дослідженні брали участь три експерти з кібербезпеки, які оцінювали безпеку за допомогою лінгвістичних змінних, демонструючи ефективність алгоритму у виявленні та ранжуванні кіберзагроз у середовищах LMS. Дане дослідження найбільше стосується фахівців з кібербезпеки, які є відповідальним за безпеку освітніх технологій та зможуть використати методологію для посилення безпеки LMS.

У статті [3] автори досліджують застосування моделі STRIDE для оцінки загроз кібербезпеки в транспортній галузі КІ. У статті висвітлено, як інтеграція STRIDE з методом аналізу небезпек і оцін-ки ризиків (HARA), що отримав назву SAHARA-підхід, забезпечує всеосяжну основу для оцінки ризиків безпеки на ранніх етапах розробки. Цей комбінований підхід дозволяє ідентифікувати та класифікувати загрози безпеці, забезпечуючи впро-вадження відповідних контрзаходів для захисту автомобільних систем від потенційних кібератак, тим самим підтримуючи

послідовну та безпечну розробку продукту протягом усього життєвого циклу.

У дослідженні [4] розглядаються питання покращення безпеки та конфіденційності, а також вразливості мереж 5G з акцентом на захисті КІ. Незважаючи на досягнення в порівнянні з попередніми поколіннями, мережі 5G все ще мають слабкі місця в технічній безпеці, які можуть бути використані. У документі використовується модель класифікації загроз STRIDE для виявлення та аналізу одинадцяти сценаріїв загроз в екосистемі 5G, що підкреслює важливість впровадження надійних заходів безпеки для зменшення цих ризиків.

У дослідженні [5] було встановлено, що критичні об'єкти інфраструктури та промислові системи управління є складними кібер-фізичними системами (КФС). Забезпечення надійної роботи таких систем вимагає комплексного моделювання загроз під час проектування та валідації системи. У цій статті представлено комплексну методологію моделювання загроз для КФС з використанням STRIDE – системного підходу до забезпечення безпеки системи на компонентному рівні. Методологію застосовано до реального випробувального стенду синхронної ізольованої системи на основі синхрофазору. Дослідження визначає типи загроз, які можуть виникнути в кожному компоненті системи, і те, як вразливості в компоненті можуть поставити під загрозу безпеку всієї системи. Доведено, що STRIDE є легкою та ефективною методологією моделювання загроз для КФС, що спрощує завдання для аналітиків з безпеки.

Встановлено, що на даний момент не існує реалізованого методу, який би дозволяв ефективно управляти ІТ-загрозами на ОКІІ. Тому розробка такого методу є надзвичайно необхідною для забезпечення більш надійного захисту від потенційних ІТ-загроз та підвищення рівня захищеності критичних інформаційних систем (КІС). Отже, ***метою даної статті*** є розробка та експеримен-тальне дослідження методу управління ІТ-загро-зами на ОКІІ.

Аналіз останніх досліджень та публікацій

У зв'язку з тим, що попередній аналіз існуючих досліджень щодо ідентифікації, оцінки та управління ІТ-загрозами не дав змогу знайти єдиний формалізований підхід, авторами було прийнято рішення розробки власного методу управління ІТ-загрозами на ОКІІ. Для цього необхідно провести додатковий аналіз ефективності міжнародних практик та методологій моделювання загроз за наступними критеріями: простота використання (EU) – оцінка легкості застосування методу на практиці, комплексність (СМ) – наскільки метод охоплює всі аспекти управління ІТ-загрозами, інтеграція з іншими системами (IS) – наскільки метод дозволяє інтегруватися з іншими системами безпеки та управління, фокус на КІ (CI) – чи враховує метод специфіку ОКІІ, об'єктивність (ОВ) – наскільки метод зменшує суб'єктивність у процесі прийняття рішень, час на застосування (ЕТ) – час, необхідний для застосування методу.

Методика класифікації загроз STRIDE [8] є популярним інструментом для аналізу загроз безпеки, розробленим Microsoft. Цей акронім розшифровується як Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. Ця методологія допомагає виявити слабкі місця в інформаційних системах, дозволяючи розробникам і спеціалістам з безпеки проактивно вживати заходів для їх усунення. Серед переваг STRIDE – комплексність, оскільки метод охоплює широкий спектр загроз, чіткість і структурованість з чітко визначеними категоріями загроз, а також можливість інтеграції з іншими методами та інструментами безпеки. Однак, для ефективного використання даної методології потрібні глибокі знання в області ІТ-безпеки.

Нормативний документ NIST SP 800-30 [9] від Національного інституту стандартів і технологій є стандартом для управління ризиками в інформаційних системах, що надає всебічний підхід до ідентифікації, оцінки та управління ризиками, враховуючи специфіку організаційних процесів і активів. Основними перевагами NIST SP 800-30 є комплексний підхід, який охоплює всі етапи управління ризиками, від ідентифікації загроз до розробки стратегії реагування, та визнання стандарту у багатьох організаціях. Однак, впровадження цього стандарту може вимагати значних ресурсів і часу, а також складнощів для малих організацій через обмежені ресурси.

