УДК 004.056.55:004.738.5
DOI: 10.31673/2409-7292.2025.026087

**Івкова В.С., Банах Р.І.**

# МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ СТАНУ ЗАХИЩЕНОСТІ ХМАРНИХ ТЕХНОЛОГІЙ ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ

У статті досліджується актуальна проблема забезпечення кібербезпеки хмарних сховищ у контексті стрімкої цифрової трансформації та зростаючої залежності організацій від хмарних технологій. Автори пропонують системну методологію оцінки стану захищеності хмарних середовищ із використанням інструментів розвідки на основі відкритих джерел (OSINT), яка дозволяє виявляти потенційні вразливості без прямої взаємодії з об'єктом дослідження. Розроблена методологія охоплює повний цикл OSINT-дослідження: від формування цілей і вибору релевантних інструментів – до збору, аналізу та документування даних. Особлива увага приділяється загрозам, характерним для хмарних сховищ, таким як неправильні конфігурації, компрометація облікових записів, незахищені API, витоки даних та інсайдерські ризики. Представлено приклади OSINT-інструментів і технік для виявлення цих загроз (Shodan, Censys, Google Dorks, Have I Been Pwned тощо). Стаття також акцентує увагу на важливості етичного підходу до дослідження, підкреслюючи необхідність дотримання законодавства під час збору інформації з відкритих джерел. Окремо розглянуто переваги OSINT як інструменту безпечної, економічно ефективної та оперативної оцінки рівня захищеності хмарної інфраструктури. Запропонована методологія є цінним практичним інструментом для фахівців із кібербезпеки, аудиторів та дослідників, що дозволяє ефективно виявляти вразливості в

**Ключові слова**: кібербезпека, хмарні сховища, OSINT, розвідка на основі відкритих джерел, безпека даних, вразливості, аналіз ризиків.

## Вступ

Епоха цифрової трансформації характеризується стрімким зростанням обсягів даних та активним переходом організацій до використання хмарних технологій для зберігання та обробки даних. Хмарні технології, зокрема хмарні сховища, завдяки своїй масштабованості, гнучкості та економічній ефективності, стали невід'ємною частиною сучасної IT-інфраструктури. Проте, зростаюча залежність від хмарних сервісів також супроводжується новими викликами у сфері кібербезпеки.

Неправильні конфігурації, недостатній контроль доступу, людський фактор та складність управління розподіленими хмарними середовищами створюють потенційні можливості для витоку конфіденційної інформації та інших кіберінцидентів [1, 2].

У цьому контексті, методи розвідки на основі відкритих джерел відіграють все більш важливу роль. OSINT дозволяє здійснювати неінвазивне дослідження інформації, що знаходиться у публічному доступі, для виявлення потенційних вразливостей та оцінки рівня захищеності цільових систем, включаючи хмарні сховища. На відміну від активних методів тестування на проникнення, OSINT не передбачає прямої взаємодії з досліджуваною інфраструктурою, що робить його безпечним та етичним способом отримання цінних розвідувальних даних [3, 4].

Компанія «TechMagic» у звіті, оновленому на початку 2025 року, вказує, що "86% організацій вже використовують мультихмарний підхід" і "понад 70% компаній перенесли принаймні частину своїх робочих навантажень до публічних хмарних сервісів." Одночасно з цим, згідно звіту компанії від 24 квітня 2025 року під назвою «Must-Know Cloud Security Statistics for 2025», 84% організацій мають принаймні один занедбаний актив, орієнтований на громадськість; 81% компаній з вищезазначеної категорії, мають ці активи з відкритими портами, що часто використовуються.

В той же час 61% організацій мають користувача root або власника облікового запису без багатофакторної автентифікації, а менше 10% підприємств зашифрували 80% або більше своїх даних у хмарі. [5]

Також, за даними організацій Statista, Cybersecurity Insiders, Check Point, - 64% компаній, які приймали учать у дослідженні та впроваджують хмарні технології, назвали втрату/витік даних найбільшою проблемою безпеки хмарних сервісів.

**Аналіз літературних джерел та формулювання проблеми**

Дослідження в області безпеки хмарних обчислень продовжують активно розвиватися, охоплюючи широкий спектр тем, від фундаментальних принципів безпеки до специфічних вразливостей окремих хмарних сервісів. Праці Зіссіса Д., Леккаса Д., Ранича В. та Ковальчука С. детально розглядають архітектурні особливості різних моделей хмарних сервісів (IaaS, PaaS, SaaS) та пов'язані з ними ризики безпеки, підкреслюючи необхідність адаптованих підходів до забезпечення захисту [6, 7].

