**DOI: 10.18372/2410-7840.25.17597**
**УДК 338.242(477)**

# СИСТЕМА ПОКАЗНИКІВ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

***Володимир Шиповський***

*У сучасному світі, де комп'ютерні технології є невід'ємною частиною більшості аспектів нашого життя, кібербезпека стає все більш актуальною та критичною. Особливо це стосується критично важливих об'єктів, таких як електростанції, транспортні системи, медичні установи, банки та інші системи, в яких недостатня кіберстійкість може призвести до серйозних наслідків, включаючи втрату життів та матеріальних збитків. У статті проведено порівняльний аналіз основних підходів до оцінювання рівня кіберзахисту інформаційних систем, проаналізовано основні критерії та показники цих підходів та розроблено загальну модель системи показників оцінювання кіберстійкості інформаційних систем критично важливих об'єктів. Оцінювання кіберстійкості таких систем є складною та відповідальною задачею, оскільки вимагає аналізу великої кількості факторів, які впливають на безпеку інформаційних систем. Тому, вибір показників та критеріїв оцінки кіберстійкості інформаційних систем критично важливих об'єктів є дуже важливою та актуальною проблемою для науково-дослідних робіт в галузі кібербезпеки.*

***Ключові слова:*** *кіберстійкість, інформаційна система, критично важливі об'єкти, методи оцінювання рівня кіберзахисту, критична інфраструктура.*

## ВСТУП

Останніми роками в галузі кібербезпеки було проведено багато досліджень та опубліковано багато статей, присвячених оцінюванню кібербезпеки (рівня кіберзахисту) інформаційних систем.

У роботі [1] розглядається проблема розробки метрик кібербезпеки для промислового Інтернету речей (Internet of Things) та визначаються ефективності цих метрик. У [2] проводиться огляд систем метрик кібербезпеки для критично важливих інформаційних інфраструктур. В науковому дослідженні [3] автори пропонують комплексну методику оцінювання кібербезпеки, яка включає в себе кілька підходів, таких як аналіз загроз, аналіз ризиків та аналіз вразливостей. Для системи SCADA в [4] проводиться огляд методів оцінювання кібербезпеки для систем управління та нагляду за технологічними процесами SCADA.

SCADA (аббр. від англ. Super visory Control and Data Acquisition – диспетчерське управління і збір даних) – програмний пакет, призначений для розробки або забезпечення роботи в реальному часі систем збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління.

Хоча публікації, що були наведені, розглядають питання кібербезпеки та оцінювання її ефективності, однак проблема визначення критеріїв та показників оцінювання кіберстійкості для різних типів інформаційних систем та їх систематизація потребує більш поглибленого наукового дослідження.

Вирішення вищезазначеної проблеми допоможе покращити існуючі методики оцінювання інформаційних систем різного призначення або розробити нові.

Метою статті є визначення системи показників для оцінювання кіберстійкості інформаційних систем критично важливих об'єктів для забезпечення всебічного оцінювання рівня кіберстійкості та розроблення ефективних заходів запобігання кібератакам, вчасного та адекватного реагування на реалізовані кібердії з боку противника.

## ОСНОВНА ЧАСТИНА

Необхідно зазначити, що кіберстійкість та кіберзахист є двома різними поняттями в області кібербезпеки. Кіберстійкість – це здатність системи або мережі залишатися операційними та забезпечувати доступ до необхідних ресурсів в умовах кібервпливу, кібертероризму, кібершпигунства та інших кіберзагроз, коли кіберзахист – це комплекс заходів та технологій, спрямованих на захист системи або мережі від різноманітних кіберзагроз, таких як кібератаки, кібершпигунство, кібер-

тероризм тощо. Кіберзахист може включати в себе технології, які блокують кібератаки, антивірусні програми, системи виявлення вторгнень, системи автентифікації та інші заходи для забезпечення безпеки даних та інформації. Отже, відмінність між кіберстійкістю та кіберзахистом полягає в тому, що кіберстійкість орієнтована на забезпечення доступу до ресурсів та операційну здатність системи під час кібернападу, тоді як кіберзахист спрямований на запобігання кіберзагрозам та захист системи від них. В різних країнах світу та для різних галузей виробничого процесу існує багато підходів до оцінювання рівня кіберзахисту інформаційних систем. У роботі розглянуті три найпоширеніші:

1. "Стандарт оцінки кібербезпеки інформаційних технологій" (CSET) від Національного інституту стандартів та технологій (NIST) США [5];

2. "Методика оцінювання кібербезпеки" від Європейського агентства з кібербезпеки (ENISA) [6];

3. "Оцінка рівня кібербезпеки на основі заходів забезпечення безпеки інформації" (ISO/IEC 27001) від Міжнародної організації зі стандартизації (ISO) [7].

