DOI: https://doi.org/10.26565/2304-6201-2025-66-04

УДК (UDC) 004.056.53

Дрозд Марія Ігорівна *здобувач вищої освіти ступеня магістра Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна*
e-mail: iammashadrozd@gmail.com
https://orcid.org/0009-0002-9736-8137

Нестеренко Сергій Дмитрович *старший викладач Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна*
e-mail: 654squad@gmail.com;
https://orcid.org/0000-0003-2097-1122

Аналіз програмного забезпечення для реалізації OSINT у сфері інформаційної безпеки

Актуальність. Глобальний сучасний кіберпростір характеризується стрімким зростанням ризиків та загроз для важливої інформації державних структур, бізнесу та суспільства. У таких умовах розвідка з відкритих джерел (OSINT) набуває актуального значення як інструмент для моніторингу інформаційного простору, виявлення потенційних загроз і забезпечення інформаційної безпеки. Програмне забезпечення для OSINT дозволяє ефективно збирати, аналізувати та інтерпретувати дані з відкритих джерел, включаючи соціальні мережі, публічні бази даних і веб-ресурси. Це сприяє своєчасному реагуванню на кіберзагрози, виявленню вразливостей і прийняттю рішень для захисту інформаційних систем і критичної інфраструктури суб'єктів інформаційних відносин держави.

Мета. Аналіз характеристик та можливостей сучасного спеціалізованого програмного забезпечення з метою їх ефективного застосування у якості інструментів розвідки з відкритих джерел (OSINT) у контексті виявлення потенційних загроз і забезпечення інформаційної безпеки суб'єктів інформаційних відносин.

Методи дослідження. У процесі написання статті використано методи технічного аналізу, порівняльно-описового підходу, систематизації та класифікації для дослідження функціональних можливостей інструментів OSINT, прогнозування їхньої ефективності та перспектив розвитку.

Результати. На основі проведеного аналізу визначено ключові характеристики програмних рішень, таких як Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r та SubFinder, оцінено їхню придатність для моніторингу інформаційного простору, виявлення ризиків та вразливостей, а також своєчасне реагування з метою виключення негативних наслідків. Запропоновано рекомендації щодо оптимального використання цих інструментів на сучасних ПЕОМ з урахуванням вимог до апаратного забезпечення, безпеки та автоматизації процесів.

Розгляд прикладних аспектів використання OSINT дає змогу сформулювати практичні рекомендації для фахівців у сфері кібербезпеки. Здійснений аналіз дозволяє інтегрувати результати у навчальні програми для підготовки спеціалістів із захисту інформації. Встановлено, що ефективність OSINT значною мірою залежить від рівня підготовки користувача та його вміння інтерпретувати отриману інформацію. Розглянутий матеріал демонструє перспективи використання машинного навчання для автоматизації процесів збору та фільтрації даних. Зроблено акцент на необхідності безперервного оновлення баз знань і алгоритмів, що використовуються в OSINT. Результати дослідження можуть бути використані для створення комплексних рішень з метою забезпечення кіберстійкості організацій.

Висновки. Розвідка з відкритих джерел (OSINT) базується на зборі, систематизації та аналізі даних із загальнодоступних джерел, таких як соціальні мережі, веб-сайти, публічні бази даних та медіа. Основою функціонування програмного забезпечення для OSINT є використання автоматизованих інструментів, які дозволяють ефективно обробляти великі обсяги інформації, виявляти зв'язки між даними та ідентифікувати потенційні загрози інформаційній безпеці. Такі інструменти, як Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r та SubFinder, забезпечують виконання завдань від пасивного збору даних до активного аналізу мережевої інфраструктури, що дає змогу виявляти вразливості, моніторити кіберпростір та підтримувати прийняття своєчасних рішень у сфері інформаційної безпеки та захисту інформації.

Проведено класифікацію програмного забезпечення для OSINT за функціональним призначенням, виділивши три основні категорії: інструменти виявлення, вилучення та агрегації даних. Запропоновано порівняльний аналіз таких інструментів, як Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r та SubFinder, з визначенням їхніх ключових характеристик, включаючи сумісність з операційними системами, методи збору інформації, автоматизацію процесів та рівень безпеки, що сприяє вибору оптимального інструменту для вирішення завдань моніторингу кіберпростору та протидії інформаційним загрозам.

Наведено перспективні напрямки подальшого розвитку програмного забезпечення для OSINT у сфері кібербезпеки держави.

Ключові слова: *OSINT, програмне забезпечення, аналіз даних, автоматизація, вразливості, .кібербезпека, інформаційна безпека.*

Як цитувати: Дрозд М. І., Нестеренко С. Д. Аналіз програмного забезпечення для реалізації OSINT у сфері інформаційної безпеки. *Вісник Харківського національного університету імені В. Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2025. вип.. 66. С.45-55. https://doi.org/10.26565/2304-6201-2025-66-04

How to quote: Drozd M., Nesterenko S., "Analysis of software for the implementation of OSINT in the field of information security", *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 66, pp. 45-55, 2025. https://doi.org/10.26565/2304-6201-2025-66-04 [in Ukrainian]

Вступ

Стрімкий розвиток цифрових технологій та глобалізація інформаційного простору значно підвищили залежність державних структур, бізнесу та суспільства від інформаційних систем і мережі Інтернет. Це спричинило зростання ризиків, пов'язаних із кібератаками, витоком конфіденційної інформації та маніпуляцією даними. У таких умовах розвідка з відкритих джерел (OSINT) набуває ключового значення як інструмент для моніторингу інформаційного простору, виявлення потенційних загроз і забезпечення інформаційної безпеки. Програмне забезпечення для OSINT дозволяє ефективно збирати, аналізувати та інтерпретувати дані з відкритих джерел, включаючи соціальні мережі, публічні бази даних і веб-ресурси. Це сприяє своєчасному реагуванню на кіберзагрози, виявленню вразливостей і підтримці стратегічного прийняття рішень для захисту інформаційних систем і критичної інфраструктури.