Міжнародний стандарт ISO/IEC 27005 [10] надає вказівки щодо управління ризиками інформаційної безпеки, пропонуючи структурований підхід до ідентифікації, оцінки та обробки ризиків. Переваги ISO/IEC 27005 включають узгодженість з іншими стандартами ISO, що дозволяє інтегрувати управління ризиками в загальну систему управління організацією, та структурованість підходу. Недоліками є вимогливість до ресурсів для впровадження стандарту і складність для малих організацій, які можуть зіткнутися з труднощами при впровадженні.

Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [11] розроблена для оцінки і управління ризиками інформаційної безпеки, зосереджуючись на кри-

тичних активах організації. Вона дозволяє визначити та захистити найважливіші активи організації та проводити самооцінку, залучаючи внутрішні ресурси. Однак, OCTAVE потребує значної участі співро-бітників на всіх рівнях організації і може бути складною для координації у великих організаціях.

Фреймворк COBIT (Control Objectives for Information and Related Technologies) [12] є фреймворком для управління IT, який включає аспекти управління ризиками, забезпечуючи інтеграцію IT з бізнес-цілями. Серед переваг COBIT є інтеграція з бізнес-процесами, що допомагає узгодити управління IT з загальними бізнес-цілями організації, та всеохоплюючий підхід, що охоплює всі аспекти управління IT. Однак, впровадження фреймворку може вимагати значних ресурсів, і малі організації можуть зіткнутися з труднощами через недостатні ресурси для повного впровадження.

Отже, в табл. 1 відображені порівняння підходів до визначення пріоритетів IT-загроз за такими критеріями: EU – простота використання, CM – комплексність, IS – інтеграція з іншими системами, CI – фокус на KI, OB – об'єктивність та ET – час на застосування.

Таблиця 1

Порівняння підходів до визначення пріоритетів IT-загроз

	EU	CM	IS	CI	OB	ET
STRIDE	+	+	+	–	+	+
NIST SP 800–30	–	+	–	+	–	–
ISO/IEC 27005	–	+	+	–	–	+
OCTAVE	–	+	–	–	+	+
COBIT	–	+	–	+	–	+

Зважаючи на аналіз зазначених критеріїв, підхід STRIDE є надзвичайно ефективним і всебічним підходом до визначення IT-загроз. Його чітка структура, можливість інтеграції з іншими методами та акцент на різноманітних типах загроз роблять його ідеальним інструментом для підвищення безпеки інформаційних систем. STRIDE дозволяє організаціям не лише ідентифікувати загрози, але й оцінити їх критичність, розробити відповідні методи захисту і забезпечити комплексний підхід до управління ризиками.

Крім цього, для визначення пріоритетів IT-загроз, необхідно розглянути питання методів прийняття рішень – підходів, які допомагають аналізувати складні проблеми та вибирати найкращий шлях дій з урахуванням різних можливих альтернатив. Ці методи включають ряд технік та інструментів, які допомагають в оцінці різних параметрів та вагомості критеріїв, з метою досягнення об'єктивного, зваженого рішення.

Аналітичний ієрархічний процес (AHP) [13], розроблений Томасом Сааті у 1980-х роках, допомагає розбити проблему прийняття рішень на ієрархію менших складових, що включає цілі, критерії, під-критерії та альтернативи. Використовуючи математичні принципи для оцінки важливості критеріїв та вибору оптимального варіанту, AHP є інтуїтивно зрозумілим і здатним об'єднувати кількісні та якісні критерії. Однак, метод може бути схильним до суб'єктивності у вагах і вимагає значної кількості часу та даних для аналізу.

Метод багатокритеріального аналізу рішень TODIM [14] є мультикритеріальним методом ухвалення рішень, заснованим на теорії перспектив Даніеля Канемана та Амоса Тверскі. Метод використовує принципи теорії корисності для моделювання вподобань особи, яка приймає рішення, в умовах невизначеності та супутніх ризиків. Основні кроки методу включають визначення критеріїв та альтернатив, оцінювання альтернатив за кожним критерієм, присвоєння ваг критеріям, розрахунок домінування кожної альтернативи над іншими з урахуванням ваг, використання функції проспек-тивної цінності для врахування ставлення до ризику, підсумовування проспективних цінностей для отримання оцінки корисності та вибір альтернативи з максимальною оцінкою корисності. Метод включає ризики та невизначеність і є інтуїтивно зрозумілим, але вимагає складних обчислень і суб'єктивної оцінки вагів.

Техніка оцінки та перегляду варіантів (TOPSIS) [15] визначає оптимальну альтернативу шляхом вибору найближчої альтернативи до ідеальної точки. Метод враховує відстані до ідеального (найкращого) та анти-ідеального (найгіршого) рішення. TOPSIS є простим у реалізації та чітко визначає кращу альтернативу, але він чутливий до відносних значень критеріїв і може бути впливовим до некоректного масштабування.

Отже, в табл. 2 відображено порівняння методів прийняття рішень, за допомогою яких можливо оцінювати IT-загрози. Аналіз проведено за такими критеріями: CI – можливість застосування у галузі KI, FL – гнучкість, SC – масштабова-

ність, CR – врахування ризиків та невизначеності, EU – простота використання.