Розглянемо кожний підхід більш детальніше. Стандарт оцінки кібербезпеки інформаційних технологій (CSET) є інструментом, розробленим Національним інститутом стандартів та технологій (NIST) США, який допомагає організаціям оцінити та збільшити рівень кібербезпеки своїх інформаційних систем.

CSET складається з п'яти модулів, які включають:

1. Модуль 1: керування кібербезпекою – надає змогу зрозуміти важливість керування кібербезпекою та розробити стратегію кібербезпеки;

2. Модуль 2: організаційна структура та політики – допомагає розробити політики та процедури, необхідні для ефективного управління кібербезпекою;

3. Модуль 3: активи та управління ризиками – дозволяє ідентифікувати та оцінити свої активи, які піддаються ризику та розробити плани управління цими ризиками;

4. Модуль 4: кібербезпека відповідно до стандартів – надає вказівки щодо впровадження стандартів кібербезпеки, таких як ISO 27001, в організації;

5. Модуль 5: створення та управління кібербезпечними програмами – надає можливості розробити та впровадити кібербезпечні програми, які включають в себе технічні та не технічні заходи забезпечення кібербезпеки.

CSET дозволяє оцінити рівень кібербезпеки організації та допомагає зрозуміти потреби та вимоги для поліпшення кібербезпеки. Крім того, CSET дозволяє організаціям здійснювати оцінку рівня кібербезпеки своїх партнерів та постачальників послуг [8].

Стандарт CSET містить порядок проведення оцінки кібербезпеки та набір інструментів, які дозволяють підвищити рівень кібербезпеки будь-якої системи.

Загальний порядок проведення оцінки кібербезпеки включає такі етапи:

- збір інформації про організацію та її інформаційні системи;
- оцінка ризиків та визначення потенційних загроз;
- оцінка захисту інформаційних систем від потенційних загроз;
- оцінка рівня кібербезпеки організації та визначення плану дій для поліпшення.

Стандарт CSET також містить інструменти для проведення оцінки кібербезпеки, такі як опитувальники, чек-листи та інші документи, які допомагають збирати необхідну інформацію та проводити оцінку [9].

Підхід CSET надає систему критеріїв для оцінювання стану виконання заходів щодо забезпечення рівня кібербезпеки.

Зрозумілість (Clarity) C – показник якості документації з кібербезпеки:

$$C = 1 - (N_K + N_E) / N_D, \quad (1)$$

де $N_D$ - загальна кількість документів; $N_K$ - кількість документів, які було незрозуміло описано; $N_E$ - кількість документів, які містять неповну або незрозумілу інформацію.

Реалістичність (Realism) $R$ – показник здатності плану забезпечення належного рівня кібербезпеки відповідати реальним загрозам та викликам:

$$R = 1 - (N_{TR} + N_F) / N_T, \quad (2)$$

де $N_T$ - загальна кількість загроз; $N_{TR}$ - кількість знайдених загроз, які згадуються в плані; $N_F$ - кількість надмірних або некоректних загроз в плані.

Застосовність (Applicability) $A$ – показник можливості практичного застосування плану кібербезпеки:

$$A = (N_{TD} + N_{FD}) / N_{PP}, \quad (3)$$

де $N_{PP}$ – кількість потенційних проблем зі застосуванням плану; $N_{TD}$ – кількість знайдених рішень або рекомендацій для вирішення проблем; $N_{FD}$ – кількість проблем, які не вирішені або вирішені невірно.

