DOI: 10.18372/2225-5036.31.20701

МЕТОД ПРИЙНЯТТЯ РІШЕНЬ ЩОДО УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ ДЕРЖАВИ

Вікторія Сидоренко[1], Андрій Максимець[2]

[1]Державний університет «Київський авіаційний інститут»
[2]Адміністрація Державної служби спеціального зв'язку та захисту інформації України

СИДОРЕНКО Вікторія Миколаївна, к.т.н., доц.
Рік і місце народження: 1990 рік, м. Попасна, Луганська область, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: доцент кафедри комп'ютерних інформаційних технологій з 2023 року.
Наукові інтереси: інформаційна безпека, кібербезпека, захист критичної інформаційної інфраструктури держави.
Публікації: 90 наукових публікацій, серед яких монографії, статті у провідних вітчизняних та закордонних наукових виданнях, тези та матеріали доповідей на конференціях.
E-mail: viktoriia.sydorenko@npp.kai.edu.ua
ORCID ID: 0000-0002-5910-0837

МАКСИМЕЦЬ Андрій Володимирович
Рік і місце народження: 1992 рік, м. Вінниця, Україна.
Освіта: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», 2015 рік,
Посада: головний спеціаліст ДПК Адміністрації Держспецзв'язку з 2025 року.
Наукові інтереси: інформаційна безпека, кібербезпека, захист критичної інфраструктури держави.
Публікації: 5 публікацій, серед яких статті, тези та матеріали доповідей на конференціях.
E-mail: andy.west.corp@gmail.com
ORCID ID: 0000-0003-3551-0628

Анотація. *В сучасних умовах зростання інтенсивності та складності кібергроз питання ефективного управління інцидентами кібербезпеки в критичній інфраструктурі (КІ) держави набуває першочергового значення для забезпечення національної безпеки та безперервності надання критично важливих послуг. Невизначеність розвитку кіберінцидентів, множинність можливих варіантів реагування та обмеженість ресурсів зумовлюють необхідність застосування формалізованих науково обґрунтованих підходів до підтримки прийняття управлінських рішень. В роботі представлено метод прийняття рішень щодо управління інцидентами кібербезпеки в КІ держави, який базується на системному підході та формалізації процесу реагування. Запропонований метод передбачає поетапний аналіз кіберінциденту, формування множини альтернатив реагування, моделювання ймовірнісних сценаріїв розвитку подій, кількісне оцінювання наслідків за допомогою матриці результатів та вибір оптимального управлінського рішення за критерієм максимізації очікуваного ефекту. Особливістю запропонованого методу є інтеграція механізму зворотного зв'язку, що дозволяє оцінювати ефективність реалізованих заходів реагування та адаптувати процес прийняття рішень до змін умов функціонування об'єктів КІ та появи нових типів кібергроз. Практична значущість результатів полягає у можливості застосування методу в центрах оперативного реагування та системах підтримки прийняття рішень для підвищення обґрунтованості управлінських дій і мінімізації негативних наслідків кіберінцидентів. Подальші дослідження будуть спрямовані на експериментальну верифікацію методу в різних секторах КІ та його розширення з урахуванням багатокритеріального аналізу й динамічних ресурсних обмежень.*

Ключові слова: *критична інфраструктура, кібербезпека, кіберінцидент, управління інцидентами, прийняття рішень, сценарний аналіз, системи підтримки прийняття рішень, очікуваний ефект, зворотний зв'язок.*

Вступ

Забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури (КІ) є одним із ключових завдань національної безпеки України. Сучасні умови функціонування держави характеризуються поєднанням різнорідних загроз, серед яких особливе місце посідають кіберінциденти, здатні порушувати безперервність надання критично важливих послуг, спричиняти значні соціально-економічні втрати та створювати передумови для ескалації кризових ситуацій. Уразливість КІ до кібератак безпосередньо впливає на стабільність функціонування держави, безпеку населення та розвиток економіки.

Нормативно-правове забезпечення у сфері захисту КІ та кібербезпеки формується Законом України «Про критичну інфраструктуру» [1], Законом України «Про основні засади забезпечення кібербезпеки України» [2], а також підзаконними нормативними актами, зокрема постановами Кабінету Міністрів України щодо категоризації об'єктів КІ, управління ризиками та забезпечення їх стійкості. Зазначені документи визначають загальні принципи та організаційні засади захисту, однак не регламентують формалізовані механізми прийняття управлінських рішень у процесі реагування на кіберінциденти.