Таблиця 2

Огляд популярних методів багатокритеріального прийняття рішень

Підхід/Критерій	CI	FL	SC	CR	EU
AHP	+	+	+	–	+
TODIM	+	+	+	+	+
TOPSIS	–	–	+	–	+

Зважаючи на аналіз зазначених критеріїв, підхід TODIM є найбільш придатним для застосування у галузі КІІ. Метод ефективно враховує ризики та невизначеність, що є важливим аспектом для ОКІІ, і демонструє високу гнучкість у врахуванні різноманітних критеріїв.

Метод управління ІТ-інцидентами на ОКІІ

Розроблений авторами метод складається з 7 ета-пів, які розглянемо більш детально.

Етап 1. Ідентифікація ІТ-загроз для ОКІІ

Ідентифікація ІТ-загроз є важливим етапом у процесі управління ІТ-загрозами для ОКІІ. Метою цього етапу є виявлення потенційних загроз, які можуть вплинути на нормальну роботу критичних інформаційних систем. На цьому етапі можна вибрати загрози за різними міжнародними підходами, такими як STRIDE, NIST SP 800-30, ISO/IEC 27005, OCTAVE або COBIT, в залежності від особливостей ОКІІ. Позначимо множину потенційних ІТ загроз як множину U_i:

$$U_i = \{U_1, U_2, \ldots, U_n\}, \quad (1)$$

де U_i:– сукупність ідентифікованих потенційних ІТ-загроз; $U_1, U_2, \ldots, U_n$ – це конкретні потенційні ІТ-загрози.

Етап 2. Визначення критеріїв оцінки ІТ-загроз для КІІ

Для кожної загрози U_i та кожного критерію k, введемо множину критеріїв оцінки K:

$$K = \{k_1, k_2, \ldots, k_m\}, \quad (2)$$

де K – це множина критеріїв, за якими буде проводитися оцінка ІТ-загроз; $k_1, k_2, \ldots, k_m$ – це конкретні критерії оцінки.

Кожна потенційна загроза U_i повинна бути оцінена за критеріями K, що дозволить визначити її вплив та пріоритетність.

Етап 3. Отримання та нормалізація даних ІТ-загроз для КІІ

На цьому етапі необхідно провести збір, оцінку та нормалізацію даних щодо ІТ-загроз для КІІ. Цей процес забезпечує об'єктивність та збалансованість підходу до оцінки загроз. Кожна загроза U_i оцінюється за визначеними критеріями K. Наприклад, експерти можуть оцінити ймовірність виникнення загрози, можливий збиток, складність реалізації тощо. Кожен критерій оцінки k має відповідний ваговий коефіцієнт w_k, де сума всіх коефіцієнтів дорівнює 1:

$$\sum_{k=1}^{K} w_k = 1, \quad (3)$$

де K – загальна кількість критеріїв; w_k – ваговий коефіцієнт для критерію k.

Етап 4. Визначення вагових коефіцієнтів критеріїв для ІТ-загроз КІІ

Визначення вагових коефіцієнтів для кожного критерію оцінки ІТ-загроз є важливим кроком, що дозволить врахувати відносну важливість різних аспектів загроз. Це допомагає забезпечити об'єк-тивність і збалансованість у процесі оцінювання ІТ-загроз. Кожен критерій оцінюється за попередньо встановленою шкалою. Автори у своїй роботі пропонують застосовувати шкалу від 1 до 5, де 5 вказує на найвищу ймовірність, шкоду або складність, а 1 – на найнижчу. Така шкала є інтуїтивно зрозумілою та легкою для використання, що спрощує процес оцінки для експертів. Для кожного критерію обчислюємо середнє геометричне оцінок, наданих експертами наступним чином:

$$k = \left(\prod_{j=1}^{n} vk_j\right)^{1/n}, \quad (4)$$

де vk_j – оцінка критерію k експертом j; n – кількість експертів.

Далі, на цьому етапі створюємо вектор вагових коефіцієнтів та обчислюємо їх шляхом нормалізації середніх геометричних оцінок:

$$W = (W_1, W_2, \ldots, W_n)^T, \quad (5)$$

де W_i – це ваговий коефіцієнт для кожного критерію i.

$$W_{jr} = \frac{W_j}{\sum_{r=1}^{n} W_r}, \quad (6)$$

де W_j – середнє геометричне для критерію j; W_r – сума середніх геометричних для всіх критеріїв.

Етап 5. Проведення парних порівнянь альтернативних загроз для КІІ

Використовуємо парне порівняння для визначення домінування кожної загрози над іншими, застосовуючи функцію проспективної цінності, яка враховує ваги критеріїв і оцінки альтернатив за кожним критерієм.

$$Dom(U_i,U_j,k)=\omega_k\times\left(\frac{vU_i,k-vU_j,k}{1+a\times vU_j,k}\right), \quad (7)$$

де U_i та U_j – загрози, які порівнюються; k – критерій, за яким ведеться порівняння; W_k – вага критерію; *vUi,k* та *vUj,k* – оцінки загроз за критерієм;

a – параметр, який відображає ставлення до ризику.

Врахування категорій ОКІ

Відповідно до Закону України «Про критичну інфраструктуру» [16], зокрема відповідно до Статті 10 «Категоризація ОКІ», ОКІ поділяються на категорії залежно від їхньої важливості та потенційного впливу на безпеку держави чи регіону. Введення змінної критичності C дозволяє інтегрувати ці категорії як додаткові критерії у багатокритеріальний аналіз за розробленим методом, що підвищує точність оцінки потенційного впливу загроз на різні рівні критичності.

