УДК 343.85(477)

**МАЗЕПА С.,** *кандидат юридичних наук, доцент*, доцент кафедри кримінального права та процесу Західноукраїнського національного університету, міжнародний дослідник Оснабрюцького університету
ORCID: https://orcid.org/0000-0003-1282-9089

# ДАНІ ЯК ТОВАР: ТЕНДЕНЦІЇ КІБЕРЗЛОЧИННОСТІ В ЄВРОПІ 2025

DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346493

***Анотація.*** *У статті досліджено актуальні тенденції кіберзлочинності в Європі з акцентом на багатофункціональну роль даних: як цілі, засобу і товару. На основі звітів Europol, ENISA, CERT-EU та інших аналітичних джерел розкрито, як персональні дані, логіни, фінансова та стратегічна інформація стають об'єктами атак з боку злочинців. Окрема увага приділена зростанню загроз, пов'язаних із використанням штучного інтелекту: створенням діпфейків, генерацією фішингових повідомлень, маніпулятивних наративів та атак нового типу — Man-in-the-Prompt. Автор наводить приклади реальних інцидентів, зокрема кейс Arup, та підкреслює ключову роль людського фактора, соціальної інженерії та цифрової необізнаності як головних вразливостей. Пріоритети безпеки зміщуються до простих, але системних речей: акцент на кібергігієну та приватність, обов'язковість багатофакторної аутентифікації, базова кіберосвіта, преведення симуляцій та експериментів, мінімізації прав доступу, регулярних оновлень і резервного копіювання, а також прозорості від постачальників. Головна мета — зменшити цінність викрадених даних і скоротити час від виявлення до відновлення.*

***Ключові слова:*** *інформаційна безпека, кібербезпека, кіберзлочинність, захист даних, штучний інтелект.*

***Summary.*** *The article explores current trends in cybercrime across Europe, with a particular focus on the multifunctional role of data — as a target, a tool, and a commodity. Drawing on analytical reports by Europol, ENISA, CERT-EU, and other expert bodies, the study examines how personal data, login credentials, financial, and strategic information become objects of criminal exploitation. Special attention is given to the growing threats associated with the use of artificial intelligence, including the creation of deepfakes, automated phishing messages, manipulative narratives, and emerging attack types such as Man-in-the-Prompt. The author provides real-world case studies, notably the Arup incident, and highlights the critical role of the human factor, social engineering, and digital illiteracy as primary vulnerabilities. Security priorities are shifting towards simple yet systemic measures: an emphasis on cyber hygiene and privacy, mandatory multi-factor authentication, basic cybersecurity education, simulation-based training, minimization of access rights, regular updates and data backups, and supply chain transparency. The overarching objective is to reduce the value of stolen data and minimize the time between incident detection and recovery.*

***Keywords:*** *information security, cybersecurity, cybercrime, data protection, artificial intelligence.*

**Вступ.** У даній статті висвітлено основні тенденції кіберзлочинності у Європі із акцентом на дані, які можуть мати різні функціональні ролі під час вчинення кіберзлочину. В основі дослідження лежать звіти Європолу Internet organized crime threat assessment 2025 [1] та Internet Organised Crime Threat Assessment 2025 [2], звіт команди реагування на кіберподії в Європейському Союзі CERT-EU Threat Landscape Report

2024 [3], звіт Агенства з кібербезпеки ЄС – ENISA Threat Landscape 2024 і 2025[4, 14] та інші авторитетні звіти та дослідження.

Не секрет, що центральним товаром у світі кіберзлочинності є дані або ж інформація. Такий товар можна вкрасти або продати, також товар може бути метою, ціллю або засобом вчинення злочину.

**Метою статті** є аналіз сучасних тенденцій розвитку кіберзлочинності у Європі на підставі міжнародних звітів експертних установ та формулювання пріоритетів інформаційної безпеки особи та держави.

