

Міністерство освіти і науки України
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»
Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

Білостоцький технологічний університет (Польща)

Університет прикладних наук (Литва)

Відземський університет прикладних наук (Латвія)

Університет «Aurel Vlaicu» в м. Арад (Румунія)

Міжнародний науково-освітній та навчальний центр (Естонія)

Київський національний університет імені Тараса Шевченка
Кафедра фінансів

Донецький національний університет імені Василя Стуса
Національний технічний університет «Дніпровська політехніка»

Луцький національний технічний університет

Одеський національний економічний університет

РОЗВИТОК ФІНАНСОВОГО РИНКУ В УКРАЇНІ: ЗАГРОЗИ, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

**Матеріали VII Міжнародної науково-практичної
конференції**

27 листопада 2025 р.

Полтава
2025

7. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки*. 2024. №. 2 (49). С. 307–313.

8. Національне агентство з питань запобігання корупції. URL: <https://dap.nazk.gov.ua/en/direction/9/table/>.

9. Onyshchenko S., Hlushko A., Maslii O., Chumak O. (2024). Digital transformation of the national economy in the context of information environment development in Ukraine. *Transformations of national economies under conditions of instability*. Scientific Route OÜ. Tallinn, Estonia, P. 169–197. DOI: <https://doi.org/10.21303/978-9916-9850-6-9.ch6>.

УДК 336.6:004.738.5

Черв'як Анна Володимирівна³,
доктор філософії, доцент

Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

OSINT ЯК ІНСТРУМЕНТ ЗМІЦНЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Гібридна війна, яку веде РФ проти України, супроводжується масштабними інформаційно-психологічними, кібернетичними та економічними атаками. Так, Державна служба спеціального зв'язку та захисту інформації України [1] повідомляла, що у 2024 році кількість кібератак на Україну зросла на 69,8%, досягнувши 4315 інцидентів, у порівнянні з 2023 роком, коли було зафіксовано 2541 кіберінцидентів. У сучасних умовах фінансова безпека держави залежить не лише від ефективності економічної політики, а й від здатності своєчасно виявляти та нейтралізувати загрози, що формуються у відкритому інформаційному середовищі. Одним із ключових інструментів такого моніторингу є OSINT.

OSINT – це розвідка з відкритих джерел, яка побудована на основі збирання, упорядкування, аналізу та використання публічно доступної інформації з метою отримання розвідувальних даних. Вона базується на відкритому доступі до інформаційних ресурсів, таких як соціальні мережі, медіа, публікації в інтернеті, урядові звіти та інші джерела [2, с. 70]. Ключова ідея розвідки з відкритих даних полягає у тому, що значний масив цінної інформації знаходиться у вільному доступі і не потребує високого рівня доступу до неї. Проте, потрібно розуміти яка інформація є важливою (з усього доступного масиву даних) та як правильно її аналізувати.

Законом України «Про національну безпеку України» визначено, що однією із фундаментальних національних інтересів України є державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями [3].

Фінансова безпека України як складова економічної та національної безпеки охоплює захист фінансової системи від зовнішніх та внутрішніх загроз, які можуть бути пов'язаними із корупційними схемами, тіншовими операціями та операціями із відмивання коштів, фінансуванням тероризму та кібератаками [4].

В умовах ведення гібридної війни вагомо значення набувають аналітичні інструменти котрі надають оперативну інформацію для аналізу та ухвалення рішень.

³ Тези підготовлено в межах виконання НДР молодих учених «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди», державний реєстраційний номер 0124U000615

OSINT є одним із таких інструментів. Відповідно до ключових положень та методів обробки інформації [4, с. 77; 5; 6], OSINT виконує наступні ключові функції у сфері фінансової безпеки:

1) ідентифікація фінансових ризиків на основі аналізу відкритих даних про компанії, партнерів, транзакції, санкції та їх обходи, зв'язки власників, ланцюги поставок;

2) моніторинг тіньових потоків за допомогою аналізу даних із відкритих реєстрів, митної статистики;

3) виявлення економічних операцій ворога, спрямованих на підрив стабільності (інформаційно-економічні диверсії, маніпуляції активами, хакерські атаки на фінансові установи);

4) аналіз поведінки ринку за допомогою даних соціальних мереж, форумів, біржових індикаторів, криптовалютних блокчейнів.

Сучасна гібридна війна активно застосовує кібератак на державні інформаційні системи, банки та фінансові установи. OSINT сприяє ранньому виявленню підготовки кібератак через моніторинг хакерських форумів, цифрових слідів та дослідженню інфраструктури бот-мереж, які можуть штучно впливати на фінансові індикатори.

Таким чином, OSINT є важливим елементом попередження та швидкої реакції на економічні диверсії, спрямовані на дестабілізацію фінансової системи України.

OSINT-технології відіграють ключову роль у зміцненні фінансової безпеки України в умовах гібридної війни. Вони забезпечують оперативне виявлення ризиків, сприяють прозорості фінансових операцій, допомагають протидіяти кіберзагрозам, тіньовим потокам та економічним диверсіям ворога. Інтеграція OSINT у державну систему фінансової безпеки створює підґрунтя для формування стійкої, технологічно захищеної економіки, здатної ефективно реагувати на виклики сучасного безпекового середовища.

Література

1. Державна служба спеціального зв'язку та захисту інформації України URL: <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvava-4315-kiberincidentiv>.

2. Murat Tinas, Dogukan Tuncal. OSINT in the Techno-Political Era: From Intelligence Collection. Security, Law, and Influence in the Age of Techno-Politics, 2025. P. 69-86. URL: https://books.google.com.ua/books?hl=uk&lr=&id=LB2PEQAAQBAJ&oi=fnd&pg=PA69&dq=osint&ots=0SNluxQOqs&sig=MRjXorxUsLpjPbVhPGQpWLBtbFc&redir_esc=y#v=onepage&q=osint&f=false.

3. Закон України «Про національну безпеку України», URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

4. Onyshchenko S., Maslii O., Maksymenko A. Financial security hazards of Ukraine: identification and systematization. *Economics & Regions*. 2019. №2 (73). P. 72-80.

5. Аналітичні показники всіх територіальних громад в Україні, URL: <https://clarity-project.info/hromada>.

6. Реєстр компаній, пов'язаних з рф та рб, для професійної перевірки контрагентів та виявлення російського коріння, URL: <https://vkursi.pro/russianbeneficiary#analysis>.

7. Маслій О.А. Методичні засади ідентифікації загроз економічній безпеці держави. *Економіка і регіон*. 2017. №6 (67). С. 28–34.

8. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. *Economic and cyber security*. Kharkiv: PC TECHNOLOGY CENTER, 30–58.

9. Маслій О.А., Глушко А.Д. Державне фінансове регулювання як інструмент мінімізації загроз економічній безпеці України в умовах воєнного стану. *Цифрова економіка та економічна безпека*. 2022. Вип. 2 (02). С. 125-130.