Змінна критичності C приймає значення від 1 до 4, які відображають рівень критичності об'єкту інфраструктури: Категорія I (C = 1): Особливо важливі об'єкти з загальнодержавним значенням. Порушення їхнього функціонування може спричинити кризу державного масштабу. Категорія II (C = 2): Життєво важливі об'єкти, чиє порушення може викликати регіональну кризу. Категорія III (C = 3): Важливі об'єкти, порушення яких може призвести до місцевої кризи. Категорія IV (C = 4): Необхідні об'єкти, чиє порушення може викликати локальні кризові ситуації.

$$Dom(U_i,U_j,k)=\sum_{k=1}^{n}\left(\frac{\omega_k(U_i,k-U_j,k)}{(1+a\times U_j,k)C}\right),$$

де U_i та U_j – загрози, які порівнюються; k – критерій, за яким ведеться порівняння; W_k – вага критерію; *vUi,k* та *vUj,k* – оцінки загроз за критерієм;

a – параметр, який відображає ставлення до ризиу, C – змінна критичності.

Етап 6. Отримання інтегративної оцінки альтернативних ІТ-загроз для КІІ

На даному етапі необхідно вирахувати значення проспективної цінності, щоб отримати оцінку корисності для кожної загрози.

$$Score(U_i)=\sum_{j\neq i}\sum_{k=1}^{K}Dom(U_i,U_j,k), \quad (8)$$

де $Score(U_i)$ – інтегративна оцінка корисності для загрози a; U_i та U_j – загрози, які порівнюються; k – критерій, за яким ведеться порівняння; $Dom(U_i, U_j,k)$ – функція проспективної цінності, для визначення домінування кожної загрози над іншими.

Етап 7. Пріоритизація та ухвалення рішень щодо ІТ-загроз для КІІ

На даному етапі необхідно провести пріоритизацію виявлених ІТ-загроз та ухвалити відповідні рішення щодо заходів з їхнього усунення або мінімізації. Це досягається шляхом обчислення віднос-ної важливості кожної загрози та ранжування їх на основі отриманих оцінок.

$$p(U_i)=\frac{Score(U_i)}{\sum_{i=1}^{n}Score(U_i)}, \quad (9)$$

де $p(U_i)$ – відносна важливість кожної потенційної ІТ-загрози, $Score(U_i)$ – інтегративна оцінка корисності для загрози a.

Далі, ІТ-загрози необхідно ранжувати від найвищого до найнижчого значення $p(U_i)$. Загрози з найвищими значеннями є найбільш критичними і потребують першочергового реагування. Виходячи з результату ранжування загроз, ухвалюються рішення щодо необхідних заходів для усунення або мінімізації кожної загрози. Це можуть бути технічні, організаційні або процедурні заходи.

Експериментальне дослідження методу управління ІТ-інцидентами на ОКІІ

Застосуємо даний метод для сектору КІІ «Цифрові технології», а саме підсектору «Електронні комунікації», відповідно до [17].

Етап 1. Ідентифікація ІТ-загроз для ОКІІ

Для покращення ІТ-безпеки ОКІІ були визначені такі ІТ-загрози, відповідно до методології STRIDE [8]:

– *Spoofing* (Підроблення ідентичності). Загроза втручання в систему шляхом використання підроблених даних або ідентифікаційних даних для отримання несанкціонованого доступу. Наприклад, хакер може використати підроблені сертифікати для доступу до мережі енергетичної компанії;

– *Tampering* (Маніпуляція даними). Внесення неправомірних змін у дані або конфігурації системи. Це може включати зміну логічних команд управління на ОКІ, що може призвести до фізичних збоїв;

– *Repudiation* (Заперечення). Неможливість відстеження або доведення здійснення дій користувачем. Наприклад, відсутність журналів аудиту може дозволити зловмисникам заперечувати факт здійснення шкідливих дій у мережі управління водопостачанням;

– *Information disclosure* (Розголошення інформації). Несанкціонований доступ до конфіденційної інформації. Наприклад, витік секретних даних з баз даних урядових агентств може призвести до серйозних наслідків для національної безпеки;

– *Denial of Service (DoS*) (Відмова у обслуговуванні). Атаки, які спрямовані на перешкоджання нормальній роботі системи, зокрема, за допомогою перевантаження ресурсів. Наприклад, DoS-атака на системи управління транспортною інфраструктурою може зупинити всі перевезення;

– *Elevation of Privilege* (Підвищення привілеїв). Загроза, що дозволяє зловмисникам отримати більші права, ніж вони мають, і використовувати їх для неправомірного доступу до систем або даних. Наприклад, зловмисник може отримати права адміністратора в системах управління здоров'ям та зловживати цими правами.

