PROCEEDINGS

1ST INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «RESILIENT SYSTEMS: SECURE DIGITAL TECHNOLOGIES AND CRITICAL INFRASTRUCTURE» (RS-2025)

June 27, 2025

Drohobych, 2025

UDC 004.56/004.08/519.6
DOI: 10.5281/ZENODO.15775240

CONFERENCE ORGANIZING:

Donetsk National Technical University
G. E. Pukhov Institute for Modeling Problems in Energy Engineering, NAS of Ukraine
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Cherkasy State Technological University
Ternopil Ivan Puluj National Technical University
State University "Zhytomyr Polytechnic"
Lviv State University of Life Safety
National Aerospace University "Kharkiv Aviation Institute"
Berdyansk State Pedagogical University
Odesa National University of Economics
State Service for Special Communications and Information Protection of Ukraine
National Bank of Ukraine
University of Zielona Góra (Poland)
Academy of Silesia (Poland)
State University of Western Paraná (Brazil)
Copenhagen Business School (Denmark)

Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference. Drohobych: Donetsk National Technical University, 2025. 184 pp.

The proceeding contains materials of the conference on theoretical and practical problems of AI, cybersecurity and critical infrastructures.

Recommended for publication by the Academic Council of the State Higher Educational Institution 'Donetsk National Technical University'

The materials are submitted in the author's edition

ORGANIZING COMMITTEE

Chair of the Organizing Committee:

Iaroslav DOROHYI – DSc, Professor, Head of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Deputy Chair of the Organizing Committee:

Mykyta ALEKSANDROV – PhD**,** Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Members of the Organizing Committee:

Yevhen BASHKOV – DSc, Professor, Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Tetiana ALTUKHOVA – CSc, Associate Professor, Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Iryna NAZAROVA – CSc, Associate Professor, Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Yelyzaveta YEZHOVA – Assistant Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Dmytro KHOMA – Assistant Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

PROGRAM COMMITTEE

Chair of the Program Committee:

Yaroslav DOROHYI – DSc, Professor, Head of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Deputy Chair of the Program Committee:

Yevhen BASHKOV – DSc, Professor, Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Members of the Program Committee:

Volodymyr MOKHOR – Corresponding Member of NASU, DSc, Professor, Director, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Oleksandr CHEMERYS – DSc, Professor, Deputy Director for Research, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Serhii HILHURT – DSc, Senior Researcher, Head of the Department of Mathematical and Econometric Modeling, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Dmytro LANDE – DSc, Professor, Head of the Department of Information Security, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” (Ukraine).

Anatolii CHEPYNOHA – CSc, Associate Professor, Dean of the Faculty of Information Technologies and Systems, Cherkasy State Technological University (Ukraine).

Roman PROSKUROVSKYI – CSc, Associate Professor, Head of the Critical Infrastructure Protection Division, National Bank of Ukraine (Ukraine).

Oleksandr BAKALYNSKYI – CSc, Senior Researcher, Senior Specialist of the Critical Infrastructure Protection Department, National Bank of Ukraine (Ukraine).

Serhii MARTSENKO – CSc, Associate Professor, Associate Professor of the Department of Computer Science, Ternopil Ivan Puluj National Technical University (Ukraine).

Andrii YEFIMENKO – CSc, Associate Professor, Head of the Department of Computer Engineering and Cybersecurity, State University “Zhytomyr Polytechnic” (Ukraine).

Maryna HRAF – PhD, Associate Professor, Head of the Department of Computer Science, State University “Zhytomyr Polytechnic” (Ukraine).

Nataliia MASLOVA – CSc, Associate Professor, Department of Information Security Management, Lviv State University of Life Safety (Ukraine).

