



**Атестаційна випускна робота магістра**
**на тему:**

# МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРІНЦИДЕНТІВ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ

***Виконав:***
*студент групи БІКСм-24.*
*Дудинець Дмитро*
***Керівник:***
*к.т.н, доцент кафедри КБКІ*
*Делембовський М.М.*

# АКТУАЛЬНІСТЬ ТЕМИ:

Об’єкти критичної інфраструктури (енергетика, транспорт, телекомунікації, фінанси, охорона здоров’я тощо) становлять основу стабільності економіки, безпеки держави та добробуту громадян. У сучасних умовах кіберзагрози є глобальним викликом: хакерські угруповання застосовують фішинг, DDoS-атаки, соціальну інженерію та шпигунські програми для підриву стійкості цих систем. Для України та інших держав, що перебувають у стані гібридної війни, ця загроза стає особливо критичною – агресор систематично спрямовує зусилля на атаки саме по критичній інфраструктурі. Як зазначено в одному дослідженні, «перебої функціонування об’єктів критичної інфраструктури можуть спричинити значні втрати живої сили та технічного забезпечення, тобто збої в роботі таких систем безпосередньо впливають на національну безпеку.

## МЕТА:

Метою цієї роботи є розробка комплексної метрики кіберстійкості об’єктів критичної інфраструктури. Такий інструмент надасть змогу оцінювати, наскільки критична інфраструктура захищена від сучасних кіберзагроз та здатна швидко відновлювати роботу після атак.

## ОБ’ЄКТ:

Об’єктом дослідження є критична інфраструктура – як складна система підприємств та мереж (включно з енергетичними, транспортними, телекомунікаційними, фінансовими тощо) – та процес забезпечення її стійкої роботи в умовах кібератак.

## ПРЕДМЕТ:

Предметом дослідження виступають методи і показники оцінки кіберстійкості цих систем, зокрема чинники, що визначають здатність критичної інфраструктури витримувати атаки та швидко відновлювати роботу.

# НАУКОВА НОВИЗНА:

Наукова новизна полягає в розробці комплексної метрики кіберстійкості КІ, яка вперше інтегрує кількісну оцінку ризиків (включаючи вразливості і ймовірності кібератак) з показниками готовності реагувати та відновлюватися після інцидентів. У рамках роботи запропоновано включити до метрики інноваційні компоненти: наприклад, оцінку ступеня використання передових технологій (штучного інтелекту, аналітики даних, систем раннього виявлення) при захисті КІ та показники співпраці з іншими суб'єктами (державними й приватними) у сфері безпеки. Також новизною є вперше запропоноване поєднання показників впливу кібератак (час відновлення, економічні збитки тощо) у єдиній метриці. Дана розробка дозволяє ліквідувати відомі недоліки існуючих методів (наприклад, упущення фактора часу чи взаємозв'язку оцінок ризиків) та забезпечує більш точну і релевантну оцінку кіберстійкості.

