DOI https://doi.org/10.32689/maup.it.2026.1.6
УДК 004.056.5

ENTERPRISE OSINT ДЛЯ УПРАВЛІННЯ РИЗИКАМИ, МОНІТОРИНГ ЦИФРОВОГО СЛІДУ КОМПАНІЇ ТА СПІВРОБІТНИКІВ

В. М. Слатвінська, В. І. Бевза

ENTERPRISE OSINT FOR RISK MANAGEMENT, MONITORING THE DIGITAL FOOTPRINT OF THE COMPANY AND EMPLOYEES

Valeria Slatvinska, Vyacheslav Bevza

Анотація

Об'єктом дослідження є процеси виявлення, інтерпретації та використання даних з відкритих джерел для управління кіберризиками підприємства в умовах розширення цифрового периметра. Проблема полягає в тому, що традиційні механізми внутрішнього моніторингу не забезпечують раннього виявлення витоків, компрометації облікових записів, тіньових цифрових активів і поведінкових сигналів, пов'язаних із цифровим слідом співробітників. У роботі удосконалено підхід до побудови Enterprise OSINT як безперервного циклу збору, нормалізації, верифікації та кореляції зовнішніх індикаторів із внутрішніми подіями безпеки. Результатом є структурна модель архітектури Enterprise OSINT, векторів загроз і методів їх детектування, а також процедура інтеграції даних OSINT у контур ISO/IEC 27001, SIEM та CTI. Запропоновані результати дозволяють вирішити проблему фрагментарності зовнішнього моніторингу завдяки поєднанню технічних, організаційних та аналітичних компонентів в єдиному контурі ризик-менеджменту. Їх відмінність полягає у фокусі не лише на інфраструктурі компанії, а й на цифровому сліді працівників, партнерських згадках, витоках у Surface, Deep і Dark Web та подальшій перевірці сигналів на хибнопозитивні спрацювання. Отримані результати пояснюються тим, що зовнішні дані розглядаються не як довідкова інформація, а як операційні індикатори ризику, придатні для автоматизованої валідації та пріоритезації. Практичне використання можливе в корпоративних системах інформаційної безпеки, SOC, службах економічної безпеки та підрозділах комплаєнсу за умови наявності політик етичного моніторингу, регламентів реагування, навчання персоналу та процедури повторної перевірки джерел. Додатково підхід орієнтований на зниження репутаційних і фінансових втрат через своєчасне виявлення зовнішніх індикаторів підготовки цільових атак.

Ключові слова: *OSINT, enterprise OSINT, кіберрозвідка, цифровий слід, корпоративна безпека, управління ризиками, SIEM, CTI.*

Abstract

The object of the study is the process of identifying, interpreting and using open-source data for enterprise cyber risk management under the conditions of an expanding digital perimeter. The problem is that traditional internal monitoring mechanisms do not provide early detection of leaks, compromised accounts, shadow digital assets and behavioral signals connected with the digital footprint of employees. The paper improves the approach to Enterprise OSINT as a continuous cycle of collection, normalization, verification and correlation of external indicators with internal security events. The results include a structural architecture model of Enterprise OSINT, a matrix of threat vectors and detection methods, and a procedure for integrating OSINT data into the ISO/IEC 27001, SIEM and CTI control loop. The proposed results solve the problem of fragmented external monitoring through the combination of technical, organizational and analytical components within a single risk management contour. Their distinctive feature is the focus not only on the company infrastructure, but also on employees digital footprints, partner mentions, leaks in the Surface, Deep and Dark Web, and subsequent false-positive verification. The results are explained by the fact that external data are treated not as background information, but as operational risk indicators suitable for automated validation and prioritization. Practical use is possible in corporate information security systems, SOCs, economic security services and compliance units provided that ethical monitoring policies, response procedures and repeated source verification are in place.

Key words: *OSINT, enterprise OSINT, cyber intelligence, digital footprint, corporate security, risk management, SIEM, CTI.*

1. Вступ. Цифровізація бізнес-процесів прискорилася. Хмарні сервіси поширюються. Віддалена робота та аутсорсингові моделі розширили межі корпоративного цифрового периметра. Підприємство втрачає можливість обмежуватися внутрішнім журналюванням подій. Значна частина сигналів ризику формується поза локальною інфраструктурою. Соціальні мережі генерують сигнали. Реєстри доменів фіксують зміни. Системи прозорості сертифікатів публікують дані. Витоки облікових даних виявляються у маркетплейсах. Тематичні спільноти обговорюють загрози. Наукові дослідження Enterprise OSINT потрібні сучасній практиці. Зовнішні ознаки атак виявляються раніше. Часові лаги реагування зменшуються. Обґрунтованість рішень у системі управління кіберризиками підвищується.