CONTENTS

SECTION 1: ARTIFICIAL INTELLIGENCE

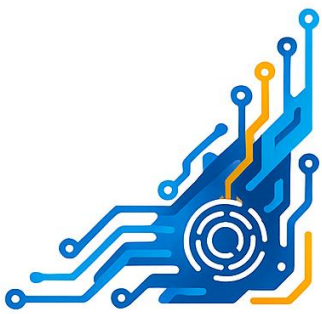
SECTION 2: CYBERSECURITY AND CRITICAL INFRASTRUCTURE

SECTION 3: INFORMATION TECHNOLOGIES

SECTION 4: COMPUTER AND MATHEMATICAL MODELING

Oleksandr Shtepa

SECTION 5: DIGITAL SYSTEMS



METHODOLOGY FOR ORGANIZING A ZETTELKASTEN-STYLE KNOWLEDGE BASE FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Illia Harbaruk, Iaroslav Dorohyi, Nataliya Maslova

МЕТОДИКА ОРГАНІЗАЦІЇ БАЗИ ЗНАНЬ У СТИЛІ ZETTELKASTEN ДЛЯ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

І. Гарбарук[1], Я. Дорогий[1], Н. Маслова[2]
[1]Донецький національний технічний університет, (Україна),
[2]Львівський державний університет безпеки життєдіяльності (Україна)

Анотація. У роботі розглянуто використання підходу Zettelkasten як методологічної основи для побудови спеціалізованої бази знань, орієнтованої на потреби захисту критичної інформаційної інфраструктури (КІІ). Обґрунтовано, що класичні моделі організації інформації не забезпечують достатньої гнучкості та зв'язності в умовах високої складності й динаміки загроз. Запропоновано застосування графової моделі знань, реалізованої в середовищі Obsidian.md, для структурування нормативних, технічних та аналітичних компонентів кібербезпеки КІІ. Представлено методику створення такої бази, що включає збір, класифікацію, побудову зв'язків і оцінку повноти знань із використанням спеціалізованих інструментів. Показано, що такий підхід дозволяє формувати адаптивну, масштабовану систему знань для підтримки прийняття рішень і забезпечення багаторівневої безпеки інфраструктурних об'єктів.

Вступ. У сучасних умовах зростання кіберзагроз особливого значення набуває безпека об'єктів критичної інформаційної інфраструктури (КІІ). Їхній захист вимагає глибокого, актуального та структурованого знання. Система Zettelkasten, заснована на принципах створення взаємопов'язаних атомарних нотаток, на її основі може бути створена перспективна методика побудови спеціалізованої бази знань, орієнтованої на підтримку процесів аналізу та забезпечення безпеки КІІ.

Критичні інфраструктури характеризуються високою складністю, міждисциплінарністю й динамікою змін – нові загрози, вразливості, техніки атак і методи захисту постійно оновлюються. Фахівці мають інтегрувати знання з різних джерел: нормативно-правових актів, технічних стандартів (NIST, ISO 27001/27035, OWASP), дослідницьких статей, OSINT-даних тощо. Zettelkasten дозволяє формувати персоналізовану базу знань, яка зберігає контекст, підтримує еволюцію ідей і сприяє підготовці висококваліфікованих спеціалістів, оцінюванню повноти знань й прийняттю актуальних рішень щодо захисту критичних інфраструктур та систем.

Постановка задачі. Метою дослідження є оцінка доцільності та ефективності побудови структурованої бази знань за методом Zettelkasten як основи аналізу повноти, зв'язності та актуальності захисту КІІ. Завдання:

- проаналізувати вимоги до знань у сфері захисту критичних інфраструктур;

- висвітліти можливості Obsidian як інструменту реалізації Zettelkasten для практичних завдань: audit, risk assessment, incident response;

- запропонувати методику **ведення бази знань у стилі Zettelkasten для захисту КІІ.**

Основна частина. Захист критичної інформаційної інфраструктури (КІІ) вимагає від фахівців не лише загальних знань з кібербезпеки, а й глибокого розуміння специфіки технологічних процесів, нормативно-правового середовища та міждисциплінарних ризиків. На відміну від звичайних інформаційних систем, об'єкти КІІ часто включають промислові контролери, SCADA-системи, телекомунікаційні вузли або енергетичне обладнання, функціонування яких критично залежить від безперервності та точності. Це означає, що знання фахівця мають охоплювати не тільки технічні аспекти (наприклад, вразливості протоколів Modbus, OPC UA чи IEC 60870-5-104), а й логіку виробничих процесів, правила реагування на інциденти в реальному часі та вимоги державних регуляторів.