**Виклад основного матеріалу.** В умовах сьогодення відбувається трансформація усіх сфер людського життя в інформаційний простір. Витік, знищення або спотворення даних (персональних даних, підприємницької інформації, відомостей, що становлять, банківську або комерційну таємницю тощо) становить чималу небезпеку. Із розвитком штучного інтелекту і активним використанням великих мовних моделей спостерігається не лише полегшення людської діяльності в різних сферах, але і зростає можливість дешево і швидко створити шкідливе програмне забезпечення, вдосконалити методи кібершахраства, таргетованого фішингу тощо. Аналітика великих даних та штучний інтелект (ШІ) можуть містити галюцинації. Висновки та прогнозування щодо поведінки, уподобань та приватного життя окремих осіб можуть бути хибними. Ці висновки ґрунтуються на дуже різноманітних та багатих на особливості даних, цінність яких неможливо передбачити, і створюють нові можливості для дискримінаційного, упередженого та інвазивного прийняття рішень [9].

В даному дослідженні ми використовуємо категорію “дані” (англ.data), розуміючи інформацію або відомості, втрата, витік, або знищення яких може завдати економічної або репутаційної шкоди фізичній або юридичній особі. У юридичній літературі існує чимало підходів до визначення інформації. Віктор Борисов, Олександр Пащенко, Михайло Карчевський, Михайло Шепітько, Леся Демидова, Олександр Дудоров, Володимир Тацій, Олександр Семенюк, Ольга Сосніна, Дарина Куковинець та інші вітчизняні науковці зробили вагомий внесок у тлумачення інформації як предмету незаконного посягання. Коротко характеризуючи, підкреслимо що цінність інформації визначає її змістовна сутність.

Згідно з Оксфордським словником для учнів (2021), дані – це “факти або інформація, особливо коли їх досліджують та використовують для з’ясування інформації або прийняття рішень” [6]. “Персональні дані” означає будь-яку інформацію, що стосується ідентифікованої фізичної особи (“суб’єкта даних”); ідентифікована фізична особа – це особа, яку можна ідентифікувати прямо чи опосередковано, зокрема, шляхом посилання на ідентифікатор, такий як ім’я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або на один чи декілька факторів, характерних для фізичної, фізіологічної, генетичної, психічної, економічної, культурної чи соціальної ідентичності цієї фізичної особи [7]. В даному дослідженні центральну увагу приділено викраденню вхідних даних (англ. credentials).

*Функціональні ролі даних в кіберзлочинності*

В умовах цифровізації особливо мають охоронятися вхідні дані, а саме паролі і логіни, які надають доступ до поштових скриньок, до профілів у соцмережах, до профілів у різноманітних сервісах і на публічних сайтах, також банківські дані, ця інформація є чутливою та потребує надійного захисту.

Крім того, деякі персональні дані злочинцям дуже легко знайти через відкриті ресурси. І такі інструменти як OSINT, є помічниками не лише для правоохоронних органів, але й для злочинців. Надзвичайно легко ідентифікувати особу, знайти її місце

проживання, інформацію про стосунки, родичів, вподобання. Отже, можна зробити аналіз інформації з відкритих джерел і знайти дуже багато інформації про особу. У звітах інституцій з кібербезпеки дані під час вчинення кіберзлочинів розглядаються в наступних якостях:

1. Дані як ціль. Такі дії як викрадення даних, їх шифрування, видалення, спотворення як у приватних осіб, так і компаній, державних інституцій, критичної інфраструктури тощо, на нашу думку поділяються на 2 види: 1) З метою збагачення; 2) З політичною метою, наприклад патріотичні настрої, та інше.

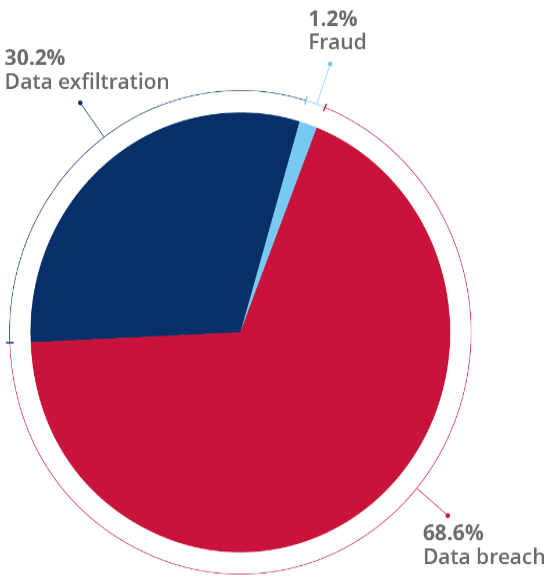
2. Дані як засіб. Персональні дані які використовуються в шахрайстві, наприклад, де людина знаходилася, чим займалася, хто вона. Для того, щоб створити певні маніпулятивні наративи для жертви і в результаті отримати гроші. Це стосується сексуальної експлуатації дітей, а також створення фейків, діпфейків щоб обманути чи обдурити наприклад банк чи працівників компанії, якщо злочинці створюють голос або навіть відео керівника.