Етап 2. Визначення критеріїв оцінки ІТ-загроз для КІІ

Даний етап передбачає детальне визначення критеріїв для оцінки кожної ІТ-загрози U_i. Критерії оцінки є ключовими параметрами, які дозволяють проводити всебічний аналіз загроз та визначати їх пріоритетність для подальшого управління. Для кожної ІТ-загрози U_i та кожного критерію k пропонується застосувати наступні параметри, відповідно до (1, 2):

– *Імовірність виникнення загрози (I)*: Оцінка ймовірності, з якою конкретна ІТ-загроза може реалізуватися. Це дозволяє визначити, наскільки часто можна очікувати виникнення даної загрози;

– *Можливий збиток від загрози (З)*: Оцінка потенційних збитків, які можуть бути завдані КІІ у разі реалізації загрози. Враховуються як фінансові втрати, так і можливий вплив на безпеку та функ-ціонування системи;

– *Складність реалізації загрози (С)*: Оцінка технічної складності, з якою загроза може бути реалізована зловмисниками. Це включає аналіз необхідних знань, інструментів та ресурсів для здійснення атаки.

Правильне визначення критеріїв дозволяє забезпечити більш глибокий та всебічний аналіз загроз, підвищуючи ефективність управління ризиками та захисту КІІ. Оптимальна кількість критеріїв для оцінки ІТ-загроз на ОКІІ залежить від склад-ності проблеми та доступних даних. Використання 3–7 критеріїв, відповідно до [13] є стандартною практикою для забезпечення всебічного аналізу.
Це дозволяє врахувати різні аспекти загроз і ризиків, забезпечуючи збалансований підхід до ухвалення рішень щодо захисту ОКІІ.

Етап 3. Отримання та нормалізація даних ІТ-загроз для КІІ.

Даний етап передбачає детальний процес збору, оцінки та нормалізації даних щодо ІТ-загроз для ОКІІ. Важливою частиною цього етапу є визначення вагових коефіцієнтів для кожного критерію оцінки, що дозволяє забезпечити об'єктивність та збалансованість у підході до оцінки загроз.

Вагові коефіцієнти для оцінки ІТ-загроз на ОКІІ мають бути визначені на основі їх відносної важливості. Імовірність виникнення загрози отримала високий коефіцієнт через її значний вплив на ризик реалізації загрози. Можливий збиток від загрози має найвищий коефіцієнт, оскільки потенційні втрати від загрози критично впливають на функціонування ОКІІ. Складність реалізації загрози отримала нижчий коефіцієнт через її відносно меншу важливість у порівнянні з іншими критеріями, але все ж важливість для оцінки технічних аспектів захисту.

Відповідно до попередніх кроків, кожен критерій оцінки k має відповідний ваговий коефіцієнт w_k, де сума всіх коефіцієнтів дорівнює 1, згідно з (3), що відображено нижче у табл. 3:

Таблиця 3

Таблиця критеріїв оцінки ІТ-загроз

Критерій, k	Опис	Ваговий коефіцієнт, w_k
Імовірність виникнення загрози (I)	Оцінка ймовірності того, що загроза може реалізуватися	0.4
Можливий збиток від загрози (З)	Оцінка потенційних втрат або збитків, які можуть бути завдані в разі реалізації загрози	0.5
Складність реалізації загрози (С)	Оцінка складності технічної реалізації загрози, що враховує необхідні ресурси, знання та інструменти	0.1

Етап 4. Визначення вагових коефіцієнтів критеріїв для ІТ-загроз КІІ

Для більш точного визначення критеріїв, використовується шкала оцінки від 1 до 5, де 1 вказує на найнижчий рівень (низька ймовірність, мінімальний збиток, низька складність) і 5 вказує на найвищий рівень (висока ймовірність, максимальний збиток, висока складність). Далі ці оцінки використовуються для парного порівняння загроз, що дозволяє визначити їх відносну важливість та критичність для ОКІІ. На основі цих критеріїв здійснюється інтегративна оцінка та пріоритизація загроз, що є основою для ухвалення управлінських рішень щодо заходів безпеки та захисту.

Отже, відповідно до (4, 5, 6), застосуємо зазначену шкалу для оцінювання альтернатив, за вказаними критеріями. Нижче наведено таблицю оцінок альтернатив за критеріями (табл 4).

Таблиця 4

Оцінка альтернатив за критеріями

Загроза	Імовірність (І)	Збиток (З)	Складність (С)
Spoofing	2	4	3
Tampering	3	5	2
Repudiation	1	3	4
Information disclosure	4	5	2
Denial of Service	5	5	1
Elevation of Privilege	2	4	3

Далі ці оцінки використовуються для парного порівняння загроз, що дозволяє визначити їх відносну важливість та критичність для ОКІІ. Це порівняння допомагає встановити, які загрози є найбільш серйозними і потребують першочергових заходів захисту. Після цього здійснюється інтегративна оцінка та пріоритизація загроз на основі отриманих результатів, що є основою для ухвалення управлінських рішень щодо заходів безпеки та захисту ОКІІ.