Крім того, така сфера вимагає розуміння стандартів (зокрема ISO/IEC 27001, NIST SP 800-82, IEC 62443), здатності інтегрувати відкриті джерела (OSINT) для виявлення потенційних загроз та навичок побудови моделей загроз, які враховують як кіберфізичну взаємодію, так і людський фактор. В умовах гібридних загроз особливо важливою стає здатність працювати з неструктурованою інформацією, виявляти приховані зв'язки між подіями та швидко адаптуватися до змін ситуації.

У контексті захисту складних об'єктів критичної інформаційної інфраструктури (КІІ) особливу роль відіграє спосіб організації знань – не лише як накопичення інформації для аналізу захищеності структур, а як основа для швидкого прийняття рішень, виявлення взаємозв'язків між подіями та формування аналітичних висновків. В процесі дослідження було проаналізовано декілька моделей організації нотаток: ієрархічну, тегову (Flat + Tagging), Dewey-style та Zettelkasten – з акцентом на їх придатність до структуризації складної, динамічної та міждисциплінарної інформації. Результати аналізу відображено в Таблиці 1.

Таблиця 1 - Моделі організації нотаток

Модель	Тип моделі	Відповідність сфері КІІ
Folder-based	ієрархічна	Недостатня, через жорсткість ієрархії; проблеми з багатоконтекстністю подій і вразливостей
Flat + Tagging	Пласка структура з тегами	Орієнтована на користувача, **без чіткої таксономії, гнучкість тегів** дозволяє швидко фільтрувати чи знаходити потрібні нотатки при умові правильного налаштування
Dewey-style	Чітка ієрархічна	Не дозволяє побудувати багатовимірне уявлення про КІІ
Zettelkasten	Графова, ассоціативна	Підходить для складних систем; підтримує багатовимірність та гнучкість

У контексті складності інфраструктурних об'єктів, саме Zettelkasten виявляється найбільш ефективною моделлю – завдяки своїй здатності відображати взаємозв'язки між багатьма рівнями інформації, підтримувати ідеї та забезпечувати гнучку навігацію в умовах невизначеності.

Підхід Zettelkasten, започаткований соціологом Нікласом Луманом сприяє глибокому осмисленню інформації, формуванню міждисциплінарних та міжоб'єктних зв'язків [1]. Ці переваги особливо актуальні в умовах високої динаміки та складності сфери кібербезпеки, зокрема щодо захисту об'єктів критичної інформаційної інфраструктури (КІІ).

Однак, як засвідчує сучасна література, підхід Zettelkasten недостатньо інтегрований у системи інформаційної безпеки, особливо в частині інцидент-менеджменту, оцінки ризиків та реагування на атаки на КІІ. Окремі дослідження зосереджуються на використанні відкритих джерел (OSINT) для виявлення загроз [2], а також на методологіях penetration testing у контексті SCADA, IoT та енергетичних систем [3]. Проте системне поєднання цих підходів із побудовою предметної бази знань залишається перспективним напрямом. Таким чином, на тлі зростаючих загроз для критичної інфраструктури виникає потреба в дослідженні й адаптації Zettelkasten як методології, що здатна підтримувати аналітичну діяльність та оперативне прийняття рішень в умовах змінної ситуації у сфері кібербезпеки.

Для реалізації підходу Zettelkasten найчастіше використовуються спеціалізовані цифрові інструменти, що підтримують створення взаємопов'язаних атомарних нотаток. У порівняльних оглядах інструментів персонального управління наборами інформації ([4], [5]) описано особливості платформ Roam Research, RemNote, Zettlr та Obsidian.md. Obsidian вирізняється як найбільш функціональний і придатний для роботи з технічно складними й міждисциплінарними темами, зокрема в галузі кіберзахисту КІІ [6].