Результати таких досліджень можуть дати практиці щонайменше три ефекти: по-перше, переведення зовнішнього моніторингу з епізодичного рівня на рівень безперервного процесу; по-друге,

інтеграцію розвідувальних сигналів у вже наявні контури СУІБ та SOC; по-третє, формування процедур належного контролю цифрового сліду, без порушення принципів пропорційності та верифікованості. Тому дослідження, присвячені Enterprise OSINT як інструменту управління ризиками та моніторингу цифрового сліду компанії й співробітників, є актуальними.

Аналіз літератури свідчить, що використання OSINT у кібербезпеці поступово переходить від опису окремих інструментів до розроблення методологій їх інтеграції в управлінські процеси. У роботі [1] автори трактують OSINT як інструмент раннього попередження шахрайства; автори праці [2] пов'язують його з процедурами оцінки ризиків у межах ISO/IEC 27001; автори праці [3] систематизують функціональні класи OSINT-рішень у кібербезпеці. У роботі [4] автори акцентують на репутаційних ризиках приватної активності співробітників у соціальних мережах, а автори праці [5] розглядають CTI як основу для динамічного ризик-менеджменту.

Подальший розвиток теми демонструється у роботі [6], які пов'язують кіберрозвідку із захистом критичної інфраструктури; у праці [7] аналізують використання та обмін CTI, сформованої на основі OSINT; авторами праці [8] розглянуто відкриті джерела як інструмент контррозвідки; автори праці [9] показують двоїстий ефект OSINT-інструментів для виявлення вразливостей; у роботі [10] автори підкреслюють необхідність автоматизації та процесної дисципліни.

У праці [11] йде опис масштабованої інфраструктури збирання та оброблення OSINT-даних. Корпоративний рівень розвідки неможливий без автоматизації колекторів. Нормалізація даних потрібна обов'язково. Централізоване сховище забезпечує доступ до інформації. У роботі [12] автори доводять, що цінність OSINT суттєво зростає тоді, коли зовнішні сигнали вбудовуються у контрольні процедури ISO/IEC 27001, а не використовуються ізольовано. Автори праці [13] наголошують, що цифровий слід працівників створює не лише репутаційні, а й операційні ризики: spear-phishing, витік know-how, цільове профілювання та маніпуляцію професійними рішеннями. У праці [14] автори показують конфлікт між прозорістю, безпекою, ефективністю та відсутністю упередженості під час автоматизації OSINT. У роботі [15] автори пов'язують зрілість корпоративної кіберрозвідки з готовністю організацій обмінюватися перевіреними індикаторами через стандартизовані механізми CTI-sharing.

Проаналізовані джерела не розв'язують загальну проблему поєднання трьох контурів у межах однієї моделі. Моніторинг інфраструктурних експозицій підприємства виконується окремо. Контроль цифрового сліду працівників здійснюється незалежно. Керована інтеграція зовнішніх сигналів у внутрішні процеси оцінки та перегляду ризиків відсутня. Проблема лишається невирішеною з об'єктивних причин. Дані є різнорідними. Частка шуму висока. Етичні обмеження щодо моніторингу працівників існують. Єдиний узгоджений підхід до верифікації зовнішніх індикаторів відсутній. Ця невирішена частина проблеми визначає логіку мети дослідження.

Метою дослідження є удосконалення концептуальної моделі Enterprise OSINT для системного управління кібер ризиками. Моніторинг цифрового сліду компанії й співробітників виконується через неї. Своєчасність виявлення зовнішніх ознак загроз підвищується. Вплив хибнопозитивних сигналів знижується. Практична інтеграція OSINT-даних у контур інформаційної безпеки підприємства забезпечується.

Для досягнення мети були поставлені наступні задачі:

– систематизувати джерела й індикатори Enterprise OSINT, релевантні для моніторингу цифрового сліду компанії та працівників;

– розробити структурну модель інтеграції OSINT-компонентів у контур управління ризиками та класифікувати ключові вектори загроз;

– визначити процедуру верифікації зовнішніх сигналів, умови практичного застосування, обмеження та напрями подальшого розвитку Enterprise OSINT.

2. Матеріали і методи. Об'єктом дослідження є процес управління зовнішньою кібер-експозицією підприємства. Інфраструктурні дані формують її. Дані про брендову присутність доповнюють картину. Цифровий слід співробітників у відкритих джерелах аналізується. Основна гіпотеза дослідження полягає у наступному. Enterprise OSINT включається у процедури ризик-менеджменту. Процедури побудовані за логікою ISO/IEC 27001. SIEM/CTI-кореляція доповнює їх. Значущі ризики виявляються раніше порівняно з моделлю, де аналізуються лише внутрішні події безпеки.

У роботі прийнято такі припущення: 1) компанія має формалізований перелік активів, доменів, облікових записів та брендових ідентифікаторів; 2) моніторинг цифрового сліду співробітників здійснюється лише щодо публічно доступних даних і в межах внутрішніх політик; 3) зовнішні сигнали не вважаються підтвердженим інцидентом до їх повторної верифікації; 4) інтеграція з SIEM і CTI є організаційно можливою.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Спрощення дослідження полягають у тому, що не розглядаються спеціальні розвідувальні дії, пов'язані з доступом до непублічних даних, не моделюються юридичні особливості окремих юрисдикцій, а кількісна оцінка ефективності пропонується у вигляді якісно-порівняльної інтерпретації. Такий підхід відповідає концептуально-методологічному характеру роботи.