У сфері застосування OSINT для цілей кібербезпеки з'являються нові дослідження, що вивчають ефективність різних інструментів та технік для виявлення конкретних типів загроз. Роботи Хілтона Д. та Ользака Т. акцентують увагу на використанні OSINT для проактивного виявлення витоків даних, аналізу соціальної інженерії та ідентифікації потенційних цілей для кібератак. Огляд наукової літератури свідчить про активне впровадження OSINT як інструменту оцінки стану кібербезпеки. Ранні дослідження показували потенціал відкритих джерел для виявлення ознак кіберзагроз, однак сучасні підходи охоплюють уже комплексні моделі оцінювання, які дозволяють формувати структуровані профілі ризиків.

Зокрема, Ланде і Шнурко-Табакова (2021) зазначають, що «OSINT-аналіз дозволяє своєчасно виявляти інформаційні індикатори кіберзагроз, формуючи систему раннього попередження». Це твердження підкреслює значення OSINT як компонента системи виявлення загроз (Threat Intelligence), що дозволяє не лише реагувати, але й прогнозувати інциденти [8].

An та Eom (2019) представили систему CloudSafe — програмний засіб для автоматизованого аналізу конфігурацій безпеки в хмарних середовищах. Вона базується на використанні OSINT-даних, що збираються з відкритих API, сканерів інфраструктури та доступних конфігурацій. Інструмент дозволяє оперативно ідентифікувати конфігураційні помилки, що створюють потенційні вектори атак [9].

Banse і Kunz (2022) розробили концепцію Cloud Property Graph — графової моделі, яка поєднує результати статичного аналізу програмного коду з даними, отриманими з відкритих джерел. Такий підхід дозволяє виявити приховані взаємозв’язки між компонентами хмарної інфраструктури і загрозами, пов’язаними з ними, включаючи потенційні витоки або неправомірні привілеї [10].

Mukhopadhyay та Luther (2023) у межах ініціативи OSINT Clinic продемонстрували, що навіть обмежені за ресурсами організації можуть отримати суттєву вигоду від використання відкритих джерел для виявлення власних цифрових вразливостей. Методика включає в себе створення карти цифрового сліду, перевірку витоків, аналіз налаштувань доступу, використовуючи лише публічно доступні інструменти та сервіси [11].

Отже, літературні джерела підтверджують ефективність OSINT як методологічного підходу до дослідження кібербезпеки, що набуває особливої актуальності у контексті хмарних технологій. Існує потреба в адаптації і формалізації цих підходів до умов локальних інфраструктур і нормативно-правових обмежень. У загальнодоступних статтях на форумах розглядаються специфічні OSINT-інструменти та методи, адаптовані для виявлення неправильних конфігурацій публічних хмарних сховищ, аналізу метаданих та ідентифікації випадково розкритих облікових даних. Проте, існує потреба у більш комплексних та систематизованих методологіях, які б враховували різноманітність хмарних сервісів та складність їхньої конфігурації. Дана стаття має на меті не лише систематизувати існуючі підходи, але й запропонувати більш глибоку та деталізовану методологію, яка б враховувала специфіку різних моделей хмарних сервісів та забезпечувала всебічну оцінку їхньої захищеності за допомогою OSINT-інструментів.

**Мета роботи та цілі дослідження**

Метою даної статті є розширення та поглиблення методології дослідження стану захищеності хмарних сховищ за допомогою OSINT-інструментів.

© Івкова В.С., Банах Р.І. (2025). Методологія дослідження стану захищеності хмарних технологій за допомогою OSINT-інструментів. Сучасний захист інформації, 2(62), 114–123.
https://doi.org/10.31673/2409-7292.2025.026087

Цілі дослідження:

1. Сформувати перелік OSINT-інструментів, за допомогою яких можливо досліджувати вразливості хмарних технологій;

2. Запропонувати модель дослідження стану кібербзпеки хмарних сховищ за допомогою OSINT-інструментів та оцінити її ефективність.

**Результати досліджень**

OSINT (Open Source Intelligence) є систематичним процесом збору та аналізу загальнодоступної інформації для отримання розвідувальних даних. У сфері кібербезпеки OSINT відіграє важливу роль у виявленні потенційних загроз, оцінці вразливостей та дослідженні інцидентів безпеки. На відміну від традиційних методів розвідки, OSINT використовує легально доступні джерела інформації, такі як веб-сайти, соціальні мережі, публічні бази даних, новини, академічні публікації та урядові звіти.