В умовах глобалізації, цифровізації та зростання міжсекторальних залежностей навіть окремий кіберінцидент може мати ефект «доміно», поширюючись від одного сектора КІ до іншого. Це обумовлює необхідність застосування системного підходу до управління кіберінцидентами, який би враховував невизначеність розвитку подій, множинність можливих альтернатив реагування та обмеженість ресурсів у процесі прийняття рішень.

Актуальність теми дослідження зумовлена відсутністю уніфікованих формалізованих методів прийняття рішень щодо управління інцидентами кібербезпеки в КІ держави. Це визначає потребу в розробленні науково обґрунтованого методу, який би поєднував вимоги чинного законодавства, міжнародних стандартів і сучасні підходи теорії прийняття рішень та забезпечував обґрунтований вибір оптимальних управлінських дій в умовах невизначеності.

1. Аналіз існуючих досліджень та постановка завдання

Забезпечення належного рівня кібербезпеки об'єктів КІ є одним із ключових завдань національної безпеки держави, оскільки порушення їх функціонування може призвести до значних соціально-економічних, техногенних та оборонних наслідків. В умовах зростання кількості складних та цілеспрямованих кібератак особливої актуальності набуває питання науково обґрунтованого прийняття рішень щодо управління кіберінцидентами з урахуванням невизначеності, обмеженості ресурсів та багатоваріантності розвитку подій.

Нормативно-правова база України

Закон України «Про критичну інфраструктуру» [1] визначає правові та організаційні засади створення і функціонування національної системи захисту КІ. У документі закладено принципи системності, безперервності та пріоритетності захисту, а також визначено суб'єктів забезпечення безпеки. Водночас закон має рамковий характер і не містить формалізованих моделей або алгоритмів підтримки прийняття управлінських рішень у процесі реагування на кіберінциденти.

Закон України «Про основні засади забезпечення кібербезпеки України» [2] встановлює загальні принципи державної політики у сфері кібербезпеки та визначає ролі основних суб'єктів національної системи кібербезпеки. Документ акцентує увагу на необхідності управління кіберризиками та реагування на інциденти, проте не визначає методів оптимального вибору дій у складних умовах інцидентного реагування.

Стратегія кібербезпеки України [3] орієнтована на розвиток національних спроможностей у сфері запобігання, виявлення та реагування на кіберінциденти. Вона підкреслює необхідність використання ризик-орієнтованого та проактивного підходів, однак не пропонує формалізованого механізму прийняття рішень щодо вибору конкретних заходів реагування в умовах невизначеності.

Міжнародні стандарти та рекомендації

Серія стандартів ISO/IEC 27035 [4] описує процес управління інцидентами інформаційної безпеки як сукупність послідовних етапів — від підготовки до аналізу та реагування. Стандарти забезпечують уніфікований підхід до організації процесів інцидент-менеджменту та широко застосовуються на практиці. Разом з тим, ISO/IEC 27035 має переважно процедурний характер і не містить математичних моделей для вибору оптимального управлінського рішення за наявності множини альтернатив і сценаріїв розвитку інциденту.

Документ NIST SP 800-61 [5] є одним із найбільш відомих керівництв з реагування на комп'ютерні інциденти. Він детально описує ролі, процеси та практики реагування, включаючи аналіз інцидентів і визначення пріоритетів. Однак підхід NIST ґрунтується здебільшого на експертних оцінках та регламентних процедурах і не забезпечує формалізованого механізму оптимізації рішень у кількісному вигляді.

Рекомендації ENISA [6] орієнтовані на практичну реалізацію процесів інцидентного реагування в організаціях та на рівні держав. Вони детально описують workflows і взаємодію між суб'єктами реагування. Водночас рекомендації ENISA не розглядають питання математичної формалізації вибору альтернатив реагування, що обмежує їх застосування як основи для систем підтримки прийняття рішень.

Зарубіжні наукові підходи

У роботах Huang та ін. [7] запропоновано використання марковських процесів прийняття рішень (MDP) для оптимального відновлення інтерзалежних інфраструктур після збоїв. Підхід дозволяє мінімізувати сумарні втрати шляхом оптимального розподілу ресурсів. Однак MDP-моделі потребують значних обчислювальних ресурсів і детальних статистичних даних, що ускладнює їх застосування для оперативного управління кіберінцидентами в реальному часі.