Аналіз наукової періодики 2021–2026 років використано для отримання результатів. Порівняльний аналіз архітектур Enterprise OSINT виконано. Метод ризик-орієнтованого картування зовнішніх індикаторів на активи підприємства застосовано. Метод структурного синтезу побудував модель взаємодії між колекторами, верифікаційним модулем, SIEM, CTI та процесами прийняття рішень. Логіка сценарного аналізу описала типові вектори атак. Компрометація облікових даних розглянута. Shadow IT проаналізовано. Описано фішинг. Підміна бренду досліджена. Профілювання працівників вивчено.

Методологічно робота спирається на поєднання технічного та управлінського підходів. З технічного боку Enterprise OSINT розглядається як безперервний цикл збору та збагачення даних із публічних джерел; з управлінського боку – як елемент процесів оцінки ризиків, повторного перегляду контролів, інформування відповідальних осіб та коригування політик. Така постановка дозволила отримати результати без змішування їх із описом процедури дослідження.

3. Результати і обговорення

3.1. Структурна модель Enterprise OSINT в контурі управління ризиками. Впровадження Enterprise OSINT вимагає переходу від епізодичного пошуку інформації до побудови безперервного циклу розвідки. Як зазначають автори у праці [1], ефективність системи залежить від здатності агрегувати дані з гетерогенних джерел: публічних реєстрів, соціальних мереж, технічних баз даних (DNS, Whois, Shodan) та спеціалізованих форумів у Dark Web. На відміну від класичного тестування на проникнення (Penetration Testing), яке є активною дією, OSINT дозволяє оцінити поверхню атаки пасивно, не залишаючи слідів у журналах цільових систем, що підтверджується дослідженнями авторами праці [2].

Одним із ключових аспектів є інтеграція OSINT із процесами ризик-менеджменту. У роботі [3] автори наголошують, що результати OSINT мають напряму впливати на перерахунок метрик ризику в межах системи управління інформаційною безпекою (СУІБ). Наприклад, виявлення облікових даних співробітників у базах витоків (Combolists) автоматично підвищує ризик несанкціонованого доступу та запускає процедуру примусової зміни паролів. Такий підхід узгоджується з рекомендаціями авторами роботи [4], які пропонують динамічно адаптувати політики безпеки на основі зовнішніх сигналів.

Окремої уваги заслуговує моніторинг цифрового сліду співробітників. У праці [5] вказують, що приватні акаунти працівників часто перетворюються на зручний вхідний канал для атак. Фото з робочого місця, геотеги офісу та згадки про відрядження дають змогу зловмисникам зібрати контекст і скласти профіль жертви для spear-phishing. Авторами роботи [6] підкреслено необхідність застосовувати методи контррозвідки, щоб виявляти фейкові профілі у LinkedIn, які видають себе за HR-менеджерів або партнерів та збирають конфіденційні відомості у співробітників.

Технічна реалізація моніторингу інфраструктури передбачає постійне сканування публічних IP-адрес та доменів компанії. У роботі [7], продемонстровано, як інструменти на кшталт Shodan або Censys дозволяють виявити незахищені порти RDP, бази даних без аутентифікації або застарілі версії веб-серверів раніше, ніж це зроблять зловмисники. У праці [8] автори підтверджують, що своєчасне виявлення фішингових доменів (typosquatting) через моніторинг сертифікатів Transparency Logs (CT Logs) є ефективним методом превентивного захисту бренду.

Для пояснення взаємодії компонентів системи та логіки перетворення сирих даних на управлінські рішення на рисунку 1 зображено структурну модель функціонування Enterprise OSINT в контурі корпоративної безпеки.

Як показано на рисунку 1, залежності між модулями мають ієрархічну структуру, а критичним етапом є нормалізація та кореляція даних перед передачею в систему управління ризиками. Це дає змогу відсіяти «інформаційний шум» і зосередитися на релевантних загрозах.

Окремий компонент архітектури становить Threat Intelligence Sharing, тобто обмін даними про загрози. За роботою [9], автори описують використання платформ обміну на кшталт MISP дозволяє доповнювати внутрішні набори даних індикаторами, які надходять від інших учасників спільноти. У результаті зростає «колективний імунітет» галузі. Проте у роботі [10], автори підкреслюють, що автоматизація цього процесу має спиратися на жорстку верифікацію джерел, інакше зростає ризик data poisoning.

Відповідно до першої задачі, було систематизовано ключові групи джерел та індикаторів, релевантних для корпоративного OSINT-моніторингу. Для пояснення взаємодії компонентів системи в науковому контексті на рисунку 2 зображено структурну модель Enterprise OSINT, у якій відображено логіку переходу від розрізнених зовнішніх сигналів до управлінських рішень у межах СУІБ.