Obsidian.md – це офлайн-редактор на базі Markdown, який забезпечує двонаправлені посилання, граф знань, систему тегів, шаблонів і розширення через плагіни. Obsidian.md є потужним інструментом реалізації підходу Zettelkasten, що чітко може проявитися у виконанні практичних завдань, таких як аудит безпеки, оцінка ризиків (risk assessment) та реагування на інциденти (incident response). Завдяки підтримці двонаправлених посилань, Obsidian дозволяє пов'язувати нормативні вимоги, знайдені вразливості, сценарії атак та дії реагування в єдину логічну мережу. Це особливо корисно під час аудиту, коли потрібно швидко зіставляти технічні характеристики систем із вимогами стандартів (наприклад, ISO 27001 або IEC 62443) та документувати відповідність.

Під час оцінки ризиків Obsidian дозволить створювати окремі нотатки для активів, загроз, вразливостей і контрзаходів, пов'язуючи їх між собою у вигляді графа. Така структура полегшує візуалізацію потенційних шляхів атаки й наслідків, а також дозволяє доповнювати базу даних у міру зміни контексту або появи нових даних.

У процесі реагування на інциденти, система дозволить підтримати швидкий доступ до SOP-документів, чек-листів, історії аналогічних випадків і контактних даних відповідальних осіб. Використання тегів (наприклад, #інцидент, #вразливість, #CVE) і шаблонів дозволяє стандартизувати ведення записів про інциденти, а плагін Graph Analysis – виявляти слабко пов'язані ділянки знань, які потребують доопрацювання.

Тож, Obsidian забезпечує не лише зберігання знань, а й розвиток аналітичного мислення, формування зв'язків між подіями, поняттями та діями – що є критично важливим для оперативного та обґрунтованого прийняття рішень у сфері кібербезпеки.

Результати. Безпосереднє значення для побудови цілісної бази даних про загрози, сценарії атак і відповідні захисні заходи, що стосуються об'єктів КІІ мають бази знань OSINT та penetration testing, оскільки саме ці напрямки дають змогу виявити вразливості, які можуть бути використані для компрометації життєво важливих систем.

OSINT (Open Source Intelligence) дозволяє збирати відомості з відкритих джерел – зокрема, про конфігурації мереж, публічно доступних IP-адрес, версій ПЗ, вразливих сервісів та навіть інформацію щодо помилкових дій персоналу. Для об'єктів КІІ, які часто мають зовнішні точки доступу (наприклад, віддалений моніторинг SCADA або веб-інтерфейси контролерів), OSINT дає змогу виявити потенційні цілі ще до початку активної фази атаки. Зібрана інформація може бути використана як частина моделі загроз та сценаріїв впливу.

Penetration testing імітує дії зловмисника й дозволяє перевірити реальну стійкість системи до атак. Для КІІ це особливо важливо, адже багато таких систем використовують застарілі або погано захищені технології, а можливість порушення їх роботи може призвести до фізичних наслідків (зупинка виробництва, енергетичного забезпечення тощо). Наявність бази знань, яка акумулює типові вектори атак, відомі CVE, результати попередніх тестувань, а також рекомендації щодо їх усунення, значно підвищує ефективність захисту.

Таким чином, інтегровані бази знань з OSINT і pentest слугують не лише інструментом технічного аналізу, а й основою для побудови заснованої на даних системи прийняття рішень у сфері захисту КІІ. Вони дозволяють бачити як загрозу в цілому, так і взаємозв'язки з іншими факторами, що є критично важливим для формування превентивних та адаптивних заходів кіберзахисту. На рисунку 1 представлено приклад, що ілюструє завдання з розслідування за електронною поштою в межах OSINT, яке, з огляду на використання техніки Google Dorks, має методичний зв'язок із тестуванням на проникнення.