Застосування OSINT у дослідженні безпеки хмарних сховищ має ряд переваг:

- широкий спектр джерел: OSINT дозволяє отримувати інформацію з різноманітних відкритих джерел, що дає змогу сформувати комплексне уявлення про стан захищеності об'єкта дослідження;
- оперативність: інформація з відкритих джерел часто є актуальною та відображає поточний стан справ, що дозволяє оперативно виявляти нові загрози та вразливості;
- економічність: використання OSINT не потребує значних фінансових витрат на придбання спеціалізованого обладнання або закритих джерел інформації;
- прозорість та верифікованість: інформація, отримана з відкритих джерел, може бути перевірена та зіставлена з даними з інших джерел, що підвищує її надійність;
- можливість моделювання дій зловмисників: дослідники можуть використовувати OSINT для збору інформації, яку потенційно можуть отримати зловмисники, що дозволяє виявити слабкі місця в системі захисту з точки зору нападника.

OSINT може бути використаний для дослідження різних аспектів безпеки хмарних сховищ, включаючи виявлення неправильних конфігурацій, пошук витоків конфіденційної інформації, аналіз цифрового сліду організації, ідентифікацію потенційних цілей для соціальної інженерії та моніторинг згадок про вразливості.

**Методологія OSINT-дослідження стану захищеності хмарних сховищ**

Процес OSINT-дослідження стану захищеності хмарних сховищ може бути структурований у кілька етапів:

1. Визначення цілей та обсягу дослідження: на цьому етапі необхідно чітко визначити, які саме аспекти безпеки хмарного сховища підлягають дослідженню. Це може включати оцінку загального рівня захищеності, виявлення конкретних вразливостей (наприклад, неправильних конфігурацій бакетів S3), пошук витоків даних або аналіз цифрового сліду організації в контексті використання хмарних технологій.

Також визначається обсяг дослідження, тобто конкретні хмарні сервіси або організації, що підлягають аналізу.

2. Вибір та підготовка OSINT-інструментів: залежно від визначених цілей дослідження, необхідно обрати відповідні OSINT-інструменти. Існує велика кількість як безкоштовних, так і комерційних інструментів, що можуть бути використані для збору та аналізу загальнодоступної інформації. Важливим етапом є підготовка дослідницького середовища, яке має забезпечувати анонімність та безпеку дослідника.

3. Збір інформації: на цьому етапі здійснюється збір загальнодоступної інформації з використанням обраних інструментів та технік. Джерела інформації можуть включати пошукові системи (з використанням розширених операторів), соціальні мережі, публічні бази даних, форуми, блоги, сайти з інформацією про вразливості, архіви веб-сайтів, дані про реєстрацію доменів та IP-адрес, сервіси моніторингу витоків даних тощо. Збір інформації може здійснюватися як в пасивному режимі (без прямої взаємодії з об'єктом дослідження), так

© Івкова В.С., Банах Р.І. (2025). Методологія дослідження стану захищеності хмарних технологій за допомогою OSINT-інструментів. Сучасний захист інформації, 2(62), 114–123.
https://doi.org/10.31673/2409-7292.2025.026087

і в напівактивному або активному режимах (з обмеженою взаємодією, наприклад, при використанні публічних API).

Таблиця 1

Зв'язок між загрозами хмарних сховищ та OSINT-техніками

| **Загроза** | **Можливі OSINT-техніки виявлення** |
|---|---|
| Неправильні конфігурації | Google Dorks, Shodan, Censys, ZoomEye, OpenBuckets, GrayhatWarfare, AWS Eye, AAD Internals, Cloud Security Test (ImmuniWeb) |
| Небезпечні інтерфейси та API | Аналіз документації, пошук відкритих API через Google Dorks, Shodan, Censys, ZoomEye |
| Компрометація облікових записів | Have I Been Pwned, Dehashed, моніторинг витоків у DarkNet, XposedOrNot |
| Витоки даних | Google Dorks, спеціалізовані пошуковики (наприклад, Intelligence X), моніторинг соціальних мереж та Pastebin, Cyble ODIN |
| Інфраструктурні вразливості | Shodan, Censys, ZoomEye, аналіз DNS, OWASP Amass, сканери вразливостей (наприклад, Trivy, Nessus) |

