

Разінкін Н.С.

аспірант

*Одеський національний економічний університет***Федосюк Д.С.**

Державний реєстратор

Razinkin Nikita

Postgraduate student

*Odesa National Economic University***Fedosiuk Dmytro**

State registrar

**БІЗНЕС-РОЗВІДКА В ЦИФРОВОМУ СЕРЕДОВИЩІ:
ЮРИДИЧНИЙ ТА АНАЛІТИЧНИЙ АСПЕКТИ****BUSINESS INTELLIGENCE IN THE DIGITAL ENVIRONMENT:
LEGAL AND ANALYTICAL ASPECTS**

У статті здійснено комплексний аналіз правових аспектів застосування бізнес-розвідки в умовах цифрової економіки, що характеризується динамічним розвитком технологій та швидким зростанням обсягів даних. Розглянуто проблематику дотримання інтелектуальних прав, конфіденційності, безпеки персональних даних, правомірності використання відкритих джерел і результатів, отриманих алгоритмічно. Звернено увагу на потребу гармонізувати національні законодавчі норми з глобальними стандартами (зокрема, GDPR), формувати етичні кодекси, запроваджувати принципи «privacy by design» і «privacy by default». Окремлено юридичні виклики впровадження штучного інтелекту, машинного навчання та глибинного аналізу, що ускладнюють правове поле. Запропоновано рекомендації для вдосконалення нормативної бази, саморегуляції, посилення корпоративних політик і зміцнення інституційної інфраструктури задля сталого, відповідального та безпечного розвитку Бі у глобальному цифровому середовищі.

Ключові слова: бізнес-розвідка, цифрове середовище, правове регулювання, персональні дані, кібербезпека, штучний інтелект.

This article examines the key legal aspects of employing Business Intelligence (BI) tools in today's rapidly evolving digital economy. As companies increasingly rely on BI to transform raw data into strategic insights, legal frameworks have become crucial to ensuring both innovation and compliance. The study highlights issues of intellectual property rights, data privacy, confidentiality, and the lawful usage of open-source and publicly accessible information, including social media profiles. It also considers the complexities introduced by artificial intelligence (AI), machine learning, and deep learning algorithms that generate new patterns and knowledge. A central concern is the alignment of national legislation with international standards, such as the EU's General Data Protection Regulation (GDPR), which enforces rigorous requirements for handling personal data. The article stresses the need for transparent licensing terms, ethical codes of conduct, and stronger corporate policies to prevent misuse of information, safeguard consumer rights, and avoid reputational damage. In this context, principles like "privacy by design" and "privacy by default" are essential to maintain trust and meet regulatory demands. As global data flows transcend jurisdictional boundaries, the paper acknowledges the importance of international cooperation and harmonized legal frameworks that promote fair competition, protect intellectual property, and ensure cybersecurity. It calls for the development of clear guidelines on algorithmically generated outputs, the reduction of discriminatory biases, and greater accountability for automated decision-making processes. In conclusion, the article suggests strategic recommendations for enhancing legal and ethical standards, improving institutional oversight, and fostering interdisciplinary dialogue. By creating robust legal infrastructures, refining corporate governance, and encouraging responsible data management, stakeholders can unlock the full potential of BI technologies while preserving fundamental rights, maintaining market integrity, and supporting sustainable digital innovation.

Keywords: efficiency, effectiveness, effect, result, resources, expenses, measuring, estimation.

Постановка проблеми. Постійний розвиток цифрового середовища та поширення технологій бізнес-розвідки відкривають перед підприємствами нові можливості для аналізу даних, формування стратегій та управлінських рішень. Проте стрімке зростання

обсягів інформації, різноманіття джерел даних, інтенсивне використання штучного інтелекту та алгоритмічних рішень зумовлюють потребу у чіткому правовому регулюванні цих процесів. Відсутність узгоджених правових рамок, гармонізованих зі світовими стандар-

тами, створює ризики порушення прав інтелектуальної власності, недотримання стандартів конфіденційності та захисту персональних даних, а також ймовірність виникнення юридичних колізій у транснаціональних транзакціях. Тобто, постає проблема розробки збалансованого правового базису, що забезпечить легітимне, етично виважене та інноваційно-сприятливе застосування ВІ-технологій (Business Intelligence, BI) у глобальному цифровому просторі.

Аналіз останніх досліджень і публікацій. Аналіз досліджень у галузі бізнес-розвідки в цифровому середовищі, зокрема в аспектах юридичного та аналітичного характеру, показує, що ці два напрямки мають тісний взаємозв'язок, зокрема через вплив цифрових технологій на стратегічне управління та забезпечення інформаційної безпеки.

Д.С. Усов [1] звертає увагу на важливість конкурентної розвідки для формування стратегії компанії, акцентуючи на необхідності врахування змін у цифровому середовищі. Ці зміни включають використання великих даних та їхню обробку, що підвищує важливість юридичних аспектів, зокрема захисту персональних даних та корпоративної інформації. В цьому контексті В.М. Шоненберг [2] та І. Падова [2] вивчають вплив нових європейських регулювань у галузі захисту даних, що створюють нові правові вимоги для бізнес-операцій в цифровому середовищі. Це, у свою чергу, визначає підходи до використання та збереження даних у процесах бізнес-розвідки.

Окрім того, дослідження таких авторів, як Д.Дж. Солов [3], вказують на обмеження прав на приватність, що додає складнощів в обробці великих даних для бізнес-цілей.