Дослідження Rehak та ін. [8] зосереджене на визначенні ключових факторів стійкості елементів критичної інфраструктури. Автори пропонують концептуальну модель, що враховує надійність, адаптивність і відновлюваність. Разом із тим, запропонований підхід має якісний характер і не містить формалізованого алгоритму прийняття управлінських рішень під час інцидентів.

У роботах Trump та Linkov [9, 10] розвинуто концепцію загрозо-незалежної (threat-agnostic) стійкості, яка орієнтована на універсальні принципи функціонування інфраструктур незалежно від типу загрози. Підхід дозволяє підвищити адаптивність систем у довгостроковій перспективі. Проте загрозо-незалежні підходи менш придатні для оперативного управління конкретними кіберінцидентами, оскільки не враховують специфіку поточної ситуації.

Підходи DSS і багатокритеріальний аналіз

У дослідженні Noor та ін. [11] запропоновано систему підтримки прийняття рішень для інвестування в кібербезпеку КІ з використанням кількісних показників ризику. Підхід дозволяє порівнювати альтернативи за декількома критеріями. Однак орієнтація на стратегічне планування обмежує можливість застосування цього підходу для оперативного реагування на інциденти.

У роботі Alizadeh та ін. [12] застосовано багатокритеріальні методи прийняття рішень для оцінювання кіберстійкості інфраструктур. Запропоновано інтеграцію технічних, організаційних та кібернетичних факторів. Разом із тим, складність багатокритеріальних моделей ускладнює їх впровадження в системи оперативного управління інцидентами.

Вітчизняні дослідження

У роботі Плахотнюка [13] запропоновано факторний підхід до забезпечення стійкості КІ держави, що враховує комплекс ризиків і загроз. Автор робить важливий внесок у систематизацію чинників стійкості. Проте питання формалізації процесу вибору управлінських дій під час кіберінцидентів у роботі розглянуто обмежено.

Герасименко [14] аналізує загрози КІ України в умовах воєнного стану, акцентуючи увагу на необхідності комплексного підходу до захисту. Дослідження є важливим з погляду актуалізації загроз. Водночас робота має переважно описовий характер і не пропонує математично обґрунтованого механізму прийняття рішень.

Проведений аналіз свідчить, що існуючі нормативні, стандартні та наукові підходи або мають регламентно-описовий характер, або зосереджуються на окремих аспектах моделювання без інтеграції повного циклу прийняття рішень [15]. Відсутній уніфікований метод, який би поєднував формалізований опис кіберінциденту, множину альтернатив реагування, ймовірнісні сценарії розвитку подій, кількісне оцінювання наслідків та механізм зворотного зв'язку.

Таким чином, **метою роботи** є розроблення нового методу прийняття рішень щодо управління інцидентами кібербезпеки в КІ держави.

Виклад основного матеріалу дослідження

Розроблення методу прийняття рішень щодо управління інцидентами кібербезпеки в КІ держави

Метод прийняття рішень щодо управління інцидентами кібербезпеки в КІ держави ґрунтується на системному підході до аналізу інцидентів, формалізації процесу реагування та вибору оптимальних управлінських дій в умовах невизначеності. Метод орієнтований на мінімізацію негативного впливу кіберінцидентів на безперервність та надійність функціонування об'єктів КІ.

Метод реалізує послідовний процес прийняття рішень (ППР), який охоплює етапи від виявлення інциденту до оцінювання ефективності прийнятих заходів реагування з урахуванням ймовірних сценаріїв розвитку подій.

Етап 1. Виявлення, опис проблемної ситуації та постановка задачі

На даному етапі здійснюється збір, кореляція та первинний аналіз інформації, що надходить із засобів моніторингу кібербезпеки.

Введемо множину ознак інциденту $\mathbf{X}$, яка визначає його поточний стан та характеристики. Загальний вигляд множини має вигляд:

$$\mathbf{X} = \{\bigcup_{i=1}^{n} X_i\} = \{X_1, X_2, \ldots, X_n\}, \quad (1)$$

де $X_i \subseteq \mathbf{X}\ (i = \overline{1,n})$ – ідентифікована ознака кіберінциденту (тип атаки, джерело, уражений компонент, рівень критичності тощо), n – загальна кількість ознак, що використовуються для опису інциденту.