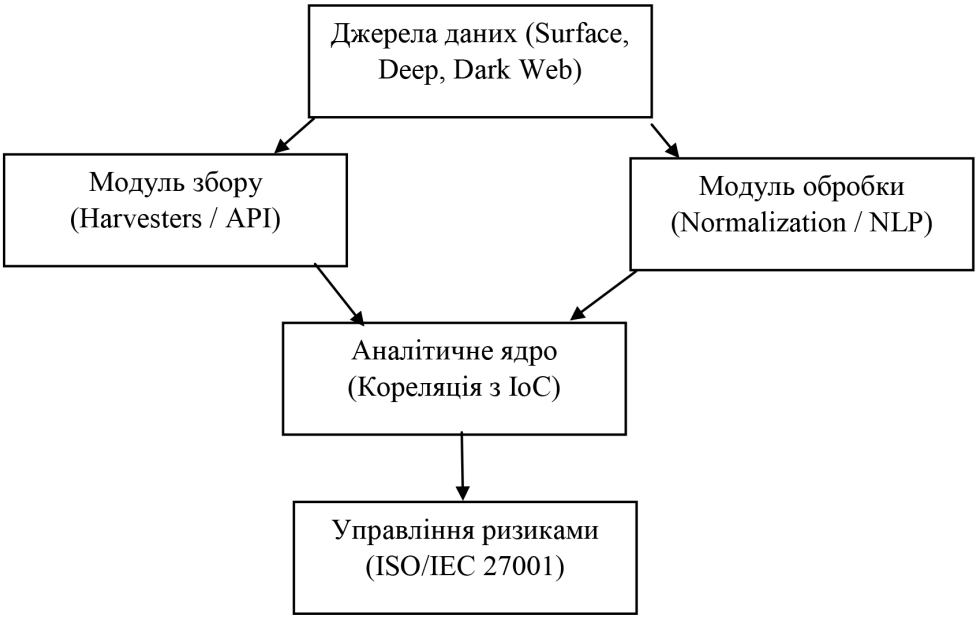

Рис. 1. Структурна модель компонентів системи Enterprise OSINT

Запропонована модель на рисунку 2 дає змогу поєднати технічні, поведінкові та організаційні індикатори в єдиному аналітичному контурі, що підвищує повноту виявлення зовнішніх ознак загроз. Її особливістю є орієнтація не лише на моніторинг цифрової експозиції інфраструктури підприємства, а й на аналіз цифрового сліду працівників як потенційного джерела ризику для корпоративної безпеки. У результаті Enterprise OSINT розглядається як інструмент проактивного виявлення загроз, здатний забезпечити своєчасне коригування заходів захисту та зниження ймовірності реалізації кібератак.

Як видно з рисунка 2, базовою умовою результативності Enterprise OSINT є наявність проміжного шару нормалізації, дедублікації та перевірки джерел. Саме цей шар зменшує інформаційний шум і відокремлює сигнали, що мають управлінську цінність, від масиву нерелевантних згадок. На відміну від підходу, де OSINT використовується лише як допоміжний інструмент розслідування постфактум, запропонована модель включає його в безперервний цикл оцінки ризиків і дозволяє оновлювати карту загроз до настання інциденту.

Отриманий результат пояснюється наступним. Зовнішні дані набувають значення після зв'язування з конкретними корпоративними активами. Облікові записи ідентифікуються. Брендові маркери фіксуються. У праці [11] автори зосереджуються на колекторній інфраструктурі переважно. Запропоноване рішення посилює управлінський контур. Сигнал після верифікації переходить у площину SIEM-кореляції автоматично. Перегляд ризику виконується наступним етапом. Положення роботи [12] підтверджується. Цінність OSINT проявляється через інтеграцію з процедурами ISO/IEC 27001.

Перевагою запропонованого рішення є поєднання інфраструктурного й поведінкового контурів моніторингу. Класичні моделі зосереджуються на зовнішній поверхні атаки доменів і хостів. Запропоноване рішення включає аналіз цифрового сліду працівників структурно. Працівники розглядаються як окреме джерело ризику. Проблемна частина закривається частково. Огляд літератури виявив її раніше. Фрагментарність між технічним і соціальним вимірами зовнішнього моніторингу усувається.

3.2. Класифікація векторів загроз та методів Enterprise OSINT. Для розв'язання другої задачі було побудовано 2 узагальнені таблиці відповідності між векторами загроз, OSINT-методами детектування, типовими індикаторами та управлінськими діями.

У таблиці 1 показано, як різні категорії зовнішніх сигналів можуть бути пов'язані з практичними рішеннями у сфері інформаційної безпеки.

У таблиці 2 продемонстровано як методи OSINT Enterprise поліпшують за допомоги управлінських рішень, рівні векторів загроз.

Для систематизації інструментарію та методів виявлення загроз, адаптованих до різних векторів атак, розроблено порівняльну характеристику, наведену в таблиці 1.

Для пояснення класифікації загроз та відповідних засобів протидії в таблиці 1 наведено співставлення векторів ризику з методами OSINT-аналізу.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

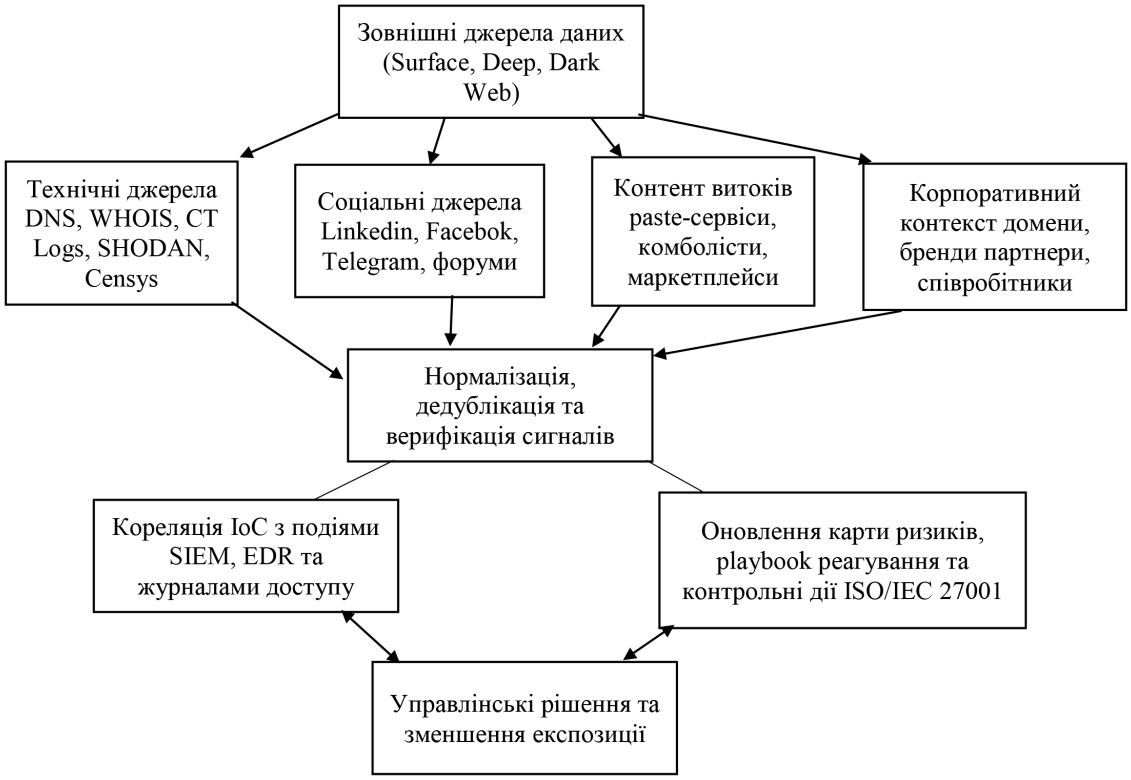

Рис. 2. Структурна модель компонентів Enterprise OSINT в контурі управління ризиками

Таблиця 1

Відповідність векторів кіберзагроз методам OSINT-виявлення та заходам реагування

Вектор загрози	Метод детектування (OSINT)	Очікуваний результат
Компрометація облікових записів	Моніторинг Dark Web маркетплейсів, аналіз Pastebin-ресурсів, пошук у витоках БД	Превентивне скидання паролів, посилення MFA
Тіньова IT-інфраструктура (Shadow IT)	Аналіз пасивного DNS, сканування піддоменів, моніторинг SSL-сертифікатів	Інвентаризація активів, закриття вразливих сервісів
Соціальна інженерія	Профілювання у соціальних мережах (SOCMINT), аналіз зв'язків співробітників	Коригування тренінгів з Security Awareness
Фішинг та клонування бренду	Виявлення тайпосквотингу, моніторинг реєстрації схожих доменів	Блокування шкідливих доменів (Takedown)

Дані таблиці 1 свідчать про те, що для кожного вектора загрози існує специфічний набір OSINT-методик, комплексне застосування яких забезпечує ешелонований захист інформаційного простору підприємства.

Для систематизації основних напрямів застосування Enterprise OSINT у контексті корпоративної безпеки доцільно співвіднести типові вектори загроз із відповідними методами їх виявлення та управлінського реагування. У таблиці 2 наведено класифікацію найбільш поширених загроз, релевантних для цифрового сліду компанії та її співробітників, а також інструментарій Enterprise OSINT, який може бути використаний для їх своєчасної ідентифікації та нейтралізації. Такий підхід дає змогу формалізувати зв'язок між зовнішніми індикаторами ризику та практичними рішеннями в межах системи управління інформаційною безпекою.

Дані таблиці 2 показують, що кожний вектор загрози вимагає не універсального, а контекстно релевантного набору OSINT-методик. Якщо для компрометації облікових записів вирішальним є моніторинг витоків і повторне зв'язування адрес із активними обліковими записами, то для соціальної інженерії ключову роль відіграє аналіз цифрового сліду співробітників. Саме на це вказують автори у роботі [13], які пов'язують публічну поведінку працівників із ризиком profiling-based attacks.

Існуючі роботи аналізують окремий тип сигналів ізольовано. Запропонована таблиця об'єднує технічні, соціальні та репутаційні вектори. Одна модель містить усі три типи. SOC працює окремо від HR-security awareness. Комплаєнс функціонує незалежно від third-party risk management. Запропонована

Таблиця 2

Класифікація векторів загроз та методів Enterprise OSINT для їх нейтралізації

Вектор загрози	Метод Enterprise OSINT	Типовий індикатор	Управлінська дія
Компрометація облікових записів	Пошук витоків у breach-базах, paste-сервісах, dark web-майданчиках	Логін або корпоративний e-mail у комболістах	Примусова зміна паролів, MFA, перегляд ризику доступу
Shadow IT та несанкціоновані активи	Моніторинг DNS, CT Logs, Shodan, Censys, ASN-зв'язків	Невідомий субдомен, тестовий сервіс, відкритий порт	Інвентаризація активів, закриття сервісу, перегляд периметра
Соціальна інженерія щодо працівників	SOCMINT, аналіз профілів, фейкових акаунтів та згадок бренду	Згадки про посаду, відрядження, структуру команди	Адресні тренінги, сповіщення працівників, правила публікацій
Фішинг і typosquatting	Моніторинг нових доменів, сертифікатів та брендових варіацій	Домен, схожий на бренд, новий сертифікат, редирект	Блокування домену, оновлення blacklist, повідомлення партнерів
Репутаційна або партнерська експозиція	Моніторинг медіа, форумів, даркнет-згадок і згадок підрядників	Негативна згадка, пропозиція продажу даних, компрометація постачальника	Ескалація комплаєнсу, third-party risk review, кризові комунікації

модель зменшує цей розрив. Результат має пряму прикладну придатність. Playbook-набори будуються на основі моделей. Triage-правила формуються з неї безпосередньо. Вступ виявив проблему фрагментарного зовнішнього моніторингу. Запропонована модель усуває її.

3.3. Верифікація сигналів, етичні межі та умови практичного застосування. Третя задача дослідження стосувалася процедури перевірки зовнішніх індикаторів, визначення обмежень та опису умов практичного впровадження. Для пояснення логіки перевірки й ухвалення рішень у науковому контексті на рисунку 3 наведено схему послідовної верифікації зовнішнього сигналу та його зіставлення з подіями SIEM.

Рисунок 3 показує логіку верифікації зовнішніх сигналів. Зовнішній сигнал не вважається підтвердженим ризиком автоматично. Первинне виявлення є першим кроком. Чотири послідовні етапи виконуються після нього. Перевірка джерела здійснюється першою. Зіставлення з корпоративними активами виконується другим етапом. Кореляція з внутрішніми подіями проводиться третім. Аналітичне підтвердження контексту завершує процес. Частка хибнопозитивних спрацювань знижується через