Таблиця 2.1

Приклади OSINT-інструментів для дослідження безпеки хмарних сховищ

| **Інструмент** | **Категорія** | **Опис** | **Призначення для дослідження хмарних сховищ** |
|---|---|---|---|
| Google Dorks | Пошукова система | Розширені оператори пошуку Google | Пошук відкритих бакетів, конфігураційних файлів, витоків даних |
| Shodan | Пошукова система для IoT | Пошук інтернет-підключених пристроїв та сервісів | Виявлення публічно доступних хмарних ресурсів та їхніх конфігурацій |
| Censys | Пошукова система для інтернет-пристроїв | Аналіз інфраструктури та сертифікатів | Виявлення хмарних сервісів з проблемами безпеки |
| ZoomEye | Пошукова система для інтернет-пристроїв | Пошук інтернет-підключених пристроїв | Аналіз хмарних сервісів та виявлення потенційних вразливостей |
| Whois | Інструмент для аналізу доменів | Отримання інформації про власників доменів | Ідентифікація доменів, пов'язаних з хмарними сервісами |
| Have I Been Pwned | Моніторинг витоків даних | Перевірка наявності облікових даних у витоках | Виявлення скомпрометованих облікових записів, пов'язаних з хмарою |
| OpenBuckets | Спеціалізована пошукова система | Пошук відкритих бакетів AWS S3, Azure Blob тощо | Пряме виявлення незахищених хмарних сховищ |

© Івкова В.С., Банах Р.І. (2025). Методологія дослідження стану захищеності хмарних технологій за допомогою OSINT-інструментів. Сучасний захист інформації, 2(62), 114–123.
https://doi.org/10.31673/2409-7292.2025.026087

| | | | |
|---|---|---|---|
| GrayhatWarfare | Спеціалізована пошукова система | Сканування інтернету на предмет відкритих бакетів AWS та Azure | Пошук загальнодоступних хмарних сховищ |
| theHarvester | Інструмент командного рядка | Збір інформації про домени, субдомени, email-адреси | Пошук зовнішніх слідів хмарної інфраструктури |
| CloudEnum | Інструмент для хмарних середовищ | Перелік ресурсів у різних хмарних провайдерів | Виявлення потенційно вразливих хмарних ресурсів |
| AWS Eye | Інструмент для AWS | Дослідження конфігурацій AWS | Ідентифікація неправильно налаштованих ресурсів AWS, включаючи бакети S3 |
| FullHunt | Пошукова система | Пошук вразливостей | Виявлення хмарних активів, що можуть бути вразливими |
| Cloud Security Test (ImmuniWeb) | Онлайн сервіс | Виявлення незахищених хмарних сховищ | Швидка перевірка наявності загальнодоступних хмарних сховищ |
| CloudMapper | Інструмент для AWS | Аналіз середовищ AWS | Візуалізація мережевих діаграм та аудит безпеки AWS |
| CloudSploit | Інструмент для хмарних середовищ | Виявлення вразливостей у хмарних інфраструктурах | Підтримка AWS, Azure, GCP, Oracle, GitHub |
| Trivy | Сканер безпеки | Сканування на вразливості, неправильні конфігурації, секрети | Підтримка контейнерів, файлових систем, Git, образів VM, Kubernetes, AWS |
| GitGuardian | Платформа безпеки | Виявлення секретів у публічних та приватних кодових базах | Моніторинг в реальному часі, підтримка багатьох типів секретів |
| HawkScan | Інструмент безпеки | Сканування образів контейнерів, виявлення секретів | Комплексна безпека контейнерів |
| TruffleHog | Інструмент командного рядка | Глибоке сканування репозиторіїв на наявність секретів | Підтримка регулярних виразів та виявлення на основі ентропії |
| Spectral Secret Scanning | Платформа безпеки | Сканування в реальному часі для виявлення секретів | Виявлення понад 750 типів секретів та хмарних облікових даних |
| AWS Secrets Manager | Сервіс AWS | Зберігання та отримання конфіденційної інформації | Перевірка, чи закодовані облікові дані в додатках |
| Legit Security | Платформа безпеки | Сканування секретів на основі ШІ | Виявлення, запобігання та усунення розкритих секретів |
| OSINTCombine | Набір скриптів | Автоматизація різних аспектів OSINT | Спрощення процесу збору розвідувальних даних |
| Cyble ODIN | Пошукова система | Сканування та каталогізація інтернет-активів | Виявлення розкритих бакетів та сканування IP-адрес |