Формування множини $\mathbf{X}$ здійснюється на основі даних, отриманих із засобів моніторингу кібербезпеки, зокрема телеметрії, журналів подій, сигналів IDS/IPS та SIEM-систем.

На основі сформованого вектора ознак $\mathbf{X}$ виконується постановка задачі управління кіберінцидентом, яка полягає у необхідності локалізації інциденту, запобігання його подальшій ескалації та мінімізації негативного впливу на функціонування об'єкта КІ.

Етап 2. Формулювання та структуризація мети управління кіберінцидентом

Метою управління кіберінцидентом у КІ є мінімізація негативного впливу інциденту на функціонування об'єкта КІ.

Для формалізації мети управління введемо функцію втрат $L(X)$, що характеризує рівень негативних наслідків кіберінциденту, описаного множиною ознак $\mathbf{X}$. Тоді задача управління формалізується у вигляді задачі мінімізації:

$$\mathbf{M} = \min L(X, A_i), \quad (2)$$

де $\min L(X, A_i)$ – функція втрат, що характеризує вплив кіберінциденту, описаного множиною ознак $\mathbf{X}$, за умови реалізації альтернативи A_i.

Етап 3. Формування множини альтернатив реагування на кіберінцидент

Для визначення можливих варіантів реагування на кіберінцидент у КІ держави введемо множину альтернатив реагування $\mathbf{A}$ у такому вигляді:

$$\mathbf{A} = \{\bigcup_{i=1}^{k} A_i\} = \{A_1, A_2, \ldots, A_k\}, \quad (3)$$

де $A_i \subseteq \mathbf{A}\ (i = \overline{1,k})$ – альтернатива реагування на кіберінцидент (ізоляція, блокування, зміна політик доступу тощо), k – загальна кількість можливих альтернатив реагування.

Формування множини $\mathbf{A}$ здійснюється з урахуванням характеристик кіберінциденту, описаного множиною ознак $\mathbf{X}$, а також технічних, організаційних і нормативних обмежень функціонування об'єкта КІ.

Етап 4. Формування множини сценаріїв розвитку кіберінциденту

Для урахування невизначеності розвитку кіберінциденту в КІ держави введемо множину можливих сценаріїв розвитку подій $\mathbf{S}$ у такому вигляді:

$$\mathbf{S} = \{\bigcup_{j=1}^{m} S_j\} = \{S_1, S_2, \ldots, S_m\}, \quad (4)$$

де $S_j \subseteq \mathbf{S}\ (j = \overline{1,m})$ – можливий сценарій розвитку кіберінциденту, що описує певний стан зовнішнього та внутрішнього середовища (ескалація атаки, локалізація інциденту, поширення на суміжні сегменти тощо), m – загальна кількість можливих сценаріїв розвитку подій..

Для кожного сценарію S_j визначається ймовірність його реалізації $P(S_j)$, при цьому виконується умова нормування:

$$\sum_{j=1}^{m} P(S_j) = 1. \quad (5)$$

Оцінювання ймовірностей сценаріїв здійснюється на основі статистичних даних,

експертних оцінок та результатів аналізу поточного стану об'єкта КІ.

Етап 5. Моделювання наслідків реалізації альтернатив реагування

Для кількісного оцінювання наслідків реалізації альтернатив реагування на кіберінцидент у КІ введемо матрицю результатів R, у такому вигляді:

$$R = \left[r_{ij} \right], i = 1, k; j \quad (6)$$

де $\left[r_{ij} \right]$ – кількісна оцінка наслідків реалізації альтернативи A_i за сценарієм S_j, що характеризує рівень втрат або ефективність реагування.

Елементи матриці r_{ij} визначаються на основі функції втрат $L(X)$, з урахуванням специфіки альтернативи реагування та сценарію розвитку кіберінциденту і можуть враховувати технічні, економічні та організаційні наслідки.

Етап 6. Вибір оптимального управлінського рішення

На основі матриці результатів $R = \left[r_{ij} \right]$, сформованої на попередньому етапі, здійснюється вибір оптимального управлінського рішення щодо реагування на кіберінцидент у КІ держави.