Постановка проблеми

Значною проблемою в реалізації розвідки з відкритих джерел (OSINT) у сфері інформаційної безпеки є стрімке зростання обсягів даних у поєднанні зі складністю їх обробки та аналізу для виявлення релевантної інформації. Сучасні інструменти OSINT стикаються з викликами, пов'язаними з різноманітністю джерел даних, їхньою динамічною природою та необхідністю забезпечення точності й актуальності результатів. З одного боку, зростання обсягів відкритих даних, зокрема з соціальних мереж, веб-ресурсів і публічних баз даних, ускладнює швидке виділення значущих зав'язків і патернів. З іншого боку, активне використання зловмисниками автоматизованих засобів для приховування слідів своєї діяльності, таких як маскування мережевого трафіку чи використання Dark Web, підвищує вимоги до ефективності та гнучкості програмного забезпечення OSINT. Крім того, обмежена сумісність деяких інструментів із різними операційними системами, висока ресурсоємність та необхідність захисту зібраних даних від несанкціонованого доступу ускладнюють їхнє застосування на сучасних ПЕОМ. У контексті гібридних загроз і кіберзлочинності перед науковцями постають завдання поглибленого аналізу сучасного програмного забезпечення для реалізації OSINT у сфері інформаційної безпеки, визначення його функціональних можливостей та ефективності, розробки спеціалізованого програмного забезпечення з метою підвищення продуктивності інструментів OSINT та його адаптивності до нових викликів інформаційної безпеки.

Аналіз останніх досліджень і публікацій

У науковій літературі активно досліджуються можливості розвідки з відкритих джерел (OSINT) для забезпечення інформаційної безпеки. У роботі [5] Williams H. та Blum I. розглянуто другу генерацію OSINT, акцентуючи увагу на його застосуванні в оборонній сфері, зокрема для аналізу великих обсягів даних із відкритих джерел. У [6] Unver A. представлено огляд цифрового OSINT, де підкреслюється важливість аналізу соціальних мереж і Dark Web для виявлення загроз. Дослідження [7] Schwarz K., Schwarz F. Та Creutzburg R. присвячено практичному застосуванню інструментів OSINT, таких як Maltego, для аналізу зав'язків між даними, а також розробці навчальних лабораторних вправ. У [9] Duffy M., Pan X. Та Wilson S. описано методи збору публічної інформації за допомогою інструментів, таких як TheHarvester, з акцентом на пасивні та активні підходи до пошуку даних.

Ураховуючи вищезазначене, дослідження програмного забезпечення для OSINT залишається актуальним завданням, оскільки воно сприяє вдосконаленню методів моніторингу кіберпростору та протидії кіберзагрозам.

Мета статті та завдання

Метою статті є аналіз функціональних можливостей сучасного програмного забезпечення для реалізації OSINT, пошук шляхів їх ефективного використання у сфері кібербезпеки держави.

У відповідності до поставленої мети головними завданнями є:

- аналіз складу та характеристик сучасних інструментів OSINT (Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r та SubFinder), оцінка їхньої можливості з моніторингу інформаційного простору, виявлення ризиків та загроз;
- класифікація програмного забезпечення для реалізації OSINT за функціональним призначенням, обґрунтування рекомендації щодо його оптимального використання на сучасних ПЕОМ з урахуванням вимог до апаратного забезпечення, безпеки та автоматизації процесів;
- обґрунтування перспективних шляхів подальшого розвитку та ефективного використання програмного забезпечення для OSINT у сфері кібербезпеки держави.

Виклад основного матеріалу дослідження

Розвідка з відкритих джерел (OSINT) базується на зборі та аналізі інформації з загальнодоступних джерел, таких як соціальні мережі, веб-сайти, публічні бази даних та медіа, що робить її важливим інструментом для забезпечення інформаційної безпеки. Програмне забезпечення для OSINT, зокрема Maltego , TheHarvester, Shodan, ZoomEye, LeaklX, Sublist3r Та SubFinder, забезпечує виконання широкого спектра завдань: від пасивного збору даних до активного аналізу мережевої інфраструктури.

Зробимо детальний аналіз наведених вище інструментів OSINT, з'ясуємо їх функціональні можливості, а також позитивні властивості, які забезпечують їх ефективне використання.

Програмне забезпечення Shodan.

Shodan - це "пошукова система" об'єктів, підключених до Інтернету, включаючи сервери, роутери, веб-сайти, бази даних, камери, промислові системи управління (ПСУ), камери, мережеві сховища та пристрої Інтернету речей (IoT). Shodan індексує сервісні банери (метадані про програмне забезпечення, що працює на пристрої) і робить їх доступними для пошуку.