Підтримка (Supportability)-показник здатності забезпечення підтримки плану кібербезпеки на протязі часу:

$$S = (N_{DP} + N_{UP}) / N_{RS}, \quad (4)$$

де $N_{RS}$ - загальна кількість вимог до підтримки; $N_{DP}$ - кількість вирішених або задовільно вирішених вимог; $N_{UP}$ - кількість проблем, які не вирішені або вирішені невірно.

В цілому, стандарт CSET є важливим інструментом для перевірки організації і виконання заходів кіберзахисту інформаційних систем та надає можливість планувати витрати на забезпечення кібербезпеки. У цьому контексті важливо враховувати рекомендації, надані стандартом CSET, та забезпечити підвищення ефективності заходів з забезпечення кібербезпеки [10].

Послідовність оцінювання кібербезпеки від Європейського агентства з кібербезпеки (ENISA) є підручником з інструкціями, рекомендаціями та практичними порадами для оцінювання кібербезпеки в організаціях та підприємствах. Цей підхід надає фреймворк для виконання комплексного аналізу та оцінки рівня кібербезпеки на різних рівнях, від окремих систем до великих і складних інформаційних інфраструктур [11].

Фреймворк – програмна платформа, що визначає структуру програмної системи; програмне забезпечення, що полегшує розробку та об'єднання різних компонентів великого програмного проекту.

Послідовність оцінювання кібербезпеки ENISA містить наступні етапи:

- підготовка до оцінювання: визначення мети оцінювання, областей, що будуть оцінюватися, вибір методів та інструментів оцінювання;
- збір інформації: збір, аналіз та оцінка інформації про систему, що оцінюється, її характеристики та потенційні загрози;
- аналіз та оцінка ризиків: визначення можливих ризиків, їх впливу та імовірності виникнення, а також розробка плану заходів для зниження рівня ризику;
- визначення рівня кібербезпеки: оцінювання рівня кібербезпеки системи на основі відповідності до стандартів, настанов та нормативних документів;
- планування заходів для підвищення кіберстійкості: розробка конкретних заходів для підвищення рівня кібербезпеки системи, визначення їх пріоритетності та часового графіка впровадження;
- підготовка звіту та документації: складання звіту про оцінювання, у якому будуть відображені результати оцінювання кіберстійкості системи [12].

Підхід ENISA також надає рекомендації щодо підготовки звіту з оцінки кібербезпеки, який містить:

- загальний опис інформаційної системи, її мети та функцій;
- визначення обмежень та умов використання системи;
- опис заходів забезпечення кібербезпеки, що застосовуються у системі;
- результати оцінки відповідності заходів забезпечення кібербезпеки вимогам нормативно-правових документів, внутрішніх політик та стандартів організації;
- аналіз ризиків та пропозиції щодо їхнього зменшення;
- рекомендації щодо поліпшення заходів забезпечення кібербезпеки;
- висновки щодо загальної оцінки кібербезпеки системи.

Підхід ENISA є безкоштовним та відкритим для всіх зацікавлених сторін. Він може бути

корисним як для організацій, що мають невеликі ресурси, так і для великих підприємств та урядових установ.

Проаналізувавши послідовність, можемо виділити деякі важливі показники та критерії оцінювання кібербезпеки.

Обсяг витрат на заходи забезпечення кібербезпеки– $Z$ можна розрахувати за формулою:

$$Z = \sum_{i=1}^{I} Z_i, \qquad (5)$$

де $Z_i$ – вартість окремого заходу забезпечення кібербезпеки; $i$ – захід забезпечення безпеки; $I$ – кількість заходів забезпечення безпеки.

Рівень захищеності від загроз $P$ визначається формулою:

$$P = \sum_{k=0}^{K} P_k \Big/ K, \qquad (6)$$

де $P_k$ – рівень захисту від окремої загрози; $K$ – загальна кількість загроз.

Рівень своєчасності виявлення та реагування на інциденти $D$ можна описати формулою:

$$D = \sum_{j=0}^{J} D_j \Big/ J, \qquad (7)$$

де $D_j$ - рівень своєчасності виявлення та реагування на $j$-тий інцидент; $J$ – загальна кількість інцидентів.