Для цього для кожної альтернативи реагування **A** обчислюється очікуваний ефект її реалізації з урахуванням імовірностей сценаріїв розвитку подій:

$$E(A_i) = \sum_{j=1}^{m} P(S_j) \cdot r_{ij}, i = 1, k. \quad (7)$$

де $P(S_j)$ – імовірність реалізації сценарію S_j, r_{ij} – елемент матриці результатів, що характеризує наслідки реалізації альтернативи A_i за сценарію S_j.

Оптимальне управлінське рішення визначається за критерієм максимізації очікуваного ефекту:

$$A^* = \arg\max_{A_i \in A} E(A_i). \quad (8)$$

Етап 7. Реалізація оптимального рішення та зворотний зв'язок

На даному етапі здійснюється реалізація оптимального управлінського рішення a^*, визначеного на попередньому етапі, у середовищі функціонування об'єкта КІ держави. Реалізація рішення передбачає виконання комплексу технічних та організаційних заходів реагування відповідно до обраної альтернативи.

Для оцінювання результативності реалізованого рішення вводиться показник фактичного ефекту реагування:

$$F = L(X_b) - L(X_a), \quad (9)$$

де $L(X_b)$ – значення функції втрат до реалізації рішення a^*, $L(X_a)$ – значення функції втрат після реалізації рішення.

Реалізоване рішення вважається ефективним, якщо виконується умова: $F > 0$.

З метою аналізу відповідності фактичних результатів очікуваним визначається різниця між очікуваним та фактичним ефектами:

$$\Delta E = E(A^*) - F, \quad (10)$$

де $E(A^*)$ — очікуваний ефект оптимального рішення, визначений на шостому етапі.

У разі, якщо відхилення перевищує допустиме порогове значення $|\Delta E| > \varepsilon$, де ε — допустимий рівень відхилення, ініціюється процедура повторного аналізу проблемної ситуації та коригування параметрів моделі прийняття рішень, починаючи з першого етапу методу.

Таким чином, запропонований метод прийняття рішень щодо управління інцидентами кібербезпеки в КІ держави, за рахунок формалізації процесу прийняття рішень, урахування множини альтернатив реагування та ймовірнісних сценаріїв розвитку кіберінцидентів, а також використання механізму зворотного зв'язку, дозволяє підвищити обґрунтованість управлінських рішень, мінімізувати негативні наслідки кіберінцидентів та забезпечити адаптивність системи управління кібербезпекою до змін умов функціонування об'єктів КІ.

Висновки

У роботі проведено комплексний аналіз сучасних наукових публікацій, міжнародних стандартів і нормативно-правових документів у сфері управління інцидентами кібербезпеки об'єктів КІ. Встановлено, що наявні підходи мають переважно регламентно-описовий або фрагментарний характер і не забезпечують формалізованого механізму вибору оптимальних управлінських рішень в умовах невизначеності, множинності альтернатив реагування та ймовірнісного розвитку кіберінцидентів, що зумовлює наявність наукової прогалини у цій сфері.

Розроблено метод прийняття рішень щодо управління інцидентами кібербезпеки в КІ держави, який базується на системному підході та формалізації процесу прийняття рішень. Запропонований метод передбачає поетапний аналіз інциденту, формування множини альтернатив реагування, моделювання ймовірнісних сценаріїв розвитку подій, кількісне оцінювання наслідків та вибір оптимального управлінського рішення за критерієм максимізації очікуваного ефекту, а також використання механізму зворотного зв'язку для адаптації прийнятих рішень.

Подальші дослідження будуть спрямовані на експериментальну верифікацію запропонованого методу на практичних сценаріях кіберінцидентів у різних секторах КІ, його інтеграцію в системи підтримки прийняття рішень та центри оперативного реагування, а також розширення методу за рахунок багатокритеріального аналізу та врахування динамічних ресурсних обмежень.

Література

[1]. Закон України «Про критичну інфраструктуру». Прийнятий 16.11.2021 № 1882-IX. Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

[2]. Закон України «Про основні засади забезпечення кібербезпеки України». Прийнятий 05.10.2017 № 2163-VIII. Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19

[3]. Стратегія кібербезпеки України. Указ Президента України від 26.08.2021 № 447/2021. Офіційний портал Президента України. URL: https://www.president.gov.ua/documents/4472021-40013

[4]. ISO/IEC 27035-1:2023. Information security, cybersecurity and privacy protection — Information security incident management — Part 1: Principles of incident management. Geneva : ISO, 2023.