Shodan пропонує такі функції:

ShodanSearch: основна пошукова система, яка робить інформацію, зібрану Shodan, доступною через веб-сайт.

ShodanMonitor: дозволяє відстежувати всі свої пристрої, до яких є прямий доступ з Інтернету, для моніторингу безпеки.

ShodanMaps: надає можливість переглядати результати пошуку візуально, а не в текстовому вигляді на головному веб-сайті. Вона відображає до 1 000 результатів одночасно, а при збільшенні/зменшенні масштабу карти пошуковий запит підлаштовується так, щоб показувати результати лише для обраної області.

ShodanImages: Shodan збирає скріншоти для багатьох різних сервісів, і як користувач ви отримуєте доступ до інтерфейсу пошуку, який значно спрощує перегляд цих скріншотів.

ShodanTrends: дозволяє шукати дані, зібрані Shodan, щоб дізнатися про тенденції в Інтернеті.

Дане програмне забезпечення надає низку корисних послуг для розробників, а саме:

1. ShodanDeveloper API: всі веб-сайти Shodan повністю побудовані на одному публічному API Shodan, до якого мають доступ всі користувачі.

2. InternetDBAPI: надає швидкий спосіб побачити відкриті порти для IP-адреси. Він дає швидке уявлення про тип пристрою, який працює за IP-адресою.

3. GeoNetAPI: дозволяє запускати мережеві інструменти з серверів, розташованих по всьому світу. Надає можливість визначати різну поведінку мережі залежно від регіону, в якому знаходиться кінцевий користувач.

4. ShodanChrono: індикатор виконання скриптів.

5. CVEDBAPI: пропонує швидкий спосіб отримати доступ до інформації про вразливості [10].

Перевагами цього інструменту є широка видимість пристроїв Інтернету речей (IoT), а також потужні можливості пошуку та фільтрації. Проте головним недоліком залишаються потенційні проблеми з конфіденційністю та безпекою.

Програмне забезпечення на платформі ZoomEye.

ZoomEye - це безкоштовна платформа, що використовується для збору інформації про сервіси та пристрої, які підключені до Інтернету, а також оцінювання їхньої безпеки та виявлення вразливостей цих систем.

За допомогою ZoomEye можна реалізувати такі операції:

1. Сканування: ZoomEye використовує вузли спостереження, розташовані по всьому світу, для пошуку відкритих портів сервісів і пристроїв.

2. Захоплення банерів: після проведення перевірки сервісу або пристрою цей інструмент накопичує інформацію про банер на порту певного сервісу, на якому він запущений. Інформація про банер зазвичай містить таку інформацію про службу як список портів, що працюють, утиліти, що використовуються та їх версії, яке обладнання використовується для цієї служби та інші характеристики.

3. Індексування: дані, зібрані на минулому етапі, зберігаються та індексуються в базі даних ZoomEye.

4. Пошук і запити: база даних підключається до API ZoomEye, тому користувачі спроможні шукати будь-яку інформацію, що зберігається в цій базі. Пошук можна здійснювати за ключовими словами, а також застосовувати фільтри для точного пошуку.

Функціональні можливості програмного забезпечення на платформі ZoomEye допомагає забезпечити безпеку кіберпростору, а саме:

- здійснює зовнішню спостережність своєї цифрової присутності з перспективи стороннього спостерігача, що дозволяє виявляти слабкі місця системи та ініціювати їх своєчасне усунення;
- надає можливість виявити потенційні вразливості та неправильні конфігурації в мережі;
- допомагає виявляти помилки, які були допущені під час експлуатації мережі, а саме: відкриті порти, застаріле програмне забезпечення або незахищені конфігурації;
- дозволяє перевірити безпеку інших організацій, компаній, що допоможе у безпечному підборі партнерів, попередженню їх про вразливості, тобто управляти сторонніми ризиками;
- забезпечує дослідження та розвідку загроз, в результаті чого користувачі можуть дізнатися, які типи технологій найчастіше використовуються, а також дослідити нові загрози та потенційні вектори атак [11].

Проте цей інструмент несе за собою низку небезпек. Так як ZoomEye доступний для всіх, він може використовуватися зловмисниками для проведення розвідки. Крім того, автоматизувавши процес збору інформації з цього інструменту та інтегруючи її до свого інструментарію, зловмисники постійно матимуть оновлену інформацію про вразливості та доступність до ваших сервісів. З цією метою зловмисники можуть використати, наприклад програмне забезпечення LeakIX. Це потужний ресурс, який дозволяє етичним хакерам, фахівцям з безпеки та іншим користувачам здійснювати всебічний пошук конфіденційної інформації, яка може бути випадково доступна в Інтернеті.

Програмне забезпечення на платформі ZoomEye розділене на дві сфери пошуку:

Services (Сервіси) - це індексація всього, що було відсканована. Сюди входять IP-адреси та віртуальні хости. Зберігається різна інформація, наприклад, банер TCP або HTTP.

Leak (Витік) - в цій сфері індексуються неправильні конфігурації та вразливості, виявлені під час сканування сервісів. Сюди відносяться: виявлена вразливість, неправильна конфігурація інфраструктури, сторінки стану та моніторингу, що містять конфіденційну інформацію, загальнодоступні конфігураційні файли, що містять конфіденційну інформацію, неправильно сконфігуровані ACL (Access Control List), внаслідок чого служби, які мають бути захищені, стають загальнодоступними [12].