## ПРОБЛЕМА ДОСЛІДЖЕННЯ :

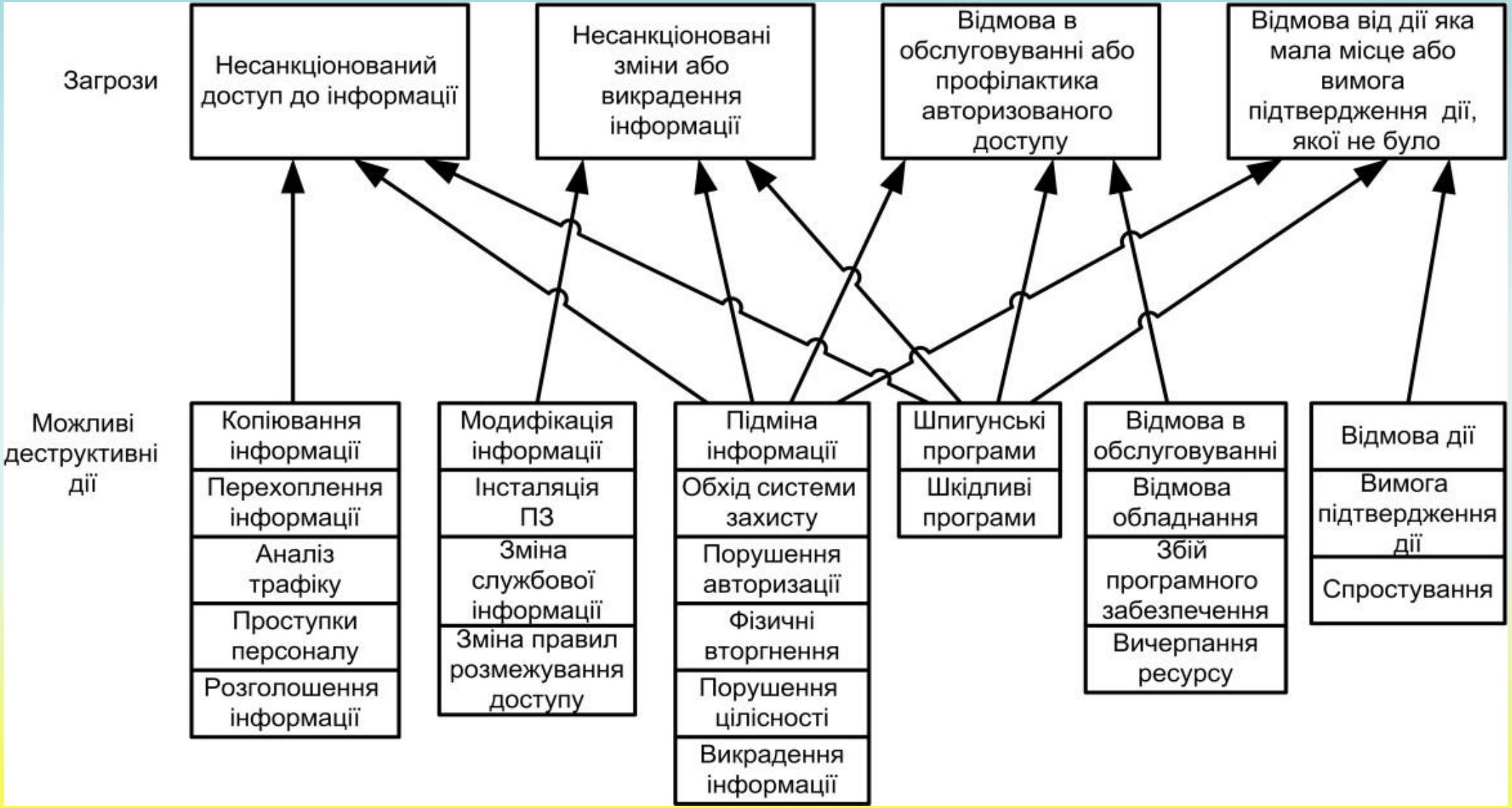
Існуючі підходи до оцінки кіберризиків не враховують усі аспекти складних сучасних загроз і можливостей відновлення. Зокрема, завдання сумарної оцінки ризику кібербезпеки об’єктів КІ досі не розв’язано повною мірою. Відомо, що оператори критичної інфраструктури часто не мають інструментів для комплексної оцінки та управління такими ризиками. Наприклад, навіть у транспортній галузі менеджери не мають засобів для жорсткої оцінки загального ризику (обмежені дані та моделі гальмують точне моделювання). Подібні висновки відображені і в роботах українських експертів: досвід кібератак (на кшталт «BlackEnergy» чи «NotPetya») виявив слабкі місця систем та показав необхідність вдосконалити механізми протидії і нормативну базу. Таким чином, існуючі рішення є недостатніми: це обґрунтовує необхідність створення нової, інтегрованої метрики кіберстійкості, яка покриватиме розширений спектр показників (оцінку вразливостей, потенціал реагування та відновлення, використання новітніх технологій і співробітництва) та вирішуватиме зазначені прогалини.

## Структура кваліфікаційної роботи :

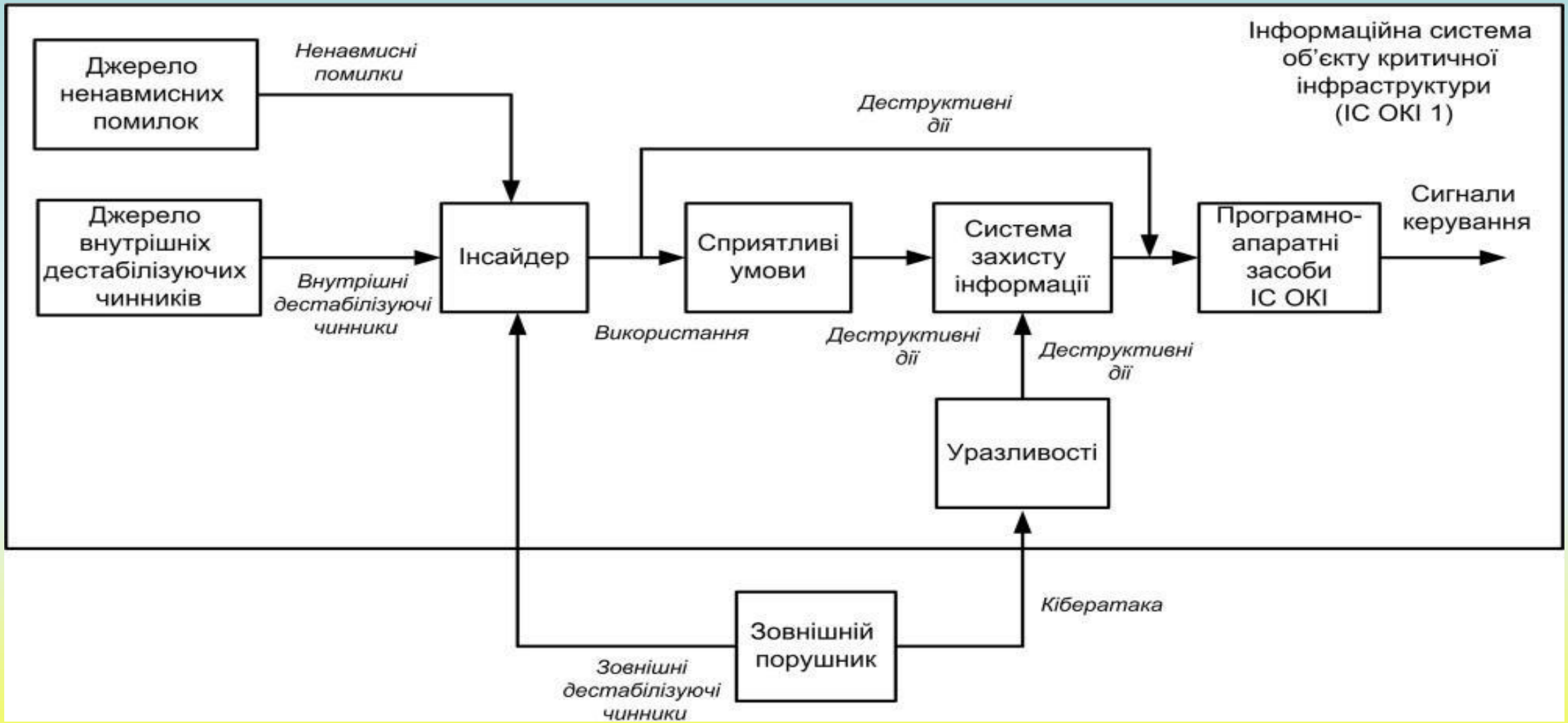
| | |
|---|---|
| **Вступ** | Обґрунтовано актуальність теми, сформульовано мету, завдання, об’єкт і предмет дослідження, визначено методи дослідження та практичну значущість роботи. |
| **Перший розділ** | Виконано аналіз предметної області, розкрито поняття та значення критичної інфраструктури, розглянуто нормативно-правове забезпечення кібербезпеки, проаналізовано наукові джерела та сформульовано проблему і постановку задачі дослідження. |
| **Другий розділ** | Досліджено сучасні кіберзагрози інформаційних систем об’єктів критичної інфраструктури, побудовано модель загроз, визначено ймовірність їх реалізації та виконано оцінювання небезпеки кібератак. |
| **Третій роділ** | Розроблено метрику кіберстійкості критичної інфраструктури, визначено її ключові компоненти, проведено оцінку рівнів стійкості та проаналізовано результати застосування запропонованого підходу. |
| **Висновок** | Узагальнено результати дослідження, сформульовано основні наукові та практичні висновки, визначено напрями подальших досліджень. |