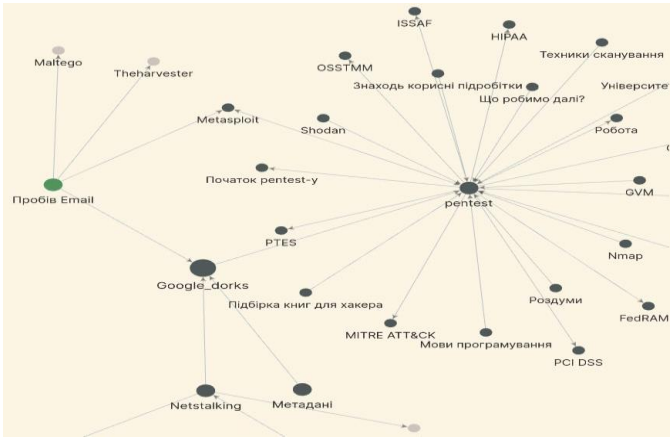


Рисунок 1 – Приклад виявлення комплексних зв'язків у системах аналізу КІІ

У контексті забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури це свідчить про перетин між інструментами пасивного збору даних і активними методами оцінювання вразливостей. Таким чином, на прикладі двох формально різних напрямів – OSINT і pentest – демонструється інтеграція підходів, що є характерною для комплексного аналізу кіберризиків у системах КІІ.

Методика ведення бази знань у стилі Zettelkasten для захисту КІІ. Методика Zettelkasten у сфері захисту критичної інформаційної інфраструктури полягає у поступовому створенні гнучкої, контекстно насиченої бази знань на основі атомарних нотаток, що пов'язані між собою двонаправленими зв'язками, доповнені тегами, джерелами, прикладами з практики та інтегровані в реальні процеси оцінки ризиків, аудиту, реагування на інциденти і моделювання загроз. Підхід дозволяє не лише систематизувати розрізнену інформацію, а й виявляти нові взаємозв'язки, прогалини у знаннях та підтримувати їх актуальність завдяки регулярному огляду й аналізу структури графа. Схема пропонованої методики наведена на рисунку 2.

Рисунок 2 – Схема методики ведення бази знань у стилі Zettelkasten для захисту КІІ

1. Підготовчий етап: формулювання мети та структури знань. На цьому етапі визначається ціль: наприклад, формування тематично повної бази знань, яка охоплює всі аспекти захисту КІІ (нормативні, технічні, процедурні) та дозволяє проводити аналіз повноти й узгодженості заходів безпеки.

2. Етап "fleeting" та "literature notes" (Збір інформації). Використовуються OSINT-джерела, технічна документація, наукові статті, стандарти, звіти CERT-UA, MITRE ATT&CK for ICS. Занотовуються короткі ідеї (fleeting notes) одразу в Obsidian. Одна ідея = одна нотатка. Створювати "literature notes" – нотатки з ключовими положеннями джерел із зазначенням джерела (через шаблон або плагін Citations).

3. Створення "постійних нотаток" (permanent notes). Сформулювати власними словами чіткі, атомарні твердження: кожна постійна нотатка містить одну ідею (наприклад, "Вразливість протоколу Modbus дозволяє здійснити DoS без автентифікації"). Обов'язково додаються двонаправлені посилання на суміжні поняття, приклади атак, пов'язані нормативи, методи захисту тощо. На цьому етапі використовується тегування (наприклад, #вразливість, #інцидент, #scada, #IEC62443).

4. Побудова графа знань. Граф формується автоматично через режим графа (graph view) – кожна нова нотатка з лінками створює новий вузол у просторі знань. Створюються Maps of Content (MOC) – індексні нотатки з навігацією по темах (наприклад: "Penetration testing for KII" → списки пов'язаних нотаток).

5. Регулярне рев'ю й уточнення знань. Періодично (наприклад, раз на тиждень) слід використовувати плагін "Random Note" або планувальник для повторного перегляду раніше створених нотаток. Уточнювати, зв'язувати, розширювати – не видаляючи старе.