Оцінка рівня кібербезпеки на основі заходів забезпечення безпеки інформації (ISO/IEC 270 01)_– міжнародний стандарт зі стандартизації, який встановлює вимоги до систем управління інформаційною безпекою (ІБ).

Цей стандарт встановлює фреймворк для розробки, впровадження, моніторингу, аналізу, підтримки та покращення систем управління ІБ [13].ISO/IEC 27001 заснований на PDCA-циклі (планування, впровадження, контроль та дії), який використовується для впровадження системи управління ІБ та забезпечення її ефективності. Цей стандарт містить загальні вимоги до систем управління ІБ, такі як політика інформаційної безпеки, ризик-аналіз, фізична безпека, безпека персоналу, управління доступом, криптографія та багато іншого.

Оцінка рівня кібербезпеки на основі заходів забезпечення безпеки інформації (ISO/IEC 27001) забезпечує високий рівень захисту інформації та допомагає організаціям знизити ризик витоку даних, крадіжки та несанкціонованого доступу до інформації. ISO/IEC 27001 також містить вимоги до оцінки ризиків та забезпечення безпеки інформації, що можуть бути використані для встановлення ефективної системи управління ІБ. Крім того, стандарт містить методи оцінки та контролю відповідності до встановлених вимог та процедур. Оцінка рівня кібербезпеки на основі заходів забезпечення безпеки інформації (ISO/IEC 27001). В основі стандарту ISO/IEC 27001лежить підхід на основі ризику, що дозволяє оцінити потенційні загрози та визначити заходи забезпечення безпеки, необхідні для зменшення ризику [14].

Стандарт ISO/IEC 27001 містить чотири основних кроки оцінки кібербезпеки:

- визначення області застосування стандарту: визначення області, на яку буде поширюватися система управління інформаційною безпекою;
- визначення ризиків: оцінка потенційних загроз безпеці інформації та визначення ризику, пов'язаного з кожною загрозою;
- вибір та визначення заходів забезпечення безпеки: вибір та визначення заходів забезпечення безпеки, які допоможуть зменшити ризик;
- оцінка ефективності системи управління інформаційною безпекою: оцінка ефективності системи управління інформаційною безпекою та її відповідність вимогам стандарту ISO/IEC 27001.

ISO/IEC 27001 визначає процеси та заходи, які повинні бути вжиті для забезпечення безпеки інформації в організації. Ця методика включає в себе стандарти та рекомендації, які допомагають організаціям розробляти та реалізувати ефективні системи управління інформаційною безпекою [15].

ISO/IEC 27001 використовує цикл PDCA (Plan-Do-Check-Act) як методологію для реалізації процесів забезпечення безпеки інформації. Цей цикл включає певні етапи.

Plan (планування): встановлення політики і цілей безпеки інформації, ідентифікація ризиків та встановлення заходів для зменшення цих ризиків.

Do (дія): виконання запланованих заходів забезпечення безпеки інформації, включаючи

процеси організації та забезпечення фізичної та логічної безпеки.

Check (перевірка): моніторинг та оцінка ефективності заходів забезпечення безпеки інформації, виявлення та виправлення недоліків.

Act (зміна): внесення змін в систему управління безпекою інформації для поліпшення ефективності та підвищення рівня безпеки.

Крім того, ISO/IEC 27001 включає в себе вимоги до документації та записів, які необхідні для демонстрації відповідності до стандарту. Зокрема, організації повинні розробляти політику безпеки інформації, проводити оцінку ризиків, встановлювати контрольні заходи, проводити навчання та свідомо розуміти важливість безпеки інформації для своєї діяльності [16].

У методиці оцінювання рівня кіберзахисту ISO/IEC 27001 проводиться у визначених та критичних для роботи системи контрольних точках – це моменти у часі, коли виконується оцінка ефективності заходів з кіберзахисту. Контрольні точки можуть бути встановлені на різних етапах життєвого циклу інформаційної системи або процесу, який підлягає оцінці кіберзахисту.