## Методи дослідження:

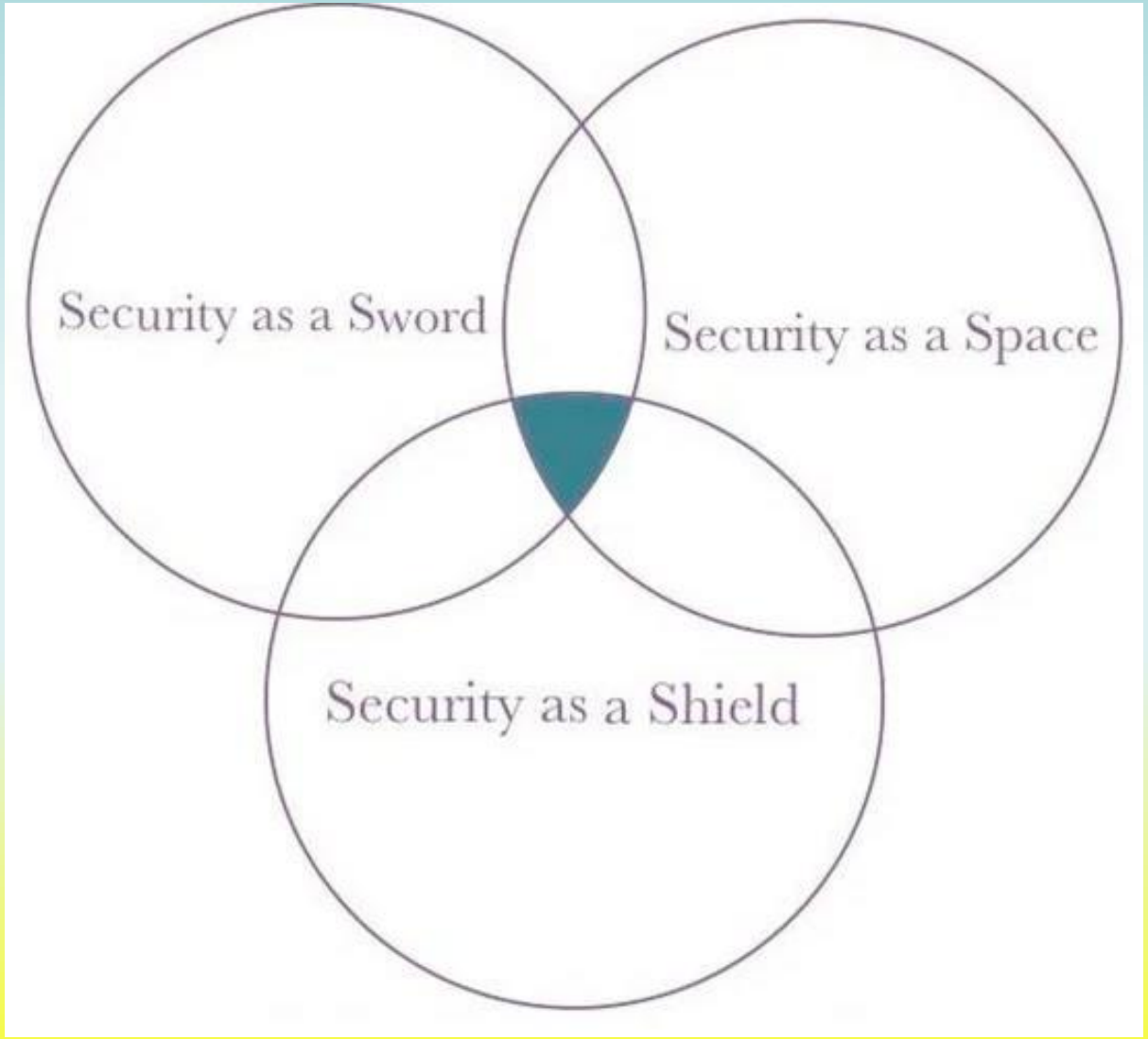
| | |
|---|---|
| **Методи системного аналізу** | Для дослідження структури та взаємозв'язків компонентів інформаційних систем об'єктів критичної інфраструктури. |
| **Методи аналізу та оцінювання ризиків** | Для визначення ймовірності реалізації кіберзагроз та оцінки їх потенційних наслідків. |
| **Методи моделювання загроз і вразливостей** | Для формування моделі кіберзагроз інформаційних систем ОКІ. |
| **Ризик-орієнтований та процесний підходи** | Для побудови метрики кіберстійкості та визначення рівнів зрілості безпекових процесів. |
| **Методи порівняльного аналізу** | Для зіставлення існуючих моделей і підходів до оцінки кіберстійкості. |
| **Методи узагальнення та експертної оцінки** | Для формування критеріїв, показників і шкал оцінювання кіберстійкості. |