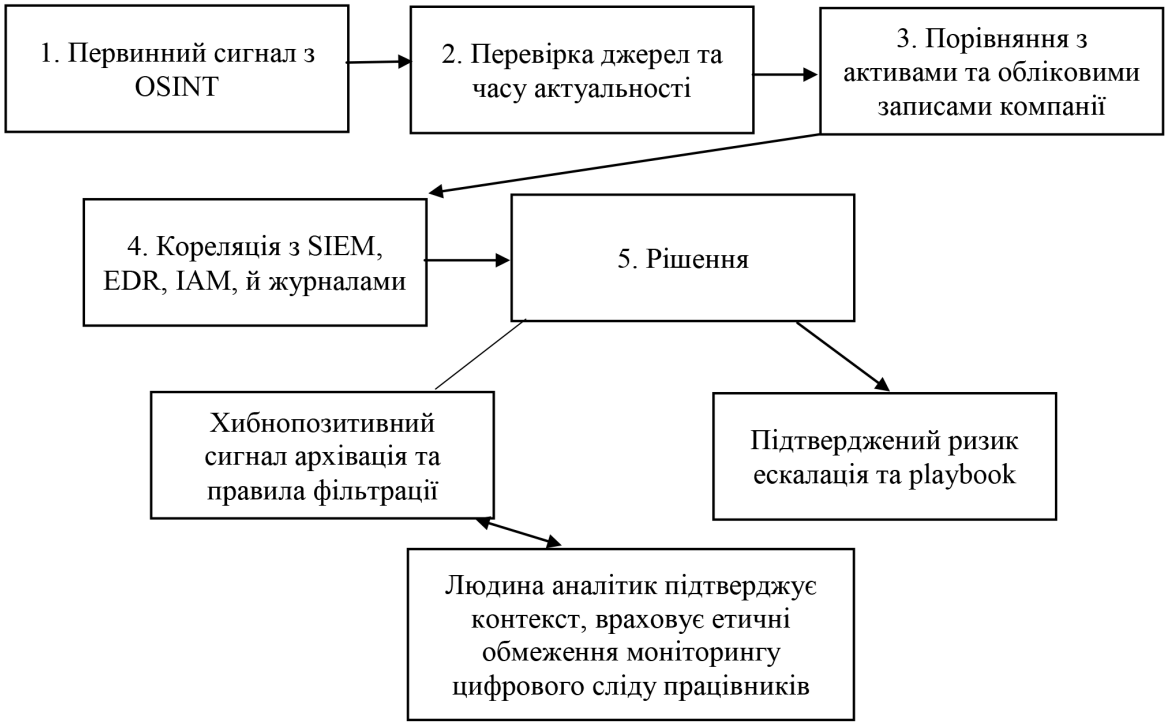

Рис. 3. Процес верифікації зовнішніх індикаторів та кореляції з подіями SIEM

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

цю логіку. Data poisoning блокується. Переваги автоматизації зберігаються. Професійне судження аналітика застосовується там, де потрібно.

Пояснення цього результату пов'язане з наявністю етичних і операційних конфліктів. Автори праці [14] демонструють, що спроба зробити OSINT-процес цілком прозорим і автоматизованим може суперечити вимогам безпеки, неупередженості й точності інтерпретації. Тому в запропонованій моделі людина-аналітик не вилучається з контуру прийняття рішення, а виконує роль верифікатора і коректора автоматично отриманих висновків. На відміну від підходів, у яких CTI-sharing існує як окремий процес, робота [15] підкреслює, що обмін індикаторами стає результативним лише за наявності стандартів їх опису, оцінки довіри до джерел та придатності до машинної обробки. Саме тому в цій роботі CTI розглядається не окремо, а як продовження верифікованого Enterprise OSINT.

Практична цінність запропонованого рішення полягає у можливості використання в SOC, службах інформаційної безпеки, комплаєнсі та корпоративній розвідці. Наявна архітектура безпеки зберігається без радикального перегляду. Перелік об'єктів моніторингу визначається для впровадження. Регламенти перевірки сигналів розробляються. Критерії ескалації встановлюються. Ролі відповідальних осіб призначаються. Обмеженнями дослідження є залежність від якості зовнішніх джерел. Правові режими варіюються між юрисдикціями. Ризик overcollection даних існує. Словники активів потребують постійної актуалізації. Брендові маркери оновлюються регулярно. Кількісна модель пріоритезації сигналів будується як перспектива розвитку. Оцінка зниження часу реагування виконується у майбутньому.

4. Висновки:

1. У межах розв'язання першої задачі систематизовано Enterprise OSINT як шести компонентну модель, що охоплює джерела даних, колектори, нормалізацію, верифікацію, SIEM/CTI-кореляцію та управлінське реагування. Відмінною рисою результату є одночасний облік інфраструктурного і поведінкового цифрового сліду, що дає перевагу над моделями, орієнтованими лише на технічну поверхню атаки. Такий результат пояснюється перенесенням зовнішніх даних у площину операційних індикаторів ризику.

2. За другою задачею розроблено модель з п'яти ключових векторів загроз, для кожного з яких визначено метод Enterprise OSINT, типовий індикатор та управлінську дію. На відміну від розрізнених описів окремих атак, запропоноване рішення формує єдину основу для triage-правил і playbook-процедур. Порівняльна перевага полягає у зв'язуванні соціальних, технічних і репутаційних ризиків у спільній таблиці, що частково закриває проблему фрагментарності моніторингу.

3. За третьою задачею визначено послідовність верифікації зовнішніх індикаторів. Перевірка джерела виконується першою. Кореляція з активами проводиться другою. Зіставлення з SIEM-подіями здійснюється третьою. Аналітичне підтвердження контексту завершує процес. Особливістю результату є збереження людини-аналітика в критичній точці ухвалення рішення. Вплив bias зменшується через це. Хибнопозитивні спрацювання знижуються. Умови для контрольованого впровадження Enterprise OSINT створюються практично. Корпоративні системи безпеки інтегрують його. Політики етичного моніторингу існують при цьому. Регламенти реагування розроблені.

Enterprise OSINT розглянуто як елемент стратегічного управління кіберризиками у межах дослідження. Додатковий інструмент розслідувань не є його функцією. Побудова результативного моніторингу цифрового сліду спирається на два компоненти. Спеціалізоване ПЗ використовується. Вбудовування у процеси СУІБ виконується паралельно. Автоматизація OSINT-даних надає ранні індикатори ризику. Вразливості інфраструктури виявляються швидше. Витоки інформації фіксуються раніше. Ймовірність успішної реалізації кібератак знижується через це. Підходи підвищують Situation Awareness у компанії. Ухвалення обґрунтованих рішень спрощується. Захист активів забезпечується. Персонал захищається. Динамічний ландшафт загроз враховується при цьому.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Валерія Слатвінська – концептуалізація, аналіз джерел, написання основного тексту; В'ячеслав Бевза – методологія, редагування, формування висновків і перевірка узгодженості структури.