Етап 5. Проведення парних порівнянь альтернативних загроз для КІІ

Відповідно до (7), на цьому етапі використовується метод парних порівнянь для визначення домінування кожної загрози над іншими. Цей метод дозволяє оцінити відносну важливість та критичність кожної загрози шляхом порівняння їх за визначеними критеріями. Застосування функції проспективної цінності враховує ваги критеріїв та оцінки альтернатив за кожним критерієм:

– *Внесення даних*: після проведення оцінки всіх загроз за визначеними критеріями на попередньому етапі, ці дані заносяться у спеціально розроблене програмне забезпечення, для проведення розрахунків;

– *Визначення параметра α*: параметр α встановлюється для врахування ставлення до ризику. Значення α можуть приймати значення залежно від конкретної ситуації, але зазвичай знаходяться в діапазоні від 0 до 1. Низькі значення α зменшують вплив ризику, тоді як високі значення підсилюють його значення;

– *Парне порівняння загроз*: кожна загроза порівнюється з іншими по всіх критеріях. Для кожної пари загроз розраховується значення домінування за допомогою вищевказаної формули;

– *Розрахунок сумарного домінування*: Після порівняння всіх пар загроз за кожним критерієм обчислюється сумарне значення домінування для кожної загрози. Це значення використовується для ранжування загроз і визначення їх пріоритетності.

Отже, цей етап дозволяє провести детальний і об'єктивний аналіз загроз, що забезпечує надійну основу для прийняття управлінських рішень щодо захисту КІІ.

Етап 6. Отримання інтегративної оцінки альтернативних ІТ-загроз для КІІ

На цьому етапі, для автоматизації цього процесу та підвищення точності розрахунків, використовується розроблений програмний застосунок для методу управління ІТ-загрозами. Цей застосунок інтегрує всі дані, проведені парні порівняння та вагові коефіцієнти для обчислення підсумкових оцінок корисності. Відповідно до (8), підсумовуємо значення проспективної цінності, щоб отримати оцінку корисності для кожної загрози. Отже, застосувавши розроблений програмний застосунок для методу управління ІТ-загрозами, отримуємо наступний результат, показаний на рис. 2.

	0.02	0.5	0.2	0.3	Dom	Rank
S		2	4	3	2.406	3
T		3	5	2	-1.564	5
R		1	3	4	5.789	2
I		4	5	2	-1.004	4
D		5	5	1	9.145	1
E		2	4	3	-13.338	6

Рис. 2. Результат застосування програмного застосунку для управління ІТ-загрозами

Етап 7. Пріоритизація та ухвалення рішень щодо ІТ-загроз для КІІ

Відповдно до (9), та на основі проведеного аналізу за розробленим методом, загрози було ранжовано згідно їх сумарного домінування. Представимо пріоритизацію загроз, де загрози з вищими значеннями сумарного домінування мають бути адресовані як найбільш критичні (табл. 5).

На рис. 3 представлено результати оцінювання ІТ-загроз для підсектору КІ «електронні комунікації», відповідно до табл. 5.

Таблиця 5

Пріоритети ІТ-загроз для підсектору КІ «Електронні комунікації»

Загроза	Рівень – Dom	Пріоритет
Denial of Service (DoS)	9.145	Найвищий
Repudiation	5.789	Високий
Spoofing	2.406	Середній
Information disclosure	-1.004	Середній
Tampering	-1.564	Низький
Elevation of Privilege	-2.338	Низький

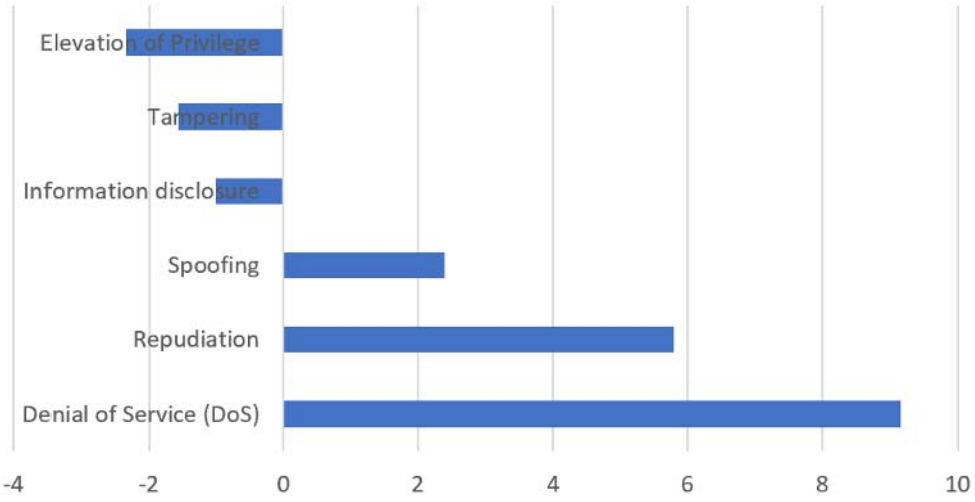

Рис. 3. Результати оцінювання ІТ-загроз для підсектору КІ «Електронні комунікації»

Отже, відповідно до результатів, отриманих за допомогою розробленого спеціального програмного забезпечення, отримали наступні рекомендації щодо ІТ-загроз:

– *Denial of Service (DoS)*: Найбільш критична загроза, що потребує першочергового усунення для зниження ризиків відмови в обслуговуванні, які можуть призвести до значних збоїв в роботі КІ. Рекомендується впровадити стійкі системи проти DoS-атак, використовуючи методи розподілу навантаження та захисту на рівні мережі;

– *Repudiation*: Вимагає удосконалення систем журналювання та аудиту для забезпечення відповідності та прозорості операцій. Слід впровадити надійні механізми логування та збереження журналів дій користувачів, а також регулярні аудити для виявлення та запобігання спробам заперечення дій;

– *Spoofing*: Необхідно зміцнити аутентифікаційні процедури та поліпшити системи ідентифікації та верифікації для запобігання несанкціонованому доступу. Рекомендується використовувати багатофакторну аутентифікацію та вдосконалені методи верифікації користувачів;

– *Information Disclosure*: Необхідно посилити механізми захисту даних, особливо конфіденційної інформації, щоб уникнути її несанкціонованого розголошення. Варто впровадити шифрування даних як під час передачі, так і під час зберігання, а також використовувати системи моніторингу та виявлення витоків інформації;

– *Tampering*: Потрібно забезпечити захист від несанкціонованого втручання в дані, хоча ця загроза не є настільки критичною, як інші. Слід вико-ристовувати контроль цілісності даних та впровад-жувати системи виявлення змін у даних;

– *Elevation of Privilege*: Хоча це серйозна загроза, вона має найнижчий показник домінування і може бути адресована після більш нагальних проблем. Для запобігання підвищенню привілеїв необхідно реалізувати принцип найменших привілеїв, регулярні перевірки прав доступу та використання інструментів для виявлення та блокування спроб підвищення прав користувачів.

Висновки та перспективи подальших досліджень

Отже, в роботі було проведено аналіз існуючих методів управління ІТ-загрозами на ОКІІ. Було визначено, що питання управління ІТ-загрозами на ОКІІ ще недостатньо досліджене, а наявні методи не забезпечують повного вирішення завдань оцінки ІТ-загроз для таких об'єктів. Саме тому, авторами було розроблено новий метод управління ІТ-загрозами на ОКІІ, шляхом синтезу багатокритеріального методу прийняття рішень TODIM та моделлю загроз STRIDE, що дозволяє ефективно ідентифікувати, оцінювати та пріоритизувати загрози, враховуючи їхню ймовірність, потенційний збиток та складність реалізації. Розроблений метод складається з наступних етапів: ідентифікацію загроз, визначення критеріїв оцінки, нормалізацію даних, визначення вагових коефіцієнтів критеріїв, проведення парних порівнянь альтернативних загроз, отримання інтегративної оцінки та пріоритизацію і ухвалення рішень, пропонує ефективний підхід для підвищення рівня захищеності КІІ.

Експериментальне дослідження розробленого методу, яке було проведено для підсектору КІ «електронні комунікації», показало, що метод ефективно сприяє управлінню ІТ-загрозами шляхом визначення пріоритетів цих загроз. Це забезпечує високий рівень захищеності КІС і дозволяє оптимізувати заходи безпеки для ефективного реагування на потенційні ІТ-загрози.

Крім того, завдяки розробленому спеціальному програмному забезпеченню, було виявлено, що для підсектору КІ «електронні комунікації» загроза відмова у обслуговуванні (*Denial of Service*) має найвищий рівень критичності. Це вказує на необхідність першочергових заходів для її нейтралізації. Загалом, визначення пріоритетів ІТ-загроз у процесі забезпечення захисту ОКІІ, може забезпечити ефективне розподілення ресурсів і застосування необхідних заходів для попередження потенційних атак.

Подальші дослідження будуть спрямовані на оптимізацію методу, зокрема:

− визначення нормованих коефіцієнтів для обраних критеріїв загроз;

− розширення рекомендацій щодо управління ІТ-інцидентами, відповідно до отриманих результатів;

− удосконалення методу, для можливості оцінювання комбінованих загроз.

ЛІТЕРАТУРА

[1] DevTools. What is incident management? URL: https://devtools.in/blog/what-is-incident-management/ (дата звернення: 01.05.2024).

[2] Lechachenko, T., Gancarczyk, T., Lobur, T., & Postoliuk, A. (2023). Cybersecurity assessments based on combining TODIM method and STRIDE model for learning management systems. *In CITI* 2023, 250–256.

[3] Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016). Threat and risk assessment methodologies in the automotive domain. *Procedia Computer Science*, 83, 1288–1294. https://doi.org/ 10.1016/j.procs.2016.04.268

[4] Holtrup, G., Blonay, W., Strohmeier, M., Mermoud, A., Chavanne, J.-P., & Lenders, V. (2023). Modeling 5G threat scenarios for critical infrastructure protection. 2023 15th International *Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, Estonia, 161–180. https://doi.org/10.23919/ CyCon58705.2023.10

[5] Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). STRIDE-based threat modeling for cyber-physical systems. 2017 IEEE PES *Innovative Smart Grid Technologies Conference Europe* (ISGT-Europe), Turin, Italy, 1–6. https://doi.org/ 10.1109/ISGTEurope.2017.8260283

[6] Wang, J., Wei, G., & Lu, M. (2018). TODIM method for multiple attribute group decision making under 2-tuple linguistic neutrosophic environment. *Symmetry*, 10(10), 486. https://doi.org/10.3390/ sym10100486

[7] Abomhara, M., Gerdes, M., & Koien, G. M. (2015). A STRIDE-based threat model for telehealth systems. NISK.
[8] Microsoft Corporation. The STRIDE Threat Model, 2005.
[9] Ross, R. (2012). Guide for Conducting Risk Assessments, Special Publication (NIST SP) 800-30 Rev 1. National Institute of Standards and Technology, Gaithersburg, MD. Available at NIST.
[10] International Organization for Standardization. (2022). *ISO/IEC 27005:*2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. ISO.
Available at ISO.
[11] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University, Software Engineering Institute. Available at SEI CMU.
[12] ISACA. (2019). *COBIT 2019* Framework: Governance and Management Objectives. Information Systems Audit and Control Association (ISACA). Available at ISACA.
[13] Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 83. https://doi.org/10.1504/ ijssci.2008.017590
[14] Llamazares, B. (2018). An analysis of the generalized TODIM method. *European Journal of Operational Research*, *269*(3), 1041–1049. https://doi.org/ 10.1016/j.ejor.2018.02.054
[15] Tzeng, G. H., & Huang, J. J. (2011). *Multiple attribute decision making: methods and applications*. CRC press.
[16] Закон України про критичну інфраструктуру. Верховна Рада України. URL: https://zakon.rada. gov.ua/laws/show/1882-20#Text (дата звернення: 01.05.2024).
[17] Кабінет Міністрів України. (2020). 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: 01.05.2024).

Сидоренко В. М., Положенцев А. А.

МЕТОД УПРАВЛІННЯ IT-ЗАГРОЗАМИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

У сучасному світі цифрових технологій захист критичної інформаційної інфраструктури (КІІ) є одним із найважливіших завдань для організації безпеки держави. Зростання кількості різних категорій загроз підвищує необхідність впровадження надійних заходів безпеки. КІІ включає в себе системи та мережі, які є життєво важливими для функціонування суспільства в таких сферах, як енергетика, транспорт, фінанси, зв'язок та охорона здоров'я. Втрата працездатності або компрометація цих компонентів може мати серйозні наслідки для національної безпеки, економіки та добробуту громадян. Тому впровадження надійних заходів захисту є критично важливим. У статті авторами розроблено та запропоновано власний метод управління IT-загрозами на об'єктах критичної інформаційної інфраструктури (ОКІІ). Метод включає синтез багатокритеріального методу прийняття рішень TODIM та моделі загроз STRIDE, що дозволяє ефективно ідентифікувати, оцінювати та пріоритизувати загрози, враховуючи їхню ймовірність, потенційний збиток та складність реалізації. Метод управління IT-загрозами складається з семи етапів: ідентифікація загроз, визначення критеріїв оцінки, нормалізація даних, визначення вагових коефіцієнтів критеріїв, проведення парних порівнянь альтернативних загроз, отримання інтегративної оцінки та пріоритизація загроз. Експериментальне дослідження методу, проведене для підсектору "Електронні комунікації" КІІ, показало його ефективність у визначенні пріоритетів загроз та підвищенні рівня захищеності критичних інформаційних систем. Зокрема, результати дослідження вказують на необхідність першочергових заходів для нейтралізації загрози відмови в обслуговуванні (DoS), яка має найвищий рівень критичності для підсектору "Електронні комунікації", ця загроза є особливо небезпечною, оскільки може призвести до значних перебоїв у роботі систем, що забезпечують життєво важливі послуги. Подальші дослідження будуть спрямовані на оптимізацію методу, розширення рекомендацій щодо управління IT-загрозами та удосконалення оцінювання комбінованих загроз, що включатиме розробку більш складних алгоритмів для виявлення та реагування на IT-загрози.

Ключові слова: критична інформаційна інфраструктура, IT-загрози, управління загрозами, STRIDE, TODIM.

Sydorenko V., Polozhentsev A.

A METHOD FOR IT THREAT MANAGEMENT AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

In the modern world of digital technologies, protecting critical information infrastructure (CII) is one of the most important tasks for organizing the state security. The growing number of different categories of threats increases the need to implement reliable security measures. CII includes systems and networks that are vital to the functioning of society in areas such as energy, transportation, finance, communications, and healthcare. The loss of performance or compromise of these components can have serious consequences for national security, the economy, and the well-being of citizens. Therefore, the implementation of reliable protection measures is critical. In this article, the authors develop and propose their own method for managing IT threats at critical information infrastructure facilities. The method includes the synthesis of the multi-criteria decision-making method TODIM and the threat model STRIDE, which allows to effectively identify, assess and prioritize threats, taking into account their probability, potential damage and complexity of implementation. The IT threat management method consists of seven stages: identifying threats, defining assessment criteria, normalizing data, determining criteria weights, conducting pairwise comparisons of alternative threats, obtaining an integrative assessment, and prioritizing threats. An experimental study of the method conducted for the CII's Electronic Communications subsector showed its effectiveness in prioritizing threats and improving the security of critical information systems. In particular, the results of the study indicate the need for priority measures to neutralize the threat of Denial of Service (DoS), which has the highest level of criticality for the Electronic Communications subsector. This threat is particularly dangerous because it can lead to significant disruptions in the operation of systems that provide vital services. Further research will be aimed at optimizing the method, expanding recommendations for IT threat management, and improving the assessment of combined threats, including the development of more complex algorithms for detecting and responding to threats.

Keywords: critical information infrastructure, IT threats, threat management, STRIDE, TODIM.

Стаття надійшла до редакції 20.05.2024 р.
Прийнято до друку 12.06.2024 р.