**Взаємозв’язок між загрозами і деструктивними діями**




**Структурна модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури.**




**Класифікація підходів до кібербезпеки**

## Домени та компоненти в рамках кібербезпеки для критичної інфраструктури

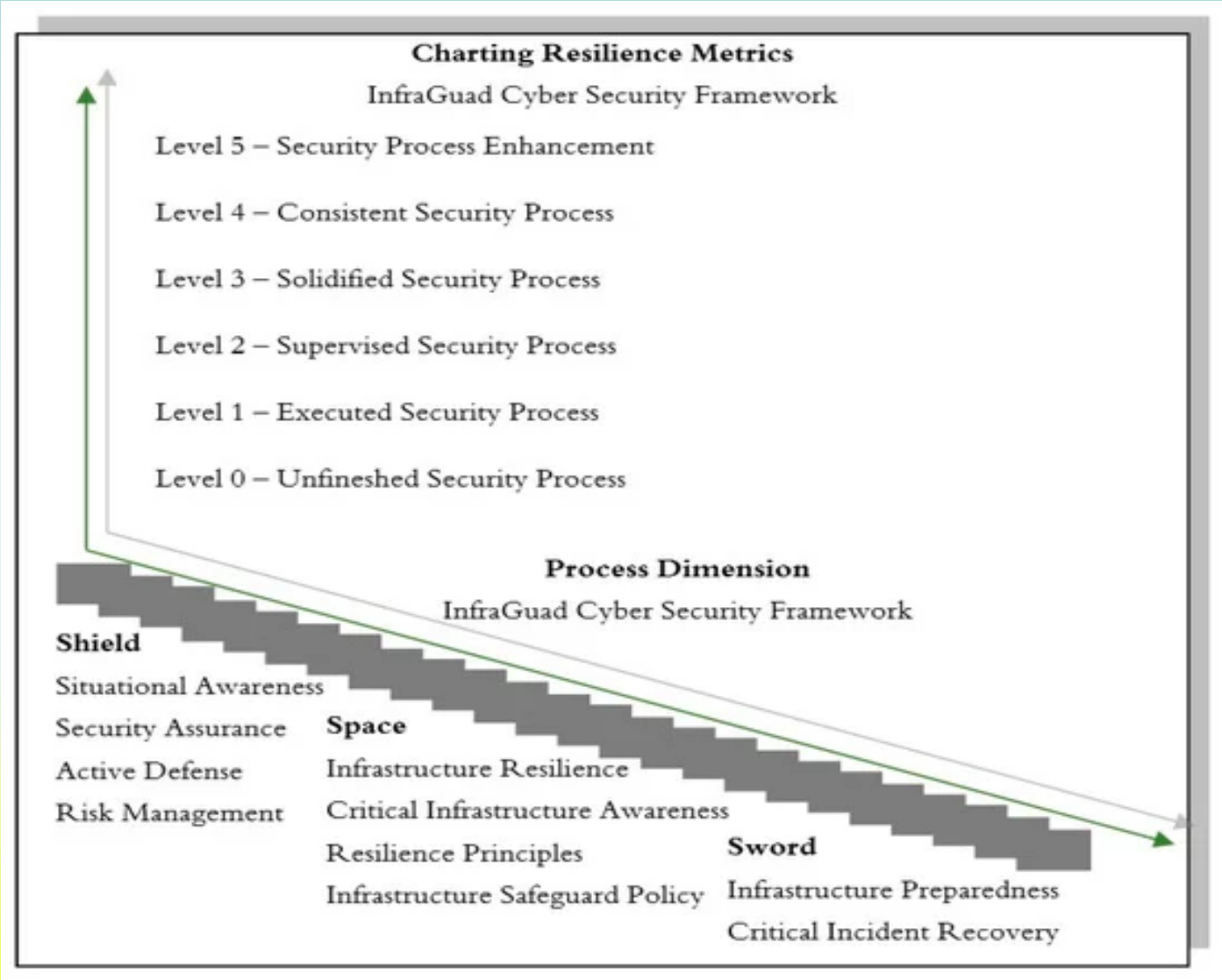
| Домен | Компонент | Індикатор | Опис |
|---|---|---|---|
| **Кіберпростір як щит** | Ситуаційна обізнаність | Можливості виявлення та моніторингу загроз | Організація може проактивно спостерігати за оперативними змінами та виявляти потенційні кіберзагрози. |
| | Гарантія безпеки | Оцінки ризиків та контроль безпеки | Включає рутинні оцінки та дотримання суворих стандартів для забезпечення захисту системи. |
| | Активний захист | Швидке реагування на загрози | Передбачає використання інструментів та стратегій для виявлення та запобігання атакам до того, як відбудеться пошкодження системи. |
| | Управління ризиками | Ідентифікація та пом'якшення ризиків | Систематичний процес оцінки загроз та визначення пріоритетів заходів щодо пом'якшення наслідків. |