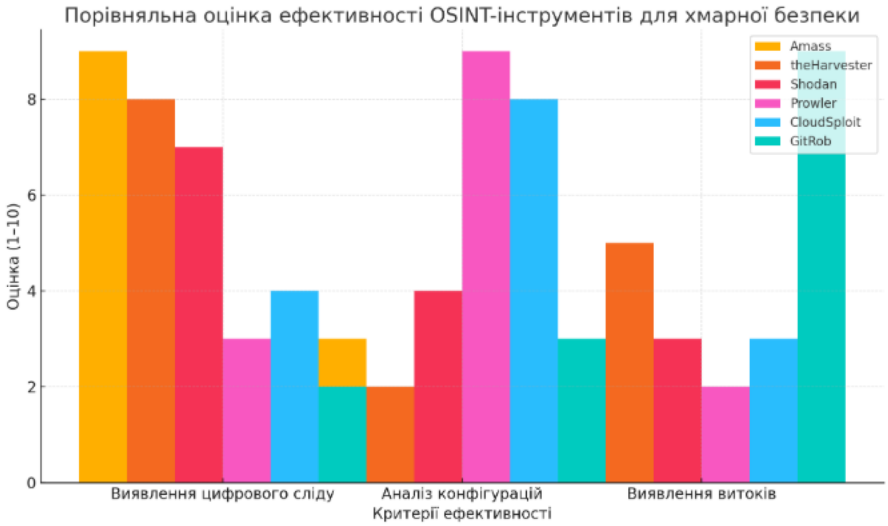


Рис.1, Порівняльна оцінка ефективності OSINT-інструментів

На діаграмі показано порівняльну оцінку ефективності OSINT-інструментів за трьома критеріями: виявлення цифрового сліду, аналіз конфігурацій хмарних середовищ та виявлення витоків. Це допомагає вибрати найдоцільніші інструменти для конкретного типу дослідження.

4. Обробка та аналіз інформації: Зібрана інформація часто є неструктурованою та потребує обробки, фільтрації та аналізу для виявлення релевантних даних. На цьому етапі можуть бути використані методи семантичного аналізу, виявлення закономірностей, кореляції даних з різних джерел, візуалізації інформації та інші аналітичні техніки. Важливою є перевірка достовірності отриманої інформації шляхом її зіставлення з даними з кількох незалежних джерел.

5. Ідентифікація вразливостей та ризиків: На основі проведеного аналізу ідентифікуються потенційні вразливості та ризики для безпеки хмарного сховища. Це може включати виявлення неправильних конфігурацій, незахищених API, витоків облікових даних, згадок про вразливості в програмному забезпеченні, що використовується, та іншу інформацію, яка може бути використана зловмисниками.

6. Звітність та документування результатів: Результати OSINT-дослідження оформлюються у вигляді звіту, який містить опис проведеної роботи, виявлені вразливості та ризики, а також рекомендації щодо їх усунення. Важливим є детальне документування всіх етапів дослідження, використаних інструментів та отриманих даних.

7. Етичні та юридичні аспекти: При проведенні OSINT-дослідження необхідно дотримуватися етичних норм та вимог законодавства про захист персональних даних.

Збір інформації повинен здійснюватися лише з публічно доступних джерел без використання незаконних методів (наприклад, взлому). Важливою є прозорість та відповідальне використання отриманих даних.

**Оцінка ефективності запропонованої моделі**

Ефективність запропонованої методології може бути оцінена за кількома критеріями:

- кількість виявлених вразливостей: чим більше потенційних вразливостей буде виявлено за допомогою OSINT-інструментів, тим вищою буде ефективність моделі;
- типи виявлених вразливостей: модель ефективна, якщо вона дозволяє виявляти як базові вразливості (наприклад, відкриті S3 бакети), так і більш складні (наприклад, скомпрометовані облікові дані через витік з інших сервісів);
- час, затрачений на дослідження: OSINT-підхід дозволяє значно скоротити час, необхідний для початкової оцінки захищеності, порівняно з традиційними методами;

• вартість дослідження: застосування переважно безкоштовних або недорогих OSINT-інструментів робить методологію економічно ефективною;

• проактивність: модель дозволяє виявляти потенційні загрози ще до того, як вони будуть використані зловмисниками, що є ключовим аспектом проактивної кібербезпеки;

• зниження ризиків: успішне застосування методології та усунення виявлених вразливостей безпосередньо призводить до зниження загального рівня ризиків для хмарних сховищ.

Для кількісної оцінки ефективності можна використовувати такі метрики:

• $Nv$: кількість виявлених вразливостей;

• $Td$: середній час, затрачений на виявлення вразливості (у годинах);

• $Ce$ орієнтовна економічна вигода від запобігання потенційному інциденту (розраховується на основі середньої вартості витоку даних);

Таким чином, ефективність (E) може бути представлена як функція від кількості виявлених вразливостей та часу, що витрачається, з урахуванням економічної вигоди:

$$\mathrm{E} = f(Nv, Td^{-1}, Ce),$$

де $Nv$,є прямо пропорційним, $Td$ є обернено пропорційним, а $Ce$ також прямо пропорційним показникам ефективності.