Дослідники, як Х.Р. Варіан [4] досліджують вплив великих даних на економічні процеси, наголошуючи на важливості їх аналізу для прийняття ефективних рішень у бізнесі. Вони підкреслюють, що в умовах цифрового середовища бізнес-розвідка набуває нових вимірів, де юридичний та аналітичний аспекти відіграють ключову роль. Варіан зазначає, що бізнес-розвідка вимагає чіткої структури і стратегії збору даних, адже в умовах цифрової трансформації дані стають не лише ресурсом, але й об'єктом правового регулювання.

А. Аквісті [5], К. Тейлор [5] та Л. Вегман [5] аналізують економіку конфіденційності, що є ключовим фактором у сфері бізнес-розвідки, оскільки збір і аналіз даних мають юридичні та етичні обмеження.

Формулювання завдання дослідження. Дослідити правові аспекти застосування технологій бізнес-розвідки в цифровому середовищі, визначити ключові напрями їх правового регулювання, а також сформулювати рекомендації щодо гармонізації національних та міжнародних норм задля забезпечення безпечної, етично обгрунтованої та інноваційно-сприятливої практики використання ВІ-інструментів у сучасних бізнес-процесах.

Виклад основного матеріалу дослідження. Бізнес-розвідка – це сукупність процесів, методів, технологій та інструментів, спрямованих на збирання, обробку, аналіз, візуалізацію та інтерпретацію бізнес-даних з метою підтримки прийняття стратегічних, тактичних і оперативних управлінських рішень. Завдяки бізнес-розвідці організації можуть краще розуміти ринкові тенденції, поведінку споживачів, ефективність

внутрішніх процесів та конкурентне середовище, що в підсумку підвищує продуктивність, конкурентоспроможність та інноваційний потенціал підприємства [1]. Сучасне цифрове середовище формує унікальний простір для збору, обробки та інтерпретації великих масивів бізнес-даних. Бізнес-розвідка, як міждисциплінарний напрям, поєднує інструменти статистики, економіко-математичного моделювання, машинного навчання та обробки природної мови з метою перетворення первинної інформації на цінні знання для стратегічних управлінських рішень. Дослідження міжнародних консалтингових компаній, таких як Gartner та IDC, підтверджують стрімкий ріст обсягів електронних транзакцій та даних – за прогнозами IDC, глобальний обсяг даних до 2025 року перевищить 175 зетабайтів. У такому контексті роль ВІ стає визначальною для формування конкурентних стратегій, адаптації до динамічних ринкових умов, підвищення ефективності бізнес-процесів і отримання довгострокових переваг [2].

Наукові дослідження у сфері ВІ та права активно проводяться у провідних університетах та аналітичних центрах. Наприклад, професор В. Майєр-Шенбергер з Оксфордського університету у своїх працях звертає увагу на політико-правові аспекти використання великих даних і підкреслює важливість регулювання, що не лише захищає приватність, а й забезпечує інноваційну динаміку ринків [3]. Професор Д. Солов з Університету Джорджа Вашингтона відомий дослідженнями у галузі права даних, конфіденційності та інформаційної безпеки, зокрема критичним аналізом правових основ захисту інформації та впливу сучасних технологій на особисті права [4]. Економіст Г. Варіан, головний економіст Google і професор Каліфорнійського університету у Берклі, досліджував економічні аспекти використання даних, враховуючи правові бар'єри та стимули, створені регуляторною базою [5]. Вчені такі як А. Аквісті з Університету Карнегі-Меллон аналізують поведінкові та економічні фактори приватності, пропонуючи правові та етичні рамки для розуміння компромісів між вигодою від використання даних та ризиками порушення конфіденційності [6].

Цифрова економіка, побудована на основі інтернет-технологій, мобільних застосунків, хмарних обчислень, соціальних мереж, технологій Інтернету речей та штучного інтелекту, вимагає чітких правових механізмів. Правова регламентація процесів збору, зберігання, аналізу, використання та транскордонної передачі даних набуває ключового значення. Забезпечення відповідності вимогам електронної комерції, захист прав споживачів, інтелектуальної власності та кібербезпеки є стратегічним викликом як для держав, так і для корпорацій. Аналітичні можливості ВІ стають не просто засобом обробки звітності, а комплексним інструментарієм виявлення прихованих закономірностей, моделювання поведінки споживачів та прогнозування ринкових трендів.

Історія застосування бізнес-розвідки в Україні розпочалася на початку 2000-х років, коли великі банки, телекомунікаційні та торговельні компанії почали впроваджувати перші аналітичні платформи для підтримки управлінських рішень. Спершу це був переважно базовий аналіз фінансово-операційних показників із використанням іноземних програмних продуктів [7]. З часом зростання обсягів даних та розвиток локаль-

ної IT-інфраструктури дали поштовх до інтеграції BI з ERP-, CRM- та іншими корпоративними системами.

Після 2010 року в Україні активніше застосовуються прогнозна аналітика, візуалізація даних, Big Data, штучний інтелект та хмарні сервіси. З'явилися місцеві фахівці та IT-компанії, що пропонують власні BI-рішення. Паралельно посилюються вимоги до безпеки та захисту даних, а бізнес усе частіше орієнтується на міжнародні стандарти й правові норми.

В Америці, де інструменти BI почали активно впроваджуватися ще у 1990-х роках, сьогодиншній ринок відзначається високим рівнем зрілості та інновацій, широким спектром програмних рішень і послуг, а також потужними науково-дослідними центрами. Саме американський досвід суттєво вплинув на світову практику використання BI, задавши стандарти інтероперабельності, інформаційної безпеки та дотримання етичних норм [8].

У Європейському Союзі центральною правовою рамкою є Загальний регламент про захист даних (GDPR, 2016/679), що з 2018 року встановив суворі вимоги до прозорості обробки персональної інформації, підзвітності суб'єктів даних та дотримання принципів «privacy by design» і «privacy by default» [9]. Реальний приклад – розробка аналітичної платформи для великