УДК 004.056.55+343.9+004.738.5

***Нихода Станіслав Сергійович***
***(наук. керівник – д-р наук із соц. комунікацій, професор Тур О. М.)***
***Кременчуцький національний університет***
***імені Михайла Остроградського, м. Кременчук***

# ДАРКНЕТ У КОНТЕКСТІ ТОРГІВЛІ ІНФОРМАЦІЄЮ

*Анотація. Автор дослідив приховані частини інтернету, а саме вказав на особливості Surface Web, Dark Web та Deep Web.*

*Ключові слова: даркнет, захист інформації, кіберзлочинність.*

Інтернет складається з трьох основних рівнів:

1. Поверхневий веб (Surface Web). Це частина інтернету доступна для індексації пошуковими системами, як-от Google чи Bing. Сюди входять публічні вебсайти, блоги, новинні ресурси та інші загальнодоступні сторінки.

2. Глибокий веб (Deep Web). Цей рівень містить контент, який не індексується пошуковими системами. Прикладом є захищені паролем сайти, приватні бази даних, внутрішні корпоративні мережі та інший контент, доступ до якого обмежений.

3. Темний веб (Dark Web). Частина глибокого вебу, доступ до якої можливий лише через спеціалізовані програмні засоби, як-от браузер Tor. Темний веб відомий своєю анонімністю та використовується для різних цілей, як легальних, так і нелегальних.

Термін «Даркнет» часто використовується як синонім темного вебу. Це мережа, яка функціонує поверх інтернету та забезпечує анонімність користувачів. Темний веб використовується для різних цілей, включно з захистом приватності, коли журналісти, активісти та інші особи використовують даркнет для обходу цензури та захисту своєї діяльності від стеження, а також для нелегальної діяльності, оскільки він став платформою для торгівлі наркотиками, зброєю, фальшивими документами та іншими незаконними товарами та послугами.

Незважаючи на свою репутацію даркнет – це не завжди щось незаконне. Важливо розуміти, що це не один сайт, а ціла прихована мережа, яку умовно можна уявити як айсберг. На вершині його є доволі звичайні запити, як-от утрачені книги, а вже на дні – щось незаконне та аморальне [2].

Найпопулярнішим інструментом для доступу до даркнету є браузер Tor (The Onion Router). Tor використовує багатошарове шифрування для анонімізації трафіка, що дає змогу користувачам приховувати свою IP-адресу та місцезнаходження. Важливо розуміти, що сам по собі доступ до даркнету не є незаконним. Насправді існують авторитетні бренди та компанії, які мають сайти, доступні через темний веб. Однак багато видів діяльності, що здійснюються в даркнеті, є протизаконними. Тому користувачам треба бути обережними та дотримуватися законів своєї країни під час використання темної сторони вебу [3].

Як вже зазначалось, одним із головних інструментів для доступу до даркнету є браузер Tor, який забезпечує анонімність завдяки технології багатошарового шифрування. Принцип його роботи можна описати так: маршрутизація через ви-

падкові вузли, коли користувач підключається до мережі Tor, його запит не йде напряму до вебсайта, а проходить через декілька проміжних серверів; шифрування на кожному етапі, де перед тим, як запит залишає пристрій користувача, він шифрується кілька разів, що є подібним до шарів цибулі, звідки й походить назва «Onion Routing»; і декодування на проміжних вузлах, де кожен вузол отримує тільки ту частину запиту, яка дає змогу йому передати його далі, не знаючи, звідки цей запит прийшов і куди він прямує.

Система Onion Routing забезпечує рівень анонімності, який робить відстеження користувачів надзвичайно складним, якщо не неможливим. Проте треба пам'ятати, що вихідний вузол може перехопити незашифровані дані, тому для додаткового захисту часто використовується VPN.

Через свою популярність як майданчика доступу до темного вебу Tor-браузер має неоднозначну репутацію. Він задумувався як браузер, здатний надати користувачеві анонімність, якої так сильно не вистачає в сучасному інтернеті, у ньому немає нічого особливого. Але через свою репутацію в деяких країнах сам факт його використання може вимагати пояснень.

Окрім Tor, існують і інші технології, що забезпечують анонімний доступ до даркнету. Це I2P (Invisible Internet Project) – децентралізована анонімна мережа, яка використовує технологію «тунелів» для приховування трафіка. Вона більш стійка до атак, ніж Tor, але менш популярна. Також є Freenet – пірингова мережа для обміну файлами, яка дає змогу розповсюджувати інформацію без централізованого контролю [1].

На відміну від Tor, який дає змогу виходу у звичайний інтернет, I2P та Freenet функціонують як повністю ізольовані мережі.

Як зазначалось раніше, даркнет не є єдиною платформою, а складається з численних ринків, які спеціалізуються на різних видах товарів та послуг. Основні категорії, які нас цікавлять – це продаж викрадених даних, як-от облікові записи, паролі, бази даних клієнтів компаній, кіберзброя, що включає шкідливе програмне забезпечення (віруси, руткіти, ботнети), та фінансові злочини, до яких належать фальшиві документи, викрадені кредитні картки та відмивання грошей через криптовалюту.

Даркнет-маркети працюють за принципом eBay або Amazon, але з акцентом на повну анонімність і криптовалютні розрахунки.

Раніше основною платформою був Silk Road, який функціонував за моделлю маркетплейсу з рейтингами продавців і гарантіями угод. Після його закриття з'явилися десятки нових майданчиків, як-от AlphaBay, Hansa Market, Wall Street Market.

Оскільки традиційні банки та платіжні системи не працюють у даркнеті, більшість угод здійснюється через криптовалюти.

Щоб підвищити рівень анонімності, користувачі можуть використовувати «блендери» (mixers) – сервіси, які перемішують кошти від різних людей, ускладнюючи їх відстеження.

Попри кримінальний характер ринків, вони функціонують за суворими правилами та принципами довіри.

Даркнет є не лише прихованою частиною інтернету, а й глобальною платформою для кіберзлочинності. Це місце, де можна знайти торгові майданчики для викрадених даних, хакерські послуги, зброю, наркотики, підроблені документи та багато іншого. Це своєрідний «дикий Захід» цифрового світу, де діють свої правила та власні механізми безпеки. Основними компонентами його економіки є маркетплейси, де продаються нелегальні товари та послуги, хакерські форуми, де обговорюють методи атак, обмінюються вразливостями та продають шкідливе ПЗ, криптовалюти, що є основним способом розрахунку, забезпечуючи анонімність платежів, та анонімні сервіси зв'язку, як-от шифровані месенджери та форуми для координації дій злочинців [4].

Даркнет важко контролювати через його децентралізовану природу. Раніше кіберзлочини здебільшого здійснювали окремі хакери-одинаки, але сьогодні діють цілі злочинні організації. Деякі з найбільших кіберкартелів функціонують як класичні мафіозні угруповання, маючи ієрархію, розподіл обов'язків і систему покарань. Сучасні кіберзлочинні угруповання працюють так само, як великі транснаціональні корпорації, використовуючи маркетинг, службу підтримки клієнтів і навіть програми лояльності для постійних покупців.

Попри складність боротьби з кіберзлочинністю у даркнеті, правоохоронні органи все активніше залучають нові методи, зокрема розвідувальні операції, які включають впровадження агентів у хакерські спільноти, злам даркнет-сервісів (наприклад, операція «Onymous», під час якої ФБР ліквідувало ринок Silk Road), співпрацю з криптобіржами для відстеження незаконних транзакцій та міжнародні санкції, що передбачають обмеження для країн, які підтримують кіберзлочинців.

Темний веб став унікальним фінансовим простором, де діють закони попиту та пропозиції, але без державного регулювання. Основними платіжними засобами тут є криптовалюти, що гарантує анонімність. Економіка даркнету функціонує на базі принципів довіри та криптографічних механізмів захисту, створюючи альтернативний ринок поза межами державного контролю.