**Опробація моделі:**

Наведемо приклад використання запропонованої моделі для дослідження безпеки хмарного сховища вигаданої компанії "TechSolutions" та оцінку її ефективності.

Приклад використання моделі дослідження безпеки хмарних сховищ.

Об'єкт дослідження: Хмарні сховища компанії "TechSolutions" (основний домен techsolutions.com). Компанія використовує AWS для зберігання клієнтських даних.

Мета дослідження: Виявити потенційні вразливості, що можуть призвести до витоку даних з хмарних сховищ "TechSolutions", використовуючи OSINT-інструменти.

Етап 1: Визначення цілей та обсягу дослідження.

• Цілі: Виявити неправильно налаштовані S3-бакети, витік облікових даних, публічно доступні файли конфігурації, інформацію про інфраструктуру, яка може бути використана для атаки.

• Обсяг: Дослідження публічно доступної інформації, що стосується домену techsolutions.com та її хмарних ресурсів AWS.

Етап 2: Збір вихідних даних.

• Базова інформація: techsolutions.com, імена відомих співробітників (отримано з LinkedIn), використання AWS.

• Пошук публічної інформації: Через LinkedIn виявлено, що у "TechSolutions" є відділ розробки, який активно використовує GitHub.

Етап 3: Вибір та підготовка OSINT-інструментів.

• Вибір інструментів:

- Google Dorks: Для пошуку загальнодоступних файлів та конфігурацій.
- Shodan / Censys: Для виявлення відкритих портів та сервісів, пов'язаних з techsolutions.com.
- OpenBuckets / GrayhatWarfare: Для пошуку відкритих S3-бакетів.
- Have I Been Pwned (HIBP): Для перевірки витоків облікових даних.
- GitHub / GitLab Search: Для пошуку секретів у репозиторіях.
- TruffleHog: Для глибокого сканування Git-репозиторіїв на наявність секретів.

Етап 4: Збір інформації.

• Google Dorks: Використання запитів типу site:techsolutions.com filetype:log, site:techsolutions.com intitle:"index of" aws, site:techsolutions.com "S3 bucket".

- Результат: Виявлено кілька публічно доступних файлів .log на субдомені, що містять деякі технічні деталі про внутрішні сервіси, але без прямого доступу до конфіденційної інформації. Також знайдено посилання на тестовий S3-бакет, що містить пусті файли.

• Shodan/Censys: Пошук IP-адрес, пов'язаних з techsolutions.com, у хмарі AWS.

- Результат: Виявлено кілька серверів AWS, що належать "TechSolutions", з відкритим портом 22 (SSH) та 3389 (RDP), але без видимих вразливостей або можливості несанкціонованого доступу. Один з серверів, що використовується для тестових розробок, має неактивний веб-сервер.

• OpenBuckets/GrayhatWarfare: Сканування на наявність відкритих S3-бакетів, пов'язаних з techsolutions.com.

- Результат: Виявлено один AWS S3-бакет (наприклад, techsolutions-test-data), який був публічно доступний і містив невелику кількість тестових файлів, які могли б бути чутливими, якби це були реальні дані. Це є вразливістю (Неправильна конфігурація).

• Have I Been Pwned (HIBP): Перевірка корпоративних email-адрес techsolutions.com на наявність у витоках даних.

- Результат: Виявлено, що 5 корпоративних email-адрес співробітників були скомпрометовані у старих витоках даних з сторонніх сервісів. Ці витоки включали хешовані паролі. Це потенційна вразливість (Компрометація облікових записів).

• GitHub/GitLab Search & TruffleHog: Пошук за ключовими словами, пов'язаними з "TechSolutions" та AWS credentials, у публічних репозиторіях GitHub/GitLab.

- Результат: Виявлено публічний репозиторій одного з розробників, що містив випадково завантажений файл aws_config.ini з жорстко закодованими AWS API-ключами (Access Key ID та Secret Access Key) для тестового середовища. Це є вразливістю (Витоки даних / Неправильні конфігурації).

Етап 5: Обробка та аналіз інформації.

• Систематизація: Зібрані дані були категоризовані за типами вразливостей: неправильні конфігурації, скомпрометовані облікові записи, витоки даних.

• Аналіз:

- Публічний S3-бакет: Хоча містив тестові дані, сам факт публічного доступу до бакету є серйозною проблемою, яка вказує на відсутність належного контролю конфігурації.
- Скомпрометовані email-адреси: Навіть хешовані паролі можуть бути розкриті, що потенційно дозволяє зловмисникам здійснити спроби авторизації за допомогою цих даних.
- API-ключі в GitHub: Це критична вразливість, оскільки ці ключі, навіть для тестового середовища, можуть бути використані для доступу до хмарних ресурсів, зміни конфігурацій або навіть отримання доступу до інших, більш захищених частин інфраструктури, якщо політики IAM налаштовані некоректно.