## Домени та компоненти в рамках кібербезпеки для критичної інфраструктури

| Домен | Компонент | Індикатор | Опис |
|---|---|---|---|
| **Кіберпростір як космос** | Стійкість інфраструктури | Надійність системи та можливості відновлення | Інфраструктура може підтримувати роботу та відновлюватися під час або після кіберінцидентів. |
| | Поінформованість про критичну інфраструктуру | Організаційна обізнаність про життєво важливі системи | Глибоке розуміння національного значення інфраструктури та пов'язаних з нею ризиків. |
| | Принципи стійкості | Стійкий дизайн та операційна філософія | Основоположні принципи побудови систем, які можуть витримувати збої. |
| | Політика захисту інфраструктури | Захисна політика та процедури | Офіційні документи та процедури захисту фізичної та цифрової інфраструктури від загроз. |

## Домени та компоненти в рамках кібербезпеки для критичної інфраструктури

| Домен | Компонент | Індикатор | Опис |
|---|---|---|---|
| **Кіберпростір як меч** | Готовність інфраструктури | Попереджувальна готовність та навчання | Наявність планів реагування на інциденти, навчання персоналу та моделювання сценаріїв. |
| | Відновлення критичних інцидентів | Швидкість відновлення та заходи безперервності | Можливість швидко та ефективно відновлювати функції системи після збоїв. |




**Графік показників стійкості**

# Рівні компетентності процесу в системі кіберстійкості InfraGuard:

## Рівень 5:

Покращення процесу безпеки: Це найвищий рівень у структурі, де процеси безпеки були повністю оптимізовані. На цьому етапі процеси безпеки не тільки проходять гладко, але й постійно вдосконалюються та вдосконалюються на основі зворотного зв'язку та навчання на попередньому досвіді. Організації на цьому рівні досягли найвищого рівня зрілості в процесах безпеки, і кожен аспект оптимізований для повної ефективності. Організації на цьому рівні є лідерами в практиці кібербезпеки.

## Рівень 4:

Послідовний процес безпеки: на цьому рівні процеси безпеки працюють послідовно та передбачувано. Процеси дають послідовні результати та відповідають встановленим стандартам якості. Послідовність тут є ключовою, а це означає, що організації можуть покладатися на процеси безпеки для досягнення передбачуваних результатів без особливих варіацій або невизначеності. Організації на цьому рівні досягли дуже високого рівня стійкості у підтримці кібербезпеки.

# Рівні компетентності процесу в системі кіберстійкості InfraGuard:

## Рівень 3:

Закріплений процес безпеки: на цьому рівні процеси безпеки стали надійними та усталеними. Процеси виявилися ефективними на практиці і стали невід'ємною частиною повсякденних операцій. Це вказує на те, що організації успішно побудували міцну основу для своєї безпеки, і ці процеси вважаються зрілими практиками в їх діяльності. Організації на цьому рівні досягли високого рівня стійкості в підтримці своєї критичної інфраструктури.

## Рівень 2:

Контрольований процес безпеки: На цьому рівні процеси безпеки ретельно контролюються, щоб гарантувати, що всі дії відбуваються відповідно до запланованих та встановлених стандартів. Нагляд тут є вирішальним компонентом, і організації гарантують, що процеси безпеки розгортаються, як очікувалося, хоча все ще може бути місце для вдосконалення. Організації на цьому рівні прагнуть підвищити свою стійкість і планують необхідні кроки для досягнення вищого рівня.