Таблиця 1

Порівняльний аналіз різних методик оцінювання кіберстійкості

| Методика оцінювання кіберстійкості ІС | Переваги | Недоліки |
|---|---|---|
| CSET | -дозволяє здійснити оцінку кібербезпеки в рамках конкретної організації або сектору;<br>-надає більш спрощений підхід до оцінки кібербезпеки, порівняно з іншими методиками;<br>-дозволяє автоматизувати процес оцінки кібербезпеки. | -методика довга та складна у застосуванні;<br>-не забезпечує автоматизацію процесу оцінки кібербезпеки, що може вимагати значних зусиль та витрат часу;<br>-вимагає наявності кваліфікованих фахівців, що може бути проблематичним для деяких організацій. |
| ENISA: | -дозволяє здійснити оцінку кібербезпеки в рамках конкретної організації або сектору;<br>-надає більш спрощений підхід до оцінки кібербезпеки, порівняно з іншими методиками;<br>-дозволяє автоматизувати процес оцінки кібербезпеки. | -не охоплює всі аспекти кібербезпеки інформаційних систем, а лише окремі аспекти;<br>-немає офіційної інтерпретації критеріїв та коефіцієнтів методики;<br>-вимагає наявності кваліфікованих фахівців, що може бути проблематичним для деяких організацій. |
| ISO/IEC 27001 | -глобальне визнання і прийняття на міжнародному рівні;<br>-гнучкість та адаптивність до різних видів організацій та різних стандартів безпеки;<br>-зосередженість на ризиках допомагає організації ідентифікувати та управляти своїми конкретними ризиками;<br>-не вимагає спеціального програмного забезпечення, але може використовуватися з іншими стандартами безпеки;<br>-стандарт враховує велику кількість вимог, що сприяє забезпеченню всебічної охорони даних та інформації. | -вимагає значних зусиль та ресурсів для розробки та впровадження стандарту;<br>-може бути складно зрозумілим для непрофесійних користувачів, оскільки є досить детальним та складним;<br>-недостатньо зосередженості на конкретних загрозах, що може призвести до того, що організація може не бути захищеною від нових загроз;<br>-потребує постійного підтримування та оновлення, оскільки стандарти безпеки постійно змінюються. |

Контрольна точка може бути встановлена, наприклад, після впровадження заходів з кіберзахисту або після проведення тестування системи на наявність вразливостей. На кожній контрольній точці здійснюється оцінка ефективності заходів з кіберзахисту та встановлюються подальші дії з урахуванням результатів оцінки. Контрольні точки є важливою складовою процесу забезпечення безпеки інформації у рамках системи керування інформаційною безпекою ISO/IEC 27001. Стандарт ISO/IEC 27001 використовує критерії, розрахунок яких дозволяє перевірити факт реалізації циклу PDCA, тобто процесів забезпечення безпеки інформації. При цьому визначаються рівні: відповідності стандарту; згоди з політикою організації; згоди з ризиками; ефективності заходів.

У табл. 1 перераховані переваги та недоліки різних методик оцінювання кіберстійкості інформаційних систем з метою їх порівняльного аналізу.

CSET, ENISA та ISO/IEC 27001 є методиками забезпечення кібербезпеки. Основні спільні характеристики цих методик включають:

- ризик-орієнтований підхід, що полягає в ідентифікації та оцінці ризиків для організації та встановленні відповідних заходів забезпечення кібербезпеки;
- управління процесами – передбачено підхід до управління процесами забезпечення кібербезпеки, що дозволяє організації планувати ці процеси та удосконалювати їх з часом;
- системний підхід, що передбачає комплексне розглядання питань забезпечення кібербезпеки та узгоджене виконання відповідних заходів;
- стандарти та нормативні вимоги – дотримання стандартів та нормативів, які визначають вимоги до системи управління інформаційною безпекою;
- постійне вдосконалення системи управління кібербезпекою, що дозволяє організації підтримувати свій рівень захищеності від нових загроз та вразливостей.

Отже, SET, ENISA та ISO/IEC 27001 – це загальні методики забезпечення кібербезпеки, які можуть бути застосовані в різних організаціях та сферах діяльності. Методики пройшли апробацію в багатьох державних та недержавних підприємствах та організаціях світу. Вони мають свої метрики та постійно вдосконалюються в залежності від актуальних викликів захисту у кіберпросторі.