Перевагами цього інструменту є велика база даних витоків і витоків даних, а також розширені можливості пошуку та аналізу. Недоліками - обмежений вільний доступ та залежність від зовнішніх джерел даних для збору інформації.

Програмне забезпечення Sublist3r.

Sublist3r - це потужний інструмент, який можна використовувати для автоматизації процесу перерахування субдоменів. Це скрипт Python з відкритим вихідним кодом, який використовує різні методи для збору інформації про субдомени з різних джерел, включаючи пошукові системи, пасивні бази даних DNS і платформи соціальних мереж. Отримавши список субдоменів можна провести їх аналіз, щоб виявити потенційні вразливості та вектори атак [13].

Такий інструментарій зазвичай використовується у комплексі з іншими, адже Sublist3r реалізує лише цю функцію. Взаємодія з Sublist3r відбувається через командний рядок.

Недоліками цього інструменту є обмежені можливості налаштування параметрів сканування та залежність від зовнішніх джерел даних DNS для збору інформації. Перевагами є швидке та ефективне перерахування субдоменів та інтеграція з декількома джерелами даних.

Зважаючи на велику кількість доступних інструментів, докладно проведемо порівняння двох ПЗ, що найчастіше використовуються для збору даних: Maltego та TheHarvester.

Програмне забезпечення Maltego.

Maltego - це інструмент візуального аналізу посилань, який постачається з плагінами з відкритим вихідним кодом під назвою "трансформації", тобто модулі [7]. Maltego дозволяє створювати візуальні графіки зав’язків між даними, такими як email-адреси, IP-адреси та доменні імена, завдяки модулям (трансформаціям), що інтегруються з різними джерелами, включаючи Blockchain.info, Shodan та Social Links CE [7, 8]. Цей інструмент фокусується на аналізі реальних взаємозв'язків між загальнодоступною інформацією про інтернет-інфраструктуру, окремих осіб та організації.

Ці можливості Maltego реалізуються завдяки модулям, з яких складається дане програмне забезпечення, а саме:

модуль CaseFile Entities - це модуль візуального зображення інформації, яку можна використовувати для визначення взаємозв'язків різних типів інформації, в також для побудови графіків взаємозв'язків між частинами інформації;

модулі Blockchain.info та CipherTrac – це модулі для відслідковування і візуалізації зав’язків і транзакцій між криптогаманцями;

модуль Have I been Pwned? – являє собою модуль, який дозволяє провірити чи було зламано сайт, електронну пошту або акаунт, шляхом пошуку в злитих базах скомпрометованих паролів та іншої інформації;

модуль Hybrid Analysis - це незалежний сервіс, який працює на базі Falcon Sandbox і надає підмножину можливостей Falcon Sandbox. Falcon Sandbox - це автоматизоване рішення, яке призначене для аналізу шкідливого програмного забезпечення. Воно виконує глибокий аналіз загроз, збагачує результати аналітикою і надає дієві індикатори компрометації;

модуль PeopleMon – використовується для пошуку інформації про користувача, якого розшукують;

модуль Shodan – дозволяє в середині Maltego використовувати свої позитивні можливості. Shodan являє собою пошукову систему, яка збирає дані з підключених до інтернету пристроїв. Інформацію, яку надає нам цей модуль, це метадані про програмне забезпечення, яке працює на пристрої. Він також дозволяє дослідникам швидко відстежувати відкриті порти, імена хостів та вразливості та пов'язані з IP-адресами;

модуль Social Links CE – дозволяє знаходити відомості про людей та компанії, завдяки використанню різних баз даних, а також надає можливість пошуку реєстраційних даних компаній [8].

Тож, позитивною властивістю та перевагою Maltego є можливість визначати та створювати зв'язки в межах набору даних будь-яким чином. Користувач не обмежений фіксованим форматом попередньо визначених трансформацій і має свободу змінювати концепцію візуалізації залежно від того, що саме є важливим для дослідження.

Програмне забезпечення TheHarvester

Програмне забезпечення TheHarvester спеціалізується на швидкому зборі публічної інформації про домени та компанії через командний рядок, використовуючи пасивні джерела, такі як Google, Bing, Twitter, а також активні методи, як-от перебір DNS [9].

Враховуючи те, що взаємодія з TheHarvester проводиться через командний рядок, користувач має можливість використовувати команди з певними параметрами.

Такими параметрами є:

- d: використовується для пошуку домену або назви компанії;
- b: використовується для вказання джерело даних: bing, google, twitter, yahoo та інші, або для пошуку в усіх джерелах – all;
- s: почати відлік результату з 0;
- v: надає можливість перевірити ім'я хоста через dns і шукати віртуальні хости:
- f: дозволяє зберегти результати у HTML та XML файл;
- n: виконує зворотній запит DNS для всіх знайдених діапазонів;
- c: виконує DNS-перебір для доменного імені;

- t: виконує пошук розширення DNS TLD (Top-Level Domain);
- e: дозволяє використовувати цей DNS-сервер;
- p: проскановує виявлені хости і перевірити їх на можливість перехоплення;
- l: обмежує кількість результатів для роботи;
- h: використовування бази даних SHODAN для запиту знайдених хостів.

Із наведеного вище переліку параметрів зрозумілими є й можливості програмного забезпечення TheHarvester в цілому.

Порівняння характеристик інструментів OSINT, а саме Maltego та TheHarvester, наведене в таблиці 1, яка демонструє їхні переваги та недоліки.

Таблиця 1. Характеристики сучасних інструментів (ПЗ) OSINT
Table 1. Characteristics of modern OSINT tools (software)

Важливі характеристики ПЗ	**MALTEGO**	**TheHarvester**
Сумісність з ОС	Windows, MacOS, Linux	Linux
Основне призначення	Аналіз посилань і пошук взаємозв'язків між даними (Email, IP-адреси, URL-адреси, телефонні номери та інше)	Виявлення публічної інформації про домен або компанію та додаткової інформації (Email, IP-адрес, URL-адреси, порти, імена працівників)
Метод збору інформації	Автоматизовані запити через модулі (трансформації)	Командний рядок з обмеженим набором параметрів
Формат відображення даних	Візуальні зв’язки	Текстові звіти з можливістю збереження у HTML та XML
Автоматизація	Так, через трансформації	Частково
Переваги	Великий набір трансформацій, інтелектуальний аналіз даних у реальному часі, візуалізація графіків, автоматизація запитів	Великий набір джерел даних, активні та пасивні методи збору інформації
Недоліки	Висока вартість, обмежена безкоштовна версія	Обмежена сумісність з ОС, відсутність візуалізації, відсутність документації

Отже, Maltego вирізняється високою функціональністю завдяки автоматизованим запитам і візуалізації, але потребує значних ресурсів, має високу вартість, а у разі використання безкоштовної версії має обмежені можливості. TheHarvester є ефективним для оперативного збору даних, але обмежений сумісністю з Linux і відсутністю візуалізації. Shodan забезпечує індексацію пристроїв, підключених до Інтернету, таких як сервери та IoT-пристрої, дозволяючи виявляти відкриті порти та вразливості [10]. ZoomEye пропонує подібні можливості, але з додатковими функціями для оцінки безпеки та виявлення неправильних конфігурацій [11]. LeakIX фокусується на пошуку конфіденційної інформації, що випадково стала доступною, тоді як Sublist3r та SubFinder ефективно перераховують субдомени, що є ключовим для аналізу потенційних векторів атак [12, 13].

Особливе значення в реалізації OSINT набувають методи збору даних, які поділяються на пасивні, напівпасивні та активні. Пасивний збір передбачає використання загальнодоступних джерел без взаємодії з цільовими системами, напівпасивний — обережне сканування з маскуванням трафіку, а активний — пряму взаємодію, як-от сканування портів [5]. Аналіз даних, зібраних інструментами OSINT, ускладнюється великими обсягами інформації, що потребує застосування технологій Big Data, хмарних обчислень і методів кластеризації для виділення

значущих груп даних. Наприклад, моніторинг соціальних мереж дозволяє створювати психологічні профілі та виявляти зв'язки між особами, тоді як аналіз Dark Web допомагає відстежувати незаконну діяльність [6].

Отже, аналіз програмного забезпечення для OSINT показує, що кожен інструмент має унікальні переваги залежно від завдання: Maltego підходить для комплексного аналізу зв'язків, TheHarvester - для оперативного збору даних, Shodan і ZoomEye - для моніторингу мережевих пристроїв, LeakIX - для пошуку витоків інформації, а Sublist3r та SubFinder - для перерахування субдоменів. Поєднання цих інструментів із сучасними технологіями, такими як штучний інтелект і Від Data, дозволяє створювати ефективні стратегії моніторингу кіберпростору та протидії кіберзагрозам, що є критично важливим для забезпечення інформаційної безпеки в умовах зростаючої інформаційної конкуренції.

Перспективи розвитку програмного забезпечення для OSINT тісно пов'язані з прогресом у сфері штучного інтелекту та машинного навчання. Алгоритми штучного інтелекту можуть автоматизувати відбір джерел, прогнозувати загрози та ідентифікувати об'єкти на зображеннях, що значно підвищує ефективність розвідки [14]. Однак сучасні інструменти стикаються з низкою викликів, таких як: високі вимоги до апаратного забезпечення, необхідність забезпечення конфіденційності даних, ризик використання інструментів зловмисниками для розвідки.

Подальші дослідження показали, що для ефективного використання OSINT на сучасних ПЕОМ, останні повинні мати, як мінімум такі характеристики: процесор – від чотирьохядерного і вище, оперативна пам'ять – не менше 8 ГБ (бажано 16 ГБ), твердотільні накопичувачі (SSD) та оптимізовані операційні системи, такі як Ubuntu, для зменшення ресурсоємності. Використання проксі-серверів, VPN, шифрування даних і регулярне оновлення програмного забезпечення є обов'язковими для забезпечення безпеки та конфіденційності.

Розглядаючи перспективи розвитку програмного забезпечення для OSINT, зараз можна зробити припущення, що подальше зростання ефективності використання OSINT буде пов'язана з високою обчислювальною потужністю процесорів ПЕОМ, їх високими можливостями оперативно виконувати складні завдання зі збору, обробки та аналізу великих обсягів даних. Здатність працювати з великими обсягами публічної інформації і комбінувати різноманітні набори даних з різних джерел значно підвищує ефективність та точність аналізу.

Важливим аспектом майбутнього розвитку програмного забезпечення для OSINT є застосування методів аналізу великих даних (Big Data) та машинного навчання. Ці технології дозволяють автоматизувати процеси розслідування та прийняття рішень, роблячи їх більш інтелектуальними та ефективними. Цей аспект буде одним із ключових у використанні OSINT, оскільки він позначить різницю між дослідженнями, керованими людиною, і дослідженнями, керованими штучним інтелектом.

Високі можливості зберігання, індексації та аналізу інформації дозволяють легко отримати доступ до великих обсягів даних та інформації. У цьому контексті, важливу роль відіграють бази даних, які можуть бути підключені до автоматичних систем збору інформації з відкритих джерел у поєднанні з системами автоматичної індексації зібраних даних та інформації, що дозволяє структурувати дані та інформацію, в тому числі впроваджувати політики щодо дозволів (прав доступу).

Технології штучного інтелекту можуть дозволити автоматизувати платформи для збору даних, а також оптимізувати вибір джерел на основі вимог до колекції. Алгоритми можуть генерувати моделі, які здатні передбачати певні завдання збору відповідно до поточної обробленої інформації, можуть ініціювати вибір найкращих джерел або визначати оптимальні частоти збору. Крім того, алгоритми глибокого навчання сприяють автоматичному прийняттю рішень, що дозволяє динамічно адаптувати завдання збору даних. Таким чином, колекція стає адаптивною, що також тягне за собою зменшення людського фактору. Крім того, застосування штучного інтелекту дозволить використовувати ефективні автоматизовані рішення на етапах обробки інформації та подальшого аналізу. Сценарний аналіз, прогнозний аналіз, встановлення як повторюваних, так і майбутніх закономірностей можливі за допомогою технологій штучного інтелекту. Машинне навчання може виявляти складні кореляції, які природно непередбачувані для людини, що значно покращує ефективність OSINT, а також, використовуючи технології штучного інтелекту, об'єкти можуть бути автоматично ідентифіковані по фотографіях.

Система OSINT є достатньо відкритою, щоб включати дані, які не були отримані з відкритих джерел. Це означає, що OSINT може бути більш ефективним, якщо додати зовнішню інформацію

для доповнення розслідувань. Наприклад, правоохоронні органи можуть використовувати ці технології для підвищення якості керованої інформації та боротьби з терористичними організаціями. У цьому випадку правоохоронні органи можуть співпрацювати з громадянами, оперативні служби можуть використовувати закриту інформацію про кіберзлочинців, а звичайні користувачі можуть поєднувати OSINT із соціальною інженерією для створення профілю своєї цілі.

Гнучке призначення та широка сфера застосування OSINT дозволяють розслідувати різноманітні проблеми та збирати інформацію по всьому кіберпростору. Це може бути корисним для екологічних, психологічних, стратегічних, журналістських, трудових та безпекових аспектів. Наприклад, у сфері злочинності та кібербезпеки OSINT може відстежувати підозрілих осіб або небезпечні групи, виявляти профілі впливу і вивчати тривожні сигнали [23].

Ще одним перспективним напрямком, пов’язаним з подальшим розвитком інструментів збору та аналізу інформації, є роботизація процесів. Ця технологія, дозволяє автоматизувати процеси шляхом конфігурації програмних роботів, які імітують та інтегрують дії людини, взаємодіючі з цифровими системами для виконання різних процесів. Вона дозволить автоматизувати повторювані завдання шляхом обробки та індексування великих обсягів даних, а також забезпечить кореляцію між базами даних, одержувачами, каналами зв'язку та іншими об'єктами. Важливим допоміжним інструментом роботизації процесів є така технологія штучного інтелекту, яка завдяки спеціальним статистичним алгоритмам, обробці природної мови та машинному навчанню дозволяє належним чином ідентифікувати джерела. Крім того, програмні рішення працюватимуть на постійно модернізованій апаратній інфраструктурі. Збільшення швидкості роботи та обчислювальних потужностей ПЕОМ сприятиме розробці все більш складних і досконалих алгоритмів [24].

Отже, розвідка даних з відкритих джерел OSINT вдосконалюється разом із загальними тенденціями технічного прогресу. Кожний етап зумовлює використання найефективніших технологій, відомих на певний час. Розвиток технологій штучного інтелекту, автоматизація роботизованих процесів, розробка та упровадження квантових комп'ютерів задля вирішення зростаючих потреб та можливостей у кіберпросторі майбутнього, без сумніву, зумовлюють передумови для пошуку у подальшій перспективі шляхів підвищення ефективності використання OSINT.

Висновки й перспективи подальших досліджень

У статті проведено аналіз програмного забезпечення для реалізації розвідки з відкритих джерел (OSINT) у сфері інформаційної безпеки, зокрема розглянуто інструменти Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r та SubFinder.

Запропоновано класифікацію цих інструментів за функціональним призначенням (виявлення, вилучення, агрегація даних) та надано рекомендації щодо їхнього оптимального використання на сучасних ПЕОМ з урахуванням вимог до апаратного забезпечення, безпеки та автоматизації процесів.

Наведено можливі напрямки подальшого розвитку з метою підвищення ефективного використання програмного забезпечення для OSINT у сфері кібербезпеки держави.

Цінність отриманих результатів дослідження у сфері інформаційної безпеки полягає у поглибленому розумінні можливостей зазначеного вище програмного забезпечення для OSINT, щодо збору, аналізу та обробки відкритих даних для виявлення кіберзагроз і вразливостей. У роботі підкреслено необхідність гнучкого вибору інструментів залежно від типу загроз і специфіки інформаційного середовища. Результати можуть бути застосовані для вдосконалення моніторингу інформаційного простору, оптимізації роботи з великими обсягами даних та підвищення ефективності захисту інформаційних систем у сучасних умовах гібридних загроз і кіберзлочинності.

Практична цінність результатів дослідження полягає в систематизації характеристик інструментів OSINT, що дозволяє сформулювати у технічному завданні на створення спеціалізованого програмного забезпечення обґрунтованих вимог щодо підвищення продуктивності інструментів OSINT, його адаптивності до стрімкого зростання гібридних загроз і кіберзлочинності у сучасних умовах.

Особливу увагу слід приділити розробці адаптивних моделей, здатних динамічно підлаштовуватися до нових джерел даних і типів кіберзагроз. Крім того, перспективним є

створення інтегрованих платформ, які поєднують можливості OSINT із технологіями Big Data та хмарними обчисленнями, а також розробка мобільних додатків для оперативного моніторингу інформаційного простору в реальному часі.

Впровадження таких технологій сприятиме підвищенню ефективності OSINT у сферах кібербезпеки, розвідки та соціальних досліджень, забезпечуючи швидке реагування на нові виклики інформаційної безпеки.

Отже, мета статті, яка полягала в аналізі програмного забезпечення для реалізації OSINT у сфері інформаційної безпеки, досягнута.

СПИСОК ЛІТЕРАТУРИ

1. National Defense Authorization Act for Fiscal Year 2006 : Public Law of 01.06.2006 no. No. 109-163. https://www.congress.gov/bill/109th-congress/house-bill/1815/text/statute
2. Гончаренко Ю., Канішев К. Інструменти інформаційної боротьби: OCIHT, ІПСО та протидія дезінформації. Інформаційно-психологічна операція (ІПСО). Як не стати жертвою чужих маніпуляцій. https://infolight.in.ua/wp-content/uploads/2023/02/brochure-2.pdf
3. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII: станом на 31 берез. 2023 р. https://zakon.rada.gov.ua/laws/show/2469-19#Text
4. Про розвідувальні органи України : Закон України від 22.03.2001 р. № 2331-III : станом на 24 жовт. 2020 р. https://zakon.rada.gov.ua/laws/show/2331-14#Text
5. 5. Williams H., Blum I. Defining second generation open source intelligence (OSINT) for the defense enterprise. RAND Corporation, 2018. https://doi.org/10.7249/rr1964
6. Unver A. Digital open source intelligence and international security: a primer. EDAM, Oxford CTGA & Kadir Has Üniversitesi, 2018. 28 p. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331638
7. Schwarz K., Schwarz F., Creutzburg R. Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT). Electronic imaging. 2020. Vol. 2020, no.3. P.278 https://library.imaging.org/admin/apis/public/api/ist/website/downloadArticle/ei/33/3/art00010
8. Аналіз інструментів збору розвідувальної інформації з відкритих джерел / А. Карпенко та ін. Комунікаційні та інформаційні системи : Вісник. Київ, 2022. С. 21. https://www.viti.edu.ua/files/zbk/2022/2022-1.pdf#page=18
9. Duffy M., Pan X., Wilson S. Information reconnaissance by accumulating public information data sources. OALib. 2024. Vol. 11, no. 04. P. 1–25. https://doi.org/10.4236/oalib.1111463
10. 1Shodan Products. https://www.shodan.io/about/products
11. ZoomEye - cyberspace search engine. ZoomEye - Cyberspace Search Engine. https://www.zoomeye.hk/doc
12. LeakIX docs. LeakIX documentation | LeakIX Docs. https://docs.leakix.net/docs/
13. What is Sublist3r and How to Use it? - GeeksforGeeks. GeeksforGeeks. https://www.geeksforgeeks.org/what-is-sublist3r-and-how-to-use-it/
14. The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends / J. Pastor-Galindo et al. IEEE access. 2020. Vol. 8. P. 10282–10304. https://doi.org/10.1109/access.2020.2965257