# Рівні компетентності процесу в системі кіберстійкості InfraGuard:

## Рівень 1:

Виконаний процес безпеки: На цьому рівні виконуються процеси безпеки. Основні заходи безпеки були впроваджені, і процеси працюють відповідно до базового плану. Це початковий крок, який вказує на те, що організація вжила основних заходів для захисту своєї інфраструктури. Поки робота все ще залишається, був зроблений перший крок до стійкості.

## Рівень 0:

Незакінчений процес безпеки: це найнижчий рівень у системі, де процеси безпеки незавершені. Деякі аспекти процесів, можливо, не були реалізовані або можуть не функціонувати належним чином. Це вказує на те, що для досягнення гідного рівня стійкості потрібна значна робота.

## Резюме програми на основі сценаріїв

| Сценарій | Сектор | Головний інцидент | Технічні примітки | Ключові компоненти | Рівень стійкості |
|---|---|---|---|---|---|
| **Зрив електричної мережі** | Енергія (електромережа) | Цільова кібератака SCADA | Modbus TCP/IP, без шифрування, плоска мережа, ручне відновлення | Ситуаційна обізнаність, управління ризиками, активний захист | Дуже низький (Рівень 1) |
| **Розумна лікарня-вимагач** | Охорона здоров'я | Вимагацьке програмне забезпечення та медичне порушення Інтернету речей | Слабка сегментація, відсутність ІЧ-координації, застарілі резервні копії | Готовність, Стійкість, Відновлення Інцидентів | Розвиток (Рівень 2-3) |
| **Саботаж системи аеропорту** | Перевезення | Віджеж системи через компроміс ОТ | Застарілі ПЛК, SOC присутні, немає уніфікованих свердлів IT-OT | Готовність, захист, координація реагування | Сильний (Рівень 3–4) |

# Дослідницькі сценарії для застосування Framework:

## Сценарій 1:

Порушення національної електричної мережі - кібератака на державні системи SCADA електричної мережі ініціює широкомасштабні регіональні відключення електроенергії. Системи SCADA на базі Modbus TCP/IP не мають шифрування та автентифікації і, таким чином, сприйнятливі до командних ін'єкцій та викрадення сеансів. Погана конструкція сегментації мережі полегшує бічне переміщення між операційними зонами. Немає інвентаризації активів або рішень для управління інформацією про безпеку та подіями (SIEM), а відновлення відбувається вручну протягом 24 годин. Це підпадає під умови технічних вразливостей, використаних під час попередніх атак, таких як атака на мережу України 2015 року.

Ключові компоненти, що впливають: ситуаційна обізнаність, управління ризиками, активний захист;

Індикативний рівень стійкості: дуже низький (рівень 1).

# Дослідницькі сценарії для застосування Framework:

## Сценарій 2:

Вимагацьке програмне забезпечення в розумній лікарняній системі - Зараження столичної лікарняної мережі програмами-вимагачами шифрує електронні медичні записи та калічить медичне обладнання з підтегомом IoT. Сегментація в лікарні мінімальна, зі спільним доступом між адміністративними робочими станціями та клінічними системами. Немає активного та функціонального механізму реагування на інциденти, де викликається захист кінцевих точок. 12-година відновлення спричиняє тимчасове порушення процесів відділення інтенсивної терапії. Це тип викриття, який використовується в реальних атаках, таких як атаки WannaCry на мережі охорони здоров'я.

Ключові компоненти, що постраждали: готовність, стійкість інфраструктури, відновлення інцидентів;

Індикативний рівень стійкості: розвивається (рівень 2-3).

# Дослідницькі сценарії для застосування Framework:

## Сценарій 3:

Сценарій 3: Інцидент кіберсаботажу в аеропорту - відбувається кібератака на процеси координації польотів та обробки багажу в міжнародному аеропорту. Сертифікований ISO/IEC 27001 аеропорт централізовано контролюється SOC (Центр операцій безпеки) без живих кібернавчань або вправ червоної команди між відділами. Багажна система працює зі застарілими ПЛК з фірмовою, не виправленою прошивкою і знаходиться під компрометацією ланцюга поставок або інсайдерською експлуатацією. Його можна відновити протягом 5 годин, але аналіз після інциденту визначає, що немає консолідації протоколів між IT та OT командами.