Враховуючи недоліки, обмеження та особливості розглянутих методик, можна дійти висновку про те, що модель ENISA може бути застосована для оцінювання кібербезпеки інформаційних систем об'єктів критичної інфраструктури (далі – ІС ОКІ). Однак, ця модель вимагає адаптації шляхом розрахунку додаткових критеріїв для урахування особливостей застосування об'єктів критичної інфраструктури. Призначення ОКІ обумовлює більш жорсткі вимоги до кіберзахищенності ІС ОКІ порівняно з кіберзахистом звичайних інформаційних систем. Основні чинники, які впливають на формування вимог до кіберстійкості ІС ОКІ.

- висока важливість: об'єкти критичної інфраструктури є ключовими для функціонування різних галузей економіки та безпеки держави, тому їх ІС мають бути максимально захищені від кібератак;
- складність: ІС ОКІ мають складну структуру, що ускладнює кіберзахист та може призводити до вразливостей;
- розподіленість: ІС ОКІ, зазвичай мають розподілену архітектуру та підключення до мережі Інтернет, що збільшує ризик кібератак;
- системність: ІС ОКІ складаються з багатьох компонентів, що взаємодіють між собою, тому кіберзахист має бути здійснено на рівні всієї системи;
- безперервність функціонування: ОКІ мають працювати цілодобово та без збоїв, тому дії стосовно кіберзахисту ІСС ОКІ та відновлення роботи ОКІ мають проводитись в найкоротші терміни;
- адаптація методики ENISA для оцінювання кіберзахищенності ІС ОКІ пропонується здійснити шляхом введення додаткового показника – індекс кіберстійкості ІС ОКІ – $I_{кс}$ .

Індекс кіберстійкості може бути представлений сумою трьох складових показників кіберстійкості:

- показник кількості відбиття деструктивних кібервпливів – $I_{кс}\ K$ ;
- вартісний показник – $I_{кс}\ Q$ ;

- часовий показник – $I_{кс}\ T$ .

Для удосконалення методики ENISA визначимо:

1. Індекс відбиття деструктивних кібервпливів представляє собою відношення суми кількостей "успішно відбитих" атак $K_{ап}$ і усунутих внутрішніх порушень безпеки $K_{пр}$ до їх загальної кількості $K_{заг}$:

$$I_{кс}(K) = \frac{K_{ап} + K_{пр}}{K_{заг}}, \qquad (8)$$

2. Вартісний показник кіберстійкості системи може бути виражений наступним чином:

$$I_{кс}(Q) = \frac{\sum_{y=1}^{Y} Q_y}{Q_{втр}}, \qquad (9)$$

де $Q_y$ – вартість реалізації $y$-го заходу забезпечення кіберзахисту системи; $Y$ – кількість заходів забезпечення безпеки – може бути представлена як апаратним або програмним заходом підвищення кібербезпеки системи, так і підвищенням кваліфікації персоналу (інструктаж, освітній захід); $Q_{втр}$ – загальна вартість втрат у разі ураження ОКІ.

3. Часовий показник кіберстійкості представляє собою наступне відношення:

$$I_{кс}(T) = \frac{T_{вияв}}{T_{відн}}, \qquad (10)$$

де $T_{вияв}$ – термін виявлення порушення безпеки – інтервал часу від моменту реалізації деструктивного впливу противника до його виявлення; $T_{відн}$ – термін відновлення роботи системи після порушення безпеки – часовий інтервал від моменту реалізації деструктивного впливу противника до усунення його впливу на мережу або систему.

4. Індекс кіберстійкості на визначений момент часу $t$ може бути виражений наступним чином: $I_{КС}(t) = W_1 \cdot I_{КС}\ K\ + W_2 \cdot I_{КС}\ Q\ + W_3 \cdot I_{КС}\ T\ ,$ де $W_1, W_2, W_3$ – вагові коефіцієнти, що відображають важливість кожного показника оцінювання.

В розгорнутому вигляді індекс кіберстійкості ІС ОК можна розрахувати за формулою:

$$I_{КС}(t) = W_1 \cdot \frac{K_{ап} + K_{пр}}{K_{заг}} + W_2 \cdot \frac{\sum_{y=1}^{Y} Q_y}{Q_{втр}} + W_3 \cdot \frac{T_{вияв}}{T_{відн}}; \qquad (11)$$

$$\sum_{\mu=1}^{3} W_\mu = 1.$$

За допомогою вагових коефіцієнтів можна змінювати важливість кожного показника в системі відповідно до цілей проведення аудиту.