6. Аналіз повноти знань (через Graph Analysis). Встановити плагін Graph Analysis і виконати обчислення основних метрик (Density – щільність зв'язків між нотатками; HITS – ключові вузли (основні теми знань); Louvain clustering – тематичні кластери (наприклад, «OSINT», «Інциденти», «IEC 62443»); Isolated notes – виявлення ізольованих записів (прогалини у знаннях); Adamic-Adar – пошук потенційних, ще не встановлених зв'язків).

7. Формування звітів і рефлексії – це документування результатів аналізу у спеціальній нотатці типу “Review_КІІ_дата”, збереження графів візуалізації у вигляді скріншотів або PDF.

8. Етап інтеграції з практичними задачами – це використання бази знань для:

- моделювання загроз (наприклад, TTP з MITRE ATT&CK),
- підготовки до аудиту (посилання на пункти нормативів),
- реагування на інциденти (чеклісти, типові сценарії),
- створення шаблонів інцидентів або процедур SOC у вигляді повторюваних структур.

Ця методика дозволяє створити гнучку, масштабовану, контекстно багату базу знань, що підтримує реальні практики у сфері захисту КІІ. Об’єднання Zettelkasten-логіки з можливостями Obsidian забезпечує не лише зберігання, а й розвиток знань, їх перевірку, самоаналіз і застосування у критичних ситуаціях.

Висновки. У результаті дослідження підтверджено доцільність і ефективність використання підходу Zettelkasten для систематизації знань щодо захисту об'єктів критичної інформаційної інфраструктури (КІІ). Проаналізовано вимоги до обсягу та структури знань, необхідних фахівцям, які працюють з КІІ, а також продемонстровано обмеження традиційних моделей організації нотаток у цій сфері.

З огляду на складність і динамічність предметної області, найбільш придатною виявилася графова, асоціативна модель Zettelkasten, реалізована в застосунку Obsidian.md. Обґрунтовано її ефективність для підтримки практичних завдань: аудиту, оцінки ризиків, реагування на інциденти, а також для пошуку неявних зв’язків (OSINT і penetration testing).

Використання середовища Obsidian.md дозволяє інтегрувати нормативні, технічні та процедурні компоненти безпеки в єдину мережеву структуру, що придатна для аналізу повноти охоплення, виявлення прогалин та асоціативного пошуку. Запропонована методика охоплює весь життєвий цикл побудови бази знань – від збору та фрагментації інформації до її перегляду, аналітики та інтеграції в управлінські та операційні процеси захисту КІІ.

Таким чином, реалізація підходу Zettelkasten у контексті захисту КІІ може розглядатися як один із інструментів формування оперативно придатного, аналітично цінного та динамічного інструменту для оцінки комплексності, зв’язності та готовності системи захисту інфраструктурних об’єктів від кіберзагроз.

ЛІТЕРАТУРА

1. Аренс З. *Як писати розумні нотатки. Система Zettelkasten і наука продуктивного письма*. – Київ: Yakaboo Publishing, 2022. – 240 с.
2. Reiss, M., & Reuter, C. *OSINT for Critical Infrastructure Protection: Challenges and Opportunities*. // Journal of Information Warfare. – 2021. – Vol. 20(3). – С. 35–47.
3. Kubecka, R. *Penetration testing in SCADA and industrial environments*. // Industrial Cybersecurity Journal. – 2020. – Vol. 4(2). – С. 14–26.
4. Gessner, A. *Zettelkasten software comparison: Roam, RemNote, Zettlr, Obsidian* [Електронний ресурс]. – 2020. – Режим доступу: https://zettelkasten.de/posts
5. Obsidian.md. *Documentation* [Електронний ресурс]. – Режим доступу: https://help.obsidian.md
6. David, D. *How I use Graph Analysis in Obsidian to find knowledge gaps* [Електронний ресурс]. – 2023. – Режим доступу: https://every.to/superorganizers/graph-analysis-in-obsidian