3. Дані як товар. Такі дані або інформація, як правило, використовується для вчинення подальших злочинів або злочинних операцій. Вони як правило продаються на спеціальних платформах, в Dark неті, та у злочинних мережах.

*Вплив на дані*

Далі ми розкриємо яким чином здійснюється вплив на дані або інформацію. На нашу думку, причиною успіхів кіберзлочинності є вразливість людини, а вразливість машини (комп'ютерного пристрою) все ж таки на другому місці. Спочатку поговоримо про те, як отримують незаконним способом вхідні дані. За допомогою різноманітних шахрайських схем. Дешевий і дієвий інструмент для злочинців – це соціальна інженерія. Це метод маніпулятивного впливу на користувачів з метою отримання конфіденційної інформації, становить серйозну загрозу сучасній кібербезпеці. На відміну від технічних атак, які базуються на експлуатації вразливостей програмного забезпечення, соціальна інженерія експлуатує вразливість людської психіки та людський фактор, зокрема довіру та допитливість користувачів [10; С.40]. За допомогою цього інструменту здійснюється персоналізований або таргентований фішинг. Часто користувачі інтернету можуть перейти по посиланню на подібний сайт, схожий інтерфейс, і різниця можливо тільки в одному знакові або букві. Таким чином, злочинці отримують інформацію про логіни та паролі. Шкідливе програмне забезпечення активно використовуються злочинцями для викрадення інформації.

***Fig. 4*** - Outcome of identified intrusions.
Source: ENISA dataset




Діаграма звіту ENISA 2025 демонструє, що із задокументованих вторгнень 68,6% призвели до витоків даних, виставлених на продаж на кіберзлочинних форумах; при цьому 2,8% із цих "рекламованих" витоків були подані як прямий наслідок атаки програм-вимагачів. Ексфільтрація

даних, зокрема викрадення облікових даних (8,9%) та стратегічне збирання даних (21,3%), разом становила 30,2% [14].

*Сучасні кейси та персональний досвід.* У 2025р. Європол розпочав співпрацю з Microsoftom та підтримав 2-у частину міжнародної операції Endgame з правоохоронцями. Мета цієї співпраці зупинити дію Луми, найбільшого викрадача інформації у світі. Злочинці за допомогою цієї програми можуть викрадати дані у великих об'ємах із скомпрометованих девайсів. Персональні дані, фінансові дані, вхідні дані, та інше є об'єктом для використання інструменту Луми. Microsoft ідентифікував близько 394.000 Windows комп'ютерів які були заражені шкідливим програмним забезпеченням Лума. В основному, злочинці використовують повідомлення, і мейли, в різноманітних месенджерах та соціальних медіа, які містять отруєні посилання, або перехід на фішингові сайти. Нещодавно я сама отримала негативний досвід, підписавшись на відому газету на фішинговому сайті. Впродовж кількох місяців з мого рахунку автоматично списувалися кошти. Сума була невеликою тому я на це одразу не звернула увагу. Тому це надзвичайно важливо, перевіряти усі деталі і оригінальність сайтів та інформації розміщеної на їхніх сторінках. Ще один новий і вже дуже поширений вид інтернет шахрайства, який я часто зустрічаю - це повідомлення від нібито кур'єрської служби. У повідомленні висловлюється прохання оплатити абсолютно мізерну суму для того, щоб кур'єр зміг здійснити повторну доставку. Або адресу було змінено і треба відкоригувати вашу адресу і відповідно користувач має надіслати уточнену адресу або якщо це оплата навіть суми у 1-2 гривні, Користувач все одно вносить в фішинговий сайт банківські реквізити, і це є великим ризиком.

Наприклад, ви можете скачати на ніби офіційному сайті якусь програму, або можливо навіть антивірус, які насправді є замаскованим шкідливим програмним забезпеченням. У звіті Європолу, також згадується техніка клік фікс, суть якої полягає в тому що інтернет користувачі можуть отримувати додаткові запити у вигляді спливаючих вікон з проханням натиснути кнопку "я не робот". І після такого натискання можна також запустити роботу шкідливого програмного забезпечення на своєму комп'ютері. Ще один варіант коли користувач копіює і вставляє текст з інтернету. Через текст також шкідливе забезпечення може потрапити у власний комп'ютер чи ноутбук. Вішинг як різновид кібершахрайства, також посідає не останнє місце. Коли інформація шахраями отримується в результаті телефонної розмови. В Україні існує чимало схем, коли запитують персональну інформацію по телефону, щоб потрапити до банківського рахунку або профілю у додатку.

Окремо слід наголосити на кібербезпеці компаній, та роботі з персоналом, у тому числі навчаннях з кібергігієни. Особливу увагу треба приділяти працівникам, які щойно прийняті на роботу,а також працівникам, яких звільнено [16; С.164].

Штучний інтелект у кіберзлочинності відіграє центральну роль. За допомогою штучного інтелекту можна покращити техніки соціальної інженерії та прописувати кращі тексти для повідомлень шахраїв, враховуючи особливості певних жертв, їхню культуру мову та інші особливості. Крім того, як відомо, злочинці можуть створювати тепер високої якості діпфейки з голосами або відео, і вчиняти шахрайства в компаніях. Наведемо кейс компанії Arup (Гонконг, 2024) – це діпфейк-шахрайство з багатомільйонними наслідками.

У 2024 році міжнародна інжинірингова компанія Arup зазнала збитків на суму приблизно 25 мільйонів доларів США внаслідок складної шахрайської операції із застосуванням технологій діпфейку. Зловмисники організували відеоконференцію за участю кількох осіб, де були використані фальшиві (діпфейкові) зображення та голоси

фінансового директора та інших співробітників компанії. Один із працівників фінансового підрозділу, вважаючи, що бере участь у справжній внутрішній нараді, отримав інструкції щодо здійснення "конфіденційного" переказу коштів. Протягом приблизно одного тижня він виконав 15 транзакцій на п'ять місцевих банківських рахунків, загальна сума переказів становила приблизно 20 мільонів фунтів. У травні 2024 року Arup офіційно підтвердила факт інциденту, зауваживши, що внутрішні інформаційні системи не були зламані. Інцидент розцінено як приклад соціальної інженерії, підсиленої новітніми цифровими технологіями [6].

Ще один новий тренд, це Man-in-the-Prompt: невидима атака на штучний інтелект, яка може зачепити кожного. Ми звикли довіряти ChatGPT, Gemini, Copilot чи Claude як "розумним помічникам" у роботі, навчанні та щоденних завданнях. Але мало хто здогадується: саме поле вводу у браузері може стати точкою зламу. Йдеться про Man-in-the-Prompt (MitP) — нову кіберзагрозу, яку експерти вже називають невидимим ворогом ШІ. Вперше описана дослідниками безпеки у 2025 році. Вона є різновидом prompt injection, але відбувається не на стороні моделі, а ще в браузері.

Атака починається зі звичайного браузерного розширення — калькулятора, словника чи нотатника. На вигляд воно безпечне, але має доступ до вмісту сторінок. У момент, коли ви вводите промпт у ChatGPT чи Gemini, плагін аналізує ваш такст та вбудовує приховані інструкції. Пізніше дані пересилаються зловмиснику. Такий відозмінений запит надсилається до великої мовної моделі, а вже відповідь містить маніпуляції. В результаті висока ймовірність витоку даних, наприклад, фінансової звітності або клієнтських баз. Небезпечним є обхід захисту, оскільки антивіруси не бачать атаку, бо вона відбувається ще у браузері.