Особливостями його економіки є відсутність традиційної фінансової звітності, використання escrow-сервісів для захисту покупців і продавців, значна частка шахрайських схем та коливання цін, які залежать від політичної та економічної ситуації.

Попри свій нелегальний характер, він має значний вплив на глобальні фінансові системи. Щороку через нелегальні маркетплейси проходять мільярди доларів. Це ціла паралельна економіка, яка впливає на реальні фінансові ринки, викликаючи зміни в законодавстві та регулюванні криптовалют. Основні наслідки такої активності для світової економіки включають зростання попиту на криптовалюти, оскільки нелегальна активність стимулює розвиток технологій блокчейну, збільшення випадків шахрайства, оскільки ринок даркнету створює загрозу для фінансових установ, і підвищення рівня кібербезпеки, адже банки та компанії змушені вдосконалювати свої системи захисту.

**Список використаних джерел**

1. Figueras-Martín E., Magán-Carrión R., Boubeta-Puig J. Drawing the web structure and content analysis beyond the Tor darknet: Freenet as a case of study. *Journal of Information Security and Applications.* 2022. 103229. Vol. 68.
2. Mirea M., Wang V., Jung J. The not so dark side of the darknet: A qualitative study. *Security Journal.* 2018.Vol. 32. P. 102–118.
3. Okyere-Agyei S. The Dark Web – A Review. *Advances in Multidisciplinary and Scientific Research Journal Publication*. 2022.
4. Yannikos Y., Heeger J., Steinebach M. Scraping and analyzing data of a large darknet marketplace. *Journal of Cyber Security and Mobility*. 2023. Vol. 12. P. 161–186.

УДК 001.89:303](73)

***Олійник Ірина Віталіївна***
***(наук. керівник: д-р іст. наук, професор Федотова О. О.)***
***Маріупольський державний університет, м. Київ***

## ДІЯЛЬНІСТЬ ЗАРУБІЖНИХ АНАЛІТИЧНИХ ЦЕНТРІВ (НА ПРИКЛАДІ ФОНДУ РАССЕЛА СЕЙДЖА)

*Анотація. Авторкою висвітлено діяльність «фабрик думок» як ключових аналітичних осередків із надання рекомендацій щодо впровадження інноваційних підходів у державному управлінні та стратегічному плануванні. Уточнено поняття «аналітичний центр» та охарактеризовано основні форми діючих аналітичних центрів. Окрему увагу приділено історії започаткування, становлення та розвитку американського Фонду Рассела Сейджа. Розкрито основні напрями функціонування осередку на сучасному етапі, зокрема щодо створення аналітичної продукції.*

*Ключові слова: аналітичні центри, «фабрики думок», «мозкові центри» США, дослідження, інформаційне забезпечення, аналітика, аналітична продукція.*

У сучасному світі інформація є стратегічним ресурсом, що визначає успішність прийняття управлінських рішень, формування державної політики та розвитку бізнесу. В умовах глобалізації, зростання обсягів даних і загострення конкуренції підвищується потреба в якісному інформаційному аналізі, що сприяє формуванню ефективних стратегій у різних сферах суспільного життя. Одним із ключових інститутів, які забезпечують аналітичний супровід процесів прийняття рішень, можна вважати фабрики думок. Вони відіграють значну роль у розробці стратегічних ініціатив, проведенні досліджень у сфері політики, економіки, технологій, екології та безпеки. Фабрики думок виступають посередниками між академічною наукою, урядами, громадянським суспільством і бізнесом, сприяючи прийняттю обґрунтованих рішень [7].

Зарубіжний досвід показує, що високорозвинені країни активно використовують потенціал таких аналітичних центрів для впровадження інноваційних підходів до державного управління та стратегічного планування.

Аналітичні центри (think tanks, «мозкові центри», «фабрики думок») – це самостійні, незалежні дослідницькі організації, що складаються з експертів, які