REFERENCES

1. National Defense Authorization Act for Fiscal Year 2006 : Public Law of 01.06.2006 no. No. 109-163.
https://www.congress.gov/bill/109th-congress/house-bill/1815/text/statute
2. Y. Honcharenko, K. Kanishev. Tools of information warfare: OSINT, IPSO and counteracting disinformation. Information and psychological operation (IPSO). How to avoid becoming a victim of other people's manipulations. [in Ukrainian]
https://infolight.in.ua/wp-content/uploads/2023/02/brochure-2.pdf
3. On the national security of Ukraine : Law of Ukraine No. 2469-VIII of June 21, 2018: as of March 31, 2023. [in Ukrainian]
https://zakon.rada.gov.ua/laws/show/2469-19#Text
4. On the intelligence agencies of Ukraine : Law of Ukraine No. 2331-III of March 22, 2001: as of October 24, 2020. [in Ukrainian]
https://zakon.rada.gov.ua/laws/show/2331-14#Text
5. Williams H., Blum I. Defining second generation open source intelligence (OSINT) for the defense enterprise. RAND Corporation, 2018.
https://doi.org/10.7249/rr1964
6. Unver A. Digital open source intelligence and international security: a primer. EDAM, Oxford CTGA & Kadir Has Üniversitesi, 2018. 28 p.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331638
7. Schwarz K., Schwarz F., Creutzburg R. Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT). Electronic imaging. 2020. Vol. 2020, no.3. P.278
https://library.imaging.org/admin/apis/public/api/ist/website/downloadArticle/ei/33/3/art00010
8. Analysis of intelligence gathering tools from open sources / A. Karpenko et al. Communication and information systems : Bulletin. Kyiv, 2022. P. 21. [in Ukrainian]
https://www.viti.edu.ua/files/zbk/2022/2022-1.pdf#page=18
9. Duffy M., Pan X., Wilson S. Information reconnaissance by accumulating public information data sources. OALib. 2024. Vol. 11, no. 04. P. 1–25.
https://doi.org/10.4236/oalib.1111463
10. Shodan Products.
https://www.shodan.io/about/products
11. ZoomEye - cyberspace search engine. ZoomEye - Cyberspace Search Engine.
https://www.zoomeye.hk/doc
12. LeakIX docs. LeakIX documentation | LeakIX Docs.
https://docs.leakix.net/docs/
13. What is Sublist3r and How to Use it? - GeeksforGeeks. GeeksforGeeks.
https://www.geeksforgeeks.org/what-is-sublist3r-and-how-to-use-it/
14. The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends / J. Pastor-Galindo et al. IEEE access. 2020. Vol. 8. P. 10282–10304.
https://doi.org/10.1109/access.2020.2965257

Drozd Maria Igorivna *Master's degree candidate, Institute of Special Communications and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
e-mail: iammashadrozd@gmail.com
https://orcid.org/0009-0002-9736-8137

Nesterenko Serhiy Dmytrovych *Senior Lecturer, Department of the Institute of Special Communications and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
e-mail: 654squad@gmail.com;
https://orcid.org/0000-0003-2097-1122

Analysis of software for the implementation of OSINT in the field of information security

Relevance. The global modern cyberspace is characterized by a rapid increase in risks and threats to important information of government agencies, business and society. In such circumstances, open source intelligence (OSINT) is gaining importance as a tool for monitoring the information space, identifying potential threats and ensuring information security. OSINT software allows you to effectively collect, analyze and interpret data from open sources, including social networks, public databases and web resources. This facilitates timely response to cyber threats, identification of vulnerabilities and decision-making to protect information systems and critical infrastructure of the state's information relations entities.

Objective. To analyze the characteristics and capabilities of modern specialized software with a view to their effective use as open source intelligence (OSINT) tools in the context of identifying potential threats and ensuring information security of subjects of information relations.

Research methods. In the process of writing this article, the author used the methods of technical analysis, comparative and descriptive approach, systematization and classification to study the functionality of OSINT tools, to predict their effectiveness and development prospects.

Results. Based on the analysis, the key characteristics of software solutions such as Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r and SubFinder are identified, their suitability for monitoring the information space, identifying risks and vulnerabilities, as well as timely response to eliminate negative consequences are assessed. Recommendations for the optimal use of these tools on modern computers are proposed, taking into account the requirements for hardware, security and process automation.

Consideration of the applied aspects of OSINT use makes it possible to formulate practical recommendations for cybersecurity professionals. The analysis makes it possible to integrate the results into training programs for information security specialists. It has been established that the effectiveness of OSINT largely depends on the level of user training and his/her ability to interpret the information received. The material reviewed demonstrates the prospects for using machine learning to automate data collection and filtering processes. The author emphasizes the need to continuously update the knowledge bases and algorithms used in OSINT. The results of the study can be used to create integrated solutions to ensure the cyber resilience of organizations.

Conclusions. Open source intelligence (OSINT) is based on the collection, systematization and analysis of data from publicly available sources, such as social networks, websites, public databases and media. The basis of OSINT software is the use of automated tools that allow you to efficiently process large amounts of information, detect connections between data, and identify potential threats to information security. Tools such as Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r, and SubFinder provide tasks ranging from passive data collection to active analysis of network infrastructure, which allows identifying vulnerabilities, monitoring cyberspace, and supporting timely decision-making in the field of information security and information protection.

The author classifies OSINT software by functional purpose, allocating three main categories: tools for detection, extraction and aggregation of data. A comparative analysis of such tools as Maltego, TheHarvester, Shodan, ZoomEye, LeakIX, Sublist3r and SubFinder is proposed, with the definition of their key characteristics, including compatibility with operating systems, methods of information collection, process automation and security level, which helps to choose the optimal tool for solving the problems of monitoring cyberspace and countering information threats.

Promising directions for further development of OSINT software in the field of cybersecurity of the State are presented.

***Keywords**: OSINT, information security, software, cyber threats, data analysis, automation, vulnerabilities.*

Надійшла у першій редакції 09.04.2025, в останній - 15.05.2025.
The first version has been received on 09.04.2025, the final version - on 15.05.2025.