На рис. 1 представлено модель системи показників кіберстійкості ІС .

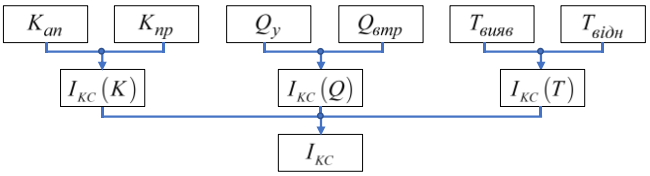


Рис. 1. Система показників кіберстійкості ІС ОКІ

## ВИСНОВКИ

У дослідженні розглянуті три найпоширеніші підходи до оцінювання рівня кіберзахисту інформаційних систем, які мають широкий спектр застосування в різних країнах світу. Порівняльний аналіз розглянутих методик дозволив виділити методику, яка охоплює найбільшу кількість рішень для вимог інформаційних систем ОКІ – а саме – методику ENISA. Система показників кіберстійкості інформаційних систем об'єктів критичної інфраструктури, запропонована в рамках даної статті, надає можливості для більш якісного та ефективного оцінювання рівня кіберзахисту та дозволяє проводити комплексне оцінювання кіберстійкості інформаційних систем, враховуючи різноманітні технічні та організаційні аспекти захисту інформації ОКІ. Практична реалізація результатів дослідження може бути використана для оцінювання кіберстійкості інформаційних систем будь-якої складності та рівня критичності, що є особливо важливим саме для критично важливих об'єктів приватного та державного секторів. Врахування різних аспектів захисту інформації дозволяє забезпечити комплексний підхід до оцінювання кіберстійкості ІС ОКІ.

Надалі планується продовжувати наукові дослідження для удосконалення існуючих методик та розробки інструментів для оцінювання кібер-

стійкості інформаційних систем для захисту ОКІ. Запропонована система показників вирішує лише деякі аспекти та особливості забезпечення кіберзахисту об'єкта дослідження, але вона не враховує наступних невирішених питань:

Визначення вимог до стійкості до фізичного вторгнення: варто визначити вимоги до стійкості до фізичного вторгнення в приміщення з серверними системами, обладнанням та іншими інфраструктурними об'єктами, і встановити відповідні заходи забезпечення кібербезпеки, які дозволять забезпечити високий рівень захисту від фізичного вторгнення.

Визначення вимог до захисту від соціальної інженерії: варто визначити вимоги до захисту від соціальної інженерії на інформаційні системи ОКІ, наприклад, від впливу фармінгу та фішингу через електронну пошту тощо.

Визначення вимог до навчання та підвищення кваліфікації персоналу: варто визначити вимоги до навчання та підвищення кваліфікації персоналу, який відповідає за кіберзахист інформаційних систем ОКІ.

Визначення критеріїв оцінювання кіберстійкості: варто визначити рівні кожного показника, по яким можливо буде стверджувати що система є кіберстійкою. Зазначений перелік вимог та критеріїв планується розглянути у подальших дослідженнях.

## ЛІТЕРАТУРА


[1] Cybersecurity in the Internetof Things in Industrial Management. R.J. Raimundo, A.T. Rosário. URL: https://www.mdpi.com/2076-3417/ 12/3/ 1598 (дата звернення: 12.02.2023).

[2] Evaluation of Cybersecurity Management Control sand Metrics of Critical Infrastructures: A Literature Review Consideringthe NIST Cybersecurity Framework. Barbara Krumay, Edward W. N. Bernroider, Roman Walser URL: https: // link. springer. com / chapter/10.1007/978-3-030-0363 8-6_23 (дата звернення: 12.02.2023).

[3] Evaluation of Cybersecurity Management Control sand Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. Barbara Krumay, Edward W. N. Bernroider, Roman Walser URL: https: // link. springer .com / chapter/ 10.1007 / 978-3-030-0363 8-6_23 (дата звернення: 12.02.2023).