References:

1. Chalicheemala, D., & Chalicheemala, D. (2022). What is open-source intelligence and how it can prevent frauds. International Journal for Research in Applied Science & Engineering Technology, 10(9), 1368–1371. https://doi.org/10.22214/ijraset.2022.46268 [in English].

2. Kilani, H., & Qusef, A. (2021). OSINT techniques integration with risk assessment ISO/IEC 27001. In Proceedings of the 2021 6th International Conference on Information Systems Engineering (pp. 1–6). https://doi.org/10.1145/3460620.3460736 [in English].

3. Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, 56, Article 1–38. https://doi.org/10.1007/s10462-023-10454-y [in English].

4. Brunner-Sperdin, A., & Situm, M. (2024). Private social media usage of employees: Implications for corporate risk management to protect corporate reputation. Journal of General Management. Advance online publication. https://doi.org/10.1177/03063070241297372 [in English].

5. Singh, P., Kumar, M., Sharma, N., & Kumar, P. (2025). Study of cyber threat intelligence, risk management and methods. Journal of Information and Optimization Sciences. Advance online publication. https://doi.org/10.47974/JIOS-1852 [in English].

6. El Amin, H., Samhat, A. E., Chamoun, M., Oueidat, L., & Feghali, A. (2024). An integrated approach to cyber risk management with cyber threat intelligence framework to secure critical infrastructure. Journal of Cybersecurity and Privacy, 4(2), 357–381. https://doi.org/10.3390/jcp4020018 [in English].

7. Rajamäki, J., & McMenamin, S. (2024). Utilization and sharing of cyber threat intelligence produced by open-source intelligence. In Proceedings of the 19th International Conference on Cyber Warfare and Security (pp. 341–349). https://doi.org/10.34190/iccws.19.1.2069 [in English].

8. Samad, M. Y., Ningtiyas, B. K., Fiqih, Rosny, F., & Permatasari, D. A. (2024). Anticipating cyber espionage: Open source intelligence (OSINT) investigation and cyber counterintelligence. Journal of Information Systems and Technology, 2(2). https://doi.org/10.31599/288ab341 [in English].

9. Pervez, M. H., Ecevit, M. İ., Naqvi, N. Z., Creutzburg, R., & Dag, H. (2023). Towards better cyber security consciousness: The ease and danger of OSINT tools in exposing critical infrastructure vulnerabilities. In Proceedings of the 8th International Conference on Ubiquitous and Future Networks (pp. 1–6). https://doi.org/10.1109/UBMK59864.2023.10286573 [in English].

10. Szymoniak, S., Foks, K., & Pyrkosz-Dziubczyk, A. (2025). Application of OSINT methods in ensuring cybersecurity. IPSI Transactions on Internet Research. https://doi.org/10.58245/ipsi.tir.2502.05 [in English].

11. Rheault, E., Nerayo, M., Leonard, J., Kolenbrander, J., Henshaw, C., Boswell, M., & Michaels, A. J. (2024). Use and Abuse of Personal Information, Part I: Design of a Scalable OSINT Collection Engine. Journal of Cybersecurity and Privacy, 4(3), 572–593. https://doi.org/10.3390/jcp4030027 [in English].

12. Shoaei, F., Pishdar, M., Bag-Mohammadi, M., & Karami, M. (2026). LROO Rug Pull Detector: A Leakage-Resistant Framework Based on On-Chain and OSINT Signals. arXiv preprint arXiv:2603.11324. https://doi.org/10.48550/arXiv.2603.11324 [in English].

13. Chen, X., Feng, X., Chen, S., Maitre, M., Rakshit, S., Duvieilh, D., Picone, A., & Tang, N. (2026). CyberThreat-Eval: Can Large Language Models Automate Real-World Threat Research? arXiv preprint arXiv:2603.09452. https://doi.org/10.48550/arXiv.2603.09452 [in English].

14. Shoaei, F., Pishdar, M., Bag-Mohammadi, M., & Karami, M. (2026). TM-RUGPULL: A Temporally Sound, Multimodal Dataset for Early Detection of RUG Pulls Across the Tokenized Ecosystem. arXiv preprint arXiv:2602.21529. https://doi.org/10.48550/arXiv.2602.21529 [in English].

15. de Jong, A., Cascavilla, G., & De Pascale, J. (2026). Breadcrumbs in the Digital Forest: Tracing Criminals through Torrent Metadata with OSINT. arXiv preprint arXiv:2601.01492. https://doi.org/10.48550/arXiv.2601.01492 [in English].

Дата надходження статті: 03.04.2026
Дата надходження виправленої версії статті: 10.04.2026
Дата прийняття статті: 17.04.2026
Дата публікації статті: 01.06.2026