Ключові компоненти, що постраждали: готовність інфраструктури, активний захист, інтеграція реагування;

Індикативний рівень стійкості: сильний (рівень 3-4).

# ВИСНОВКИ

У дипломній роботі розглянуто актуальну науково-прикладну проблему забезпечення кіберстійкості об’єктів критичної інфраструктури в умовах зростання інтенсивності та складності сучасних кіберзагроз. Проведений аналіз показав, що критична інфраструктура є ключовим елементом національної безпеки, економічної стабільності та соціальної життєздатності держави, а порушення її функціонування внаслідок кібератак може мати масштабні негативні наслідки.

У ході дослідження було проаналізовано сучасний стан і тенденції розвитку критичної інфраструктури, визначено основні типи загроз для її інформаційних та кіберфізичних компонентів, зокрема атаки типу ransomware, APT-кампанії, DDoS-атаки, уразливості операційних технологій та людського фактору. Показано, що традиційні підходи до кіберзахисту, орієнтовані переважно на запобігання атакам, є недостатніми, оскільки не враховують здатність системи адаптуватися, відновлюватися та зберігати критичні функції під час інцидентів.

# ВИСНОВКИ

Значну увагу в роботі приділено аналізу нормативно-правової бази у сфері кібербезпеки об’єктів критичної інфраструктури. Розглянуто законодавство України, підзаконні акти, державні стратегії та міжнародні стандарти (ISO/IEC 27001, ISO/IEC 27005, NIST CSF, вимоги Директиви NIS2 ЄС). Установлено, що чинні нормативні документи визначають загальні вимоги до кіберзахисту, однак не містять єдиної формалізованої методики кількісної оцінки кіберстійкості, що ускладнює процес прийняття управлінських рішень.

На основі аналізу наукових джерел і сучасних підходів до оцінювання стійкості запропоновано методику оцінки кіберстійкості об’єктів критичної інфраструктури, яка базується на ризик-орієнтованому підході та інтегрує технічні, організаційні й управлінські аспекти кіберзахисту. Методика передбачає формування системи критеріїв і показників, що відображають здатність об’єкта запобігати кібератакам, виявляти інциденти, реагувати на них та відновлювати функціонування з мінімальними втратами.

# ВИСНОВКИ

У рамках роботи розроблено інформаційно-аналітичний механізм для реалізації запропонованої методики, який дозволяє автоматизувати процес збору та обробки даних, розрахунок показників кіберстійкості та формування рекомендацій щодо підвищення рівня захищеності. Практичне застосування запропонованого підходу продемонструвало його придатність для використання в різних секторах критичної інфраструктури та можливість адаптації до специфіки конкретних об’єктів. Отримані результати підтверджують доцільність переходу від виключно захисних моделей кібербезпеки до концепції кіберстійкості, яка забезпечує комплексний підхід до управління ризиками та безперервністю функціонування критичних систем. Практична цінність роботи полягає в можливості використання розробленої методики під час проведення аудитів кібербезпеки, оцінювання ризиків, планування заходів із підвищення стійкості та підтримки прийняття управлінських рішень у сфері захисту об’єктів критичної інфраструктури.

INDEX COPERNICUS

GS 141125-066 dated 14.11.2025

# CERTIFICATE
## OF PARTICIPATION AND PUBLICATION

**Dmytro Dudynets**

participated in the X Correspondence International Scientific and Practical Conference

**Scientific researches and methods of their carrying out: world experience and domestic realities**

held on November 14th, 2025 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

and published scientific paper

***МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРІНЦЕДЕНТІВ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ***

in Periodical scientific journal «**GRAIL OF SCIENCE**»

№ **58**. ISSN 2710-3056; Media identifier R30-02704;
DOI 10.36074/grail-of-science.14.11.2025

IHTIC

**0.6 ECTS credits (18 hours)**
Recommended by the Academic Council of the «Institute of Scientific and Technical Integration and Cooperation». Protocol № 45 from November 13th, 2025.

Head of the
NGO «European Scientific Platform»
Chairman of the Organizing committee
**GOLDENBLAT MIRIAM**

Head of Community Outreach at the
LLC «International Centre
Corporative Management»
**RACHAEL APARO**

# ДЯКУЮ ЗА УВАГУ!