Етап 6: Ідентифікація вразливостей та ризиків.

• Виявлені вразливості (Nv =3):

1. Публічно доступний AWS S3-бакет (techsolutions-test-data).
2. П'ять скомпрометованих корпоративних email-адрес співробітників.
3. AWS API-ключі для тестового середовища, витіклі в публічному репозиторії GitHub.

• Карта атаки: Зловмисник міг би використовувати витіклі API-ключі для доступу до тестового середовища AWS, а потім спробувати підвищити привілеї або використати інші вразливості, щоб отримати доступ до виробничих систем. Скомпрометовані облікові дані можуть бути використані для атак соціальної інженерії або спроб злому облікових записів. Публічний S3-бакет може бути використаний для витоку даних або ін'єкції шкідливих файлів.

• Оцінка ризиків:

- API-ключі в GitHub: Високий ризик. Можливість несанкціонованого доступу та впливу на хмарну інфраструктуру.

o Публічний S3-бакет: Середній-високий ризик. Потенційний витік даних, репутаційні втрати.

o Скомпрометовані email-адреси: Середній ризик. Загроза фішингу та соціальної інженерії.

Етап 7: Формування рекомендацій та звітів.

• Рекомендації:

o Негайно змінити AWS API-ключі та відкликати скомпрометовані. Впровадити автоматичний моніторинг репозиторіїв на наявність секретів (наприклад, за допомогою GitGuardian ).

o Налаштувати правильні політики доступу для всіх S3-бакетів, забезпечивши, що вони не є публічно доступними, якщо це не потрібно. Регулярно перевіряти конфігурації бакетів за допомогою інструментів (наприклад, CloudMapper ).

o Примусово вимагати зміну паролів для скомпрометованих облікових записів та впровадити багатофакторну автентифікацію (MFA) для всіх користувачів, особливо для привілейованих.

o Провести навчання співробітників з питань безпеки, зокрема щодо безпечної роботи з кодом та конфіденційною інформацією.

• Звіт: Підготовлено детальний звіт для керівництва та IT-відділу "TechSolutions" з описом виявлених вразливостей, їхнім впливом та рекомендаціями щодо усунення.

**Оцінка ефективності запропонованої моделі**

Використаємо формулу:

$$\mathrm{E} = f(Nv, Td^{-1}, Ce),$$

• $Nv$: (кількість виявлених вразливостей): у цьому прикладі виявлено 3 значні вразливості. Це свідчить про високу ефективність моделі у виявленні конкретних проблем безпеки;

• $Td$ (середній час, затрачений на виявлення вразливості): припустимо, що на проведення повного OSINT-дослідження (збір даних, аналіз) для "TechSolutions" знадобилося близько 16 годин (2 робочих дні). Це значно менше, ніж проведення повноцінного тестування на проникнення або аудиту безпеки, що займає тижні. Таким чином, $Td$ є відносно низьким, що підвищує ефективність ($Td^{-1}$є високим);

• $Ce$ (орієнтовна економічна вигода від запобігання потенційному інциденту): за даними різних звітів, середня вартість витоку даних може становити мільйони доларів (наприклад, за даними IBM у 2023 році, середня вартість витоку даних становила $4.45 млн). Запобігання витоку даних через виток API-ключі або публічний S3-бакет може уникнути цих значних фінансових втрат, а також репутаційних збитків, штрафів та судових витрат. Отже $Ce$ є дуже високим.

Висновок щодо ефективності:

1. Запропонована модель виявилася дуже ефективною в даному прикладі. Вона дозволила проактивно виявити критичні вразливості (Nv = 3) за відносно короткий час (Td = 16 годин), що дозволило уникнути потенційно значних економічних збитків (Ce - мільйони доларів);

2. Модель також підтвердила свою здатність виявляти різнотипні вразливості – від неправильних конфігурацій хмарних ресурсів до витоків конфіденційної інформації у публічних репозиторіях.

Таким чином, використання методології OSINT, як показано в цій моделі, є потужним, економічно ефективним та проактивним підходом до підвищення безпеки хмарних сховищ.