[4] A comprehensive framework for the assessment of Governmen tprojects J. Rhoda, C. Joseph b URL: https: // www. sciencedirect. com/science/ article/abs/pii/S0740624X07000603 (дата звернення: 18.02.2023).

[5] Національний інститут стандартів та технологій (NIST) США. URL: https://www.nist.gov/ cyberframework / cybersecurity-framework (дата звернення: 10.02.2023).

[6] Європейське агентства з кібербезпеки (ENISA). URL: https: // www.enisa.europa.eu/topics/cybersecurity-act/cybersecurity-certification (дата звернення: 15.02.2023).

[7] Міжнародна організація зі стандартизації (ISO). URL:https://www.nist.gov/cyberframework/cybersecurity - framework (дата звернення: 10.02. 2023).

[8] NIST Cybersecurity Framework, NIST. URL: https://www.nist.gov/cyberframework (дата звернення: 11.02.2023).

[9] Introduction to the Cybersecurity Capability Maturity Model (C2M2), NIST. URL: https://www.nist. gov/services-resources/software/cybersecurity-evaluation-tool-cset (дата звернення: 11.03. 2023).

[10] Cybersecurity Evaluation Tool, CSET.URL: https: //www.nist.gov/cyberframework/cybersecurity-framework (дата звернення: 10.02.2023).

[11] Cybersecurity of AI and Standardisation. URL: https:// www. enisa. europa.eu / publications /cybersecurity-of-ai-and-standardisation (дата звернення: 22.02.2023).

[12] Embedded Sim Ecosystem, Security Risksand-Measures. URL: https: //www.enisa.europa. eu/ publications/embedded-sim-ecosystem-security-risks-and-measures (дата звернення: 11.03.2023).

[13] Building Effective Governance Frameworksfor the Implementation of National Cybersecurity Strategies. URL: https: // www. enisa. europa.eu /publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity - strategies (дата звернення: 10.02. 2023).

[14] Стандарты управления информационной безопасностью ISO/IEC 27001:2013. URL:https:// learn.microsoft. com / ru-ru /compliance/regulatory/offering-iso-27001 (дата звернення: 20.02. 2023).

[15] Сертифікація систем управління інформаційною безпекою. URL: https://www.bureauveritas.com.ua/needs/iso-27001-sertifikaciya-sistem-

upravlinnya-informaciynoyu-bezpekoyu (дата звернення: 21.02.2023).

[16] Розробка системи ISO 27001. URL: https: // atestor.ua / uk / services / vnedrenie-standarta-ISO-27001 / (дата звернення: 20.02.2023).

## SYSTEM OF CYBER RESISTANC ASSESSMENT INDICATORS INFORMATION SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS

In today's world, where computer technology is an integral part of most aspects of our lives, cyber security is becoming more and more relevant and critical. This is especially true for critical facilities such as power plants, transportation systems, medical facilities, banks, and other systems where insufficient cyber resilience can lead to serious consequences, including loss of life and property damage. The article provides a comparative analysis of the main approaches to assessing the level of cyber protection of information systems, analyzes the main criteria and indicators of these approaches, and develops a general model of the system of indicators for assessing the cyber resistance of information systems of critical objects. Evaluating the cyber resistance of such systems is a complex and responsible task, as it requires the analysis of a large number of factors that affect the security of information systems. Therefore, the selection of indicators and criteria for assessing the cyber resilience of information systems of critical objects is a very important and urgent problem for scientific research in the field of cyber security.

**Keywords:** cyber resistance, information system, critical objects, methods of assessing the level of cyber protection, critical infrastructure.

**Шиповський Володимир Володимирович,** ад'юнкт кафедри інформаційно-аналітичних технологій Інституту інформаційно-телекомунікаційних технологій та кібероборони Національного університету оборони України імені Івана Черняховського.

**Volodymyr Shypovskyi**, adjunct of the Department of Information and Analytical Technologies of the Institute of Information and Telecommunication Technologies and Cyber Defense of the National Defense University of Ukraine named after Ivan Chernyakhovsky.
E-mail: stratcom.ndl@gmail.com.
Orcid ID: 0000-0003-3743-3064.