[5]. NIST. Computer Security Incident Handling Guide (SP 800-61 Rev. 2). Gaithersburg, MD : National Institute of Standards and Technology, 2012.

[6]. ENISA. Good Practice Guide for Incident Management. Luxembourg : Publications Office of the European Union, 2010.

[7]. Huang L., Chen X., Zhou Y. Optimal recovery of interdependent critical infrastructure systems using Markov decision processes. Reliability Engineering & System Safety. 2019. Vol. 185. P. 381–395. DOI: 10.1016/j.ress.2019.01.016.

[8]. Rehak D., Senovsky P., Slivkova S. Resilience of critical infrastructure elements and its main factors. International Journal of Critical Infrastructure Protection. 2018. Vol. 21. P. 3–15. DOI: 10.1016/j.ijcip.2018.03.001.

[9]. Trump B., Florin M.-V., Linkov I. Governing resilience: principles and decision support for critical infrastructure. Environment Systems and Decisions. 2018. Vol. 38. P. 370–380. DOI: 10.1007/s10669-018-9690-1.

[10]. Linkov I., Trump B. The science and practice of resilience. Cham : Springer, 2019. 348 p. DOI: 10.1007/978-3-030-04565-4.

[11]. Noor A., Kumar R., Pant R. A decision support framework for cybersecurity investment in critical infrastructure. Decision Support Systems. 2020. Vol. 134. 113281. DOI: 10.1016/j.dss.2020.113281.

[12]. Alizadeh H., Sharif H., Ghazizadeh M. Cyber resilience assessment of critical infrastructures: A multi-criteria decision-making approach. Sustainable Cities and Society. 2021. Vol. 64. 102546. DOI: 10.1016/j.scs.2020.102546.

[13]. Плахотнюк Р. Факторний підхід до забезпечення стійкості критичної інфраструктури України. Науковий вісник. 2022. № 4. С. 45–53.

[14]. Герасименко О. Класифікація загроз критичній інфраструктурі України в умовах воєнного стану. Право та безпека. 2023. № 2. С. 67–75.

[15]. Сидоренко, В., Максимець, А. (2025). Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 560–571. https://doi.org/10.28925/2663-4023.2025.27.779.

УДК ***004.056.53:004.938.5***

Sydorenko V., Maksymets A. Decision-Making Method for Cybersecurity Incident Management in Critical Infrastructure of the State. *In modern conditions of increasing intensity and complexity of cyber threats, the issue of effective cybersecurity incident management in critical infrastructure of the state becomes a top priority for ensuring national security and the continuity of critical services. The uncertainty of cyber incident development, the multiplicity of possible response options, and limited resources necessitate the application of formalized and scientifically grounded approaches to decision support. This paper presents a decision-making method for cybersecurity incident management in critical infrastructure of the state, which is based on a systems approach and formalization of the response process. The proposed method provides a step-by-step analysis of a cyber incident, formation of a set of response alternatives, modeling of probabilistic development scenarios, quantitative assessment of consequences using a results matrix, and selection of an optimal managerial decision based on the criterion of maximizing the expected effect. A distinctive feature of the proposed method is the integration of a feedback mechanism that enables evaluation of the effectiveness of implemented response measures and adaptation of the decision-making process to changing operating conditions of critical infrastructure facilities and the emergence of new types of cyber threats. The practical significance of the results lies in the applicability of the method in security operation centers and decision support systems to improve the justification of managerial actions and minimize the negative consequences of cyber incidents. Further research will focus on experimental verification of the method in various critical infrastructure sectors and its extension using multi-criteria analysis and dynamic resource constraints.*

Key words: *critical infrastructure, cybersecurity, cyber incident, incident management, decision-making, scenario analysis, decision support systems, expected effect, feedback mechanism.*

Сидоренко Вікторія Миколаївна, к.т.н., доцент, доцент кафедри комп'ютерних інформаційних технологій Державного університету «Київський авіаційний інститут».
Sydorenko Viktoriia, PhD, Associate Professor, Associate Professor of the Department of Computer Information Technologies, State University «Kyiv Aviation Institute».

Максимець Андрій Володимирович, головний спеціаліст ДПК Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Maksymets Andrii, Chief Specialist of the Department of Cyber Protection, Administration of the State Service of Special Communications and Information Protection of Ukraine.