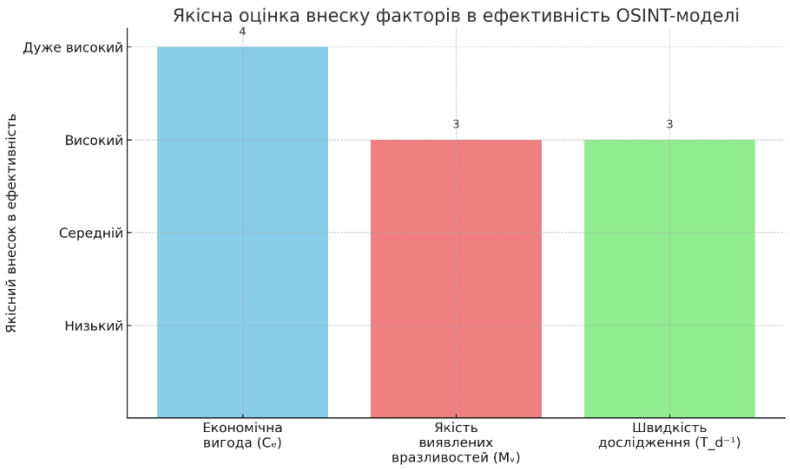


Рис.2 Якісна оцінка ефективності запропонованої моделі

**Висновки**

Запропонована методологія дослідження стану захищеності хмарних сховищ за допомогою OSINT-інструментів є більш глибоким, систематизованим та всебічним підходом до оцінки ризиків безпеки у хмарних середовищах. Її застосування дозволяє отримати цінну інформацію про потенційні вразливості, складні слабкі місця та приховані загрози без активної взаємодії з інфраструктурою, що робить її етичним та безпечним методом оцінки. Врахування специфіки різних моделей хмарних сервісів та детальне дослідження різноманітних відкритих джерел інформації дозволяє виявити не лише поверхневі, але й більш глибокі та складні вразливості, які можуть бути пропущені при використанні традиційних методів аудиту безпеки. Детальна оцінка ризиків та розробка багаторівневих рекомендацій щодо підвищення рівня безпеки забезпечують практичну цінність запропонованої методології для організацій, які використовують хмарні сховища. Важливо підкреслити необхідність дотримання етичних норм та законодавства при проведенні OSINT-досліджень. Збір та аналіз інформації повинні здійснюватися в рамках закону, без спроб несанкціонованого доступу до приватних даних.

**Перелік посилань**

1. Таксін О. П., Корнійчук О. М. Безпека хмарних обчислень: актуальні загрози та методи захисту // Інформаційні технології та комп'ютерна інженерія. 2020. № 1. С. 55-62.

2. Subashini S., Kavitha V. A survey on security issues in cloud computing // Journal of Network and Computer Applications. 2011. Vol. 34, No. 1. P. 1-11., Режим доступу: https://doi.org/10.1016/j.jnca.2010.07.006

3. Ничик В. М., Романов В. В., Терещенко Т. О. Розвідка на основі відкритих джерел: концептуальні засади та інструментарій // Інформаційна безпека. 2019. № 1. С. 15-22.

4. Bremmer J. N. Open source intelligence techniques: Resources for searching and analyzing online information. Lulu.com, 2010.

5. Shutenko V., Teres K. Must-Know Cloud Security Statistics for 2025 Режим доступу: https://www.techmagic.co/blog/cloud-security-statistics

6. Zissis D., Lekkas D. Addressing cloud computing security issues // Future Generation Computer Systems. 2012. Vol. 28, No. 3. P. 583-592, Режим доступу: https://doi.org/10.1016/j.future.2010.12.006

7. Ранич В. М., Ковальчук С. В. Аналіз вразливостей хмарних сервісів зберігання даних // Захист інформації. 2018. № 2. С. 45-51.

8. Lande D., Shnurko-Tabakova E. OSINT as a part of cyber defense system. Theoretical and Applied Cybersecurity. 2019. Vol. 1, no. 1. URL: https://doi.org/10.20535/tacs.2664-29132019.1.169091

9. CloudSafe: A Tool for an Automated Security Analysis for Cloud Computing / S. An et al. 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019. 2019. URL: https://doi.org/10.1109/trustcom/bigdatase.2019.00086

10. Cloud Property Graph: Connecting Cloud Security Assessments with Static Code Analysis / C. Banse et al. 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Chicago, IL, USA, 5–10 September 2021. 2021. URL: https://doi.org/10.1109/cloud53861.2021.00014

11. Mukhopadhyay A., Luther K. OSINT Clinic: Co-designing AI-Augmented Collaborative OSINT Investigations for Vulnerability Assessment. CHI 2025: CHI Conference on Human Factors in Computing Systems, Yokohama Japan. New York, NY, USA, 2025. P. 1–22. URL: https://doi.org/10.1145/3706598.3713283

Надійшла 15.05.2025