*Прогнозування розвитку кіберзлочинності та формулювання пріоритетів інформаційної безпеки особи та держави (***замість висновку***).*

Отже, дані сьогодні стали головною "валютою" кіберзлочинців. В умовах революції штучного інтелекту спостерігається зсув балансу, де штучний інтелект допомагає злочинцям більше ніж так званим білим хакерам, які захищають системи критичної інфраструктури. Кіберзлочинці, здебільшого мають корисливий мотив або мотиви певних переконань або патріотизму. Злочинці прагнуть не лише зламати систему — їм потрібні персональні записи, фінансова інформація, комерційні, банківські та державні таємниці. Завдяки розвитку штучного інтелекту тепер доступний широкий вибір інструментів для створення фішингових листів, та підроблених документів. Крадіжка паролів і сесій відбувається тихо й швидко. Паралельно зростають ризики у хмарних сервісах і ланцюгах постачання: помилки налаштувань, "зайві" доступи та уражені оновлення здатні призвести до масових витоків.

Замість класичного шифрування дедалі частіше застосовується "чистий" шантаж: дані просто викрадають, погрожують оприлюднити і вимагають викуп. Очікується чимало нових ризиків та викликів, пов'язані з ШІ. Небепека використання персональних даних із приватних ботів великих мовних моделей, відновлення прихованої інформації з моделей, отруєння та промпт ін'єкції датасетів, підміна контенту тощо.

Таким чином пріоритети безпеки зміщуються до простих, але системних речей: акцент на кібергігієну та приватність, обов'язковість багатофакторної аутентифікації, базова кіберосвіта, преведення симуляцій та експериментів, мінімізації прав доступу, регулярних оновлень і резервного копіювання, а також прозорості від постачальників. Мета — зменшити цінність викрадених даних і скоротити час від виявлення до відновлення.

**Використана література:**

1. Europol. Steal, deal and repeat – How cybercriminals trade and exploit your data : Internet Organised Crime Threat Assessment (IOCTA) 2025. Luxembourg : Publications Office of the European Union, 2025. 28 p. – URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf (дата звернення: 18.09.2025).

2. Europol. The changing DNA of serious and organised crime : European Union Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA 2025). Luxembourg : Publications Office of the European Union, 2025. 100 p. – URL: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime (дата звернення: 18.09.2025).

3. CERT-EU. Threat Landscape Report 2024: A Year in Review. Version 1 – 25 February 2025. Brussels : CERT-EU, 2025. 20 p. – URL: https://cert.europa.eu/publications/threat-intelligence/tlr2024/ (дата звернення: 18.09.2025).

4. Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Lage der IT-Sicherheit in Deutschland 2024. Bonn : BSI, 2024. – URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf (дата звернення: 18.09.2025).

5. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. 2024. – URL: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (дата звернення: 18.09.2025).

6. Oxford Learner's Dictionary. (2021). Data. Oxford University Press. Retrieved May 3, 2021, URL: https://www.oxfordlearnersdictionaries.com/definition/english/data

7. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник ЄС. 2016. L 119. С. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 01.10.2025).

8. Кримінально-правова охорона інформаційної безпеки в Україні:монографія [В. І. Борисов, О. О. Пащенко, Д. П. Євтєєва та ін.]; за заг.ред. В. І. Борисова, О. О. Пащенка ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків. Право, 2024. 328 с.

9. Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2).

10. Жмурко О. І. Соціальна інженерія як загроза кібербезпеці: методи запобігання та захисту. Педагогіка безпеки. 2024. С. 37-42

11. UK engineering firm Arup falls victim to £20m deepfake scam. URL: https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video

12. Mike K., Hazzan O. What is data science? Communications of the ACM. 2023. Т. 66. №. 2. С. 12-13.

13. Solove D. J. Data is what data does: Regulating based on harm and risk instead of sensitive data Nw. UL Rev. 2023. Т. 118. С. 1081.

14. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf (дата звернення: 18.10.2025).

15. Mazepa S. Digital Violence and the Human Rights Dimension //Krytyka Prawa. 2025. С. 138.

16. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. Актуальні проблеми правознавства. 2025. №. 2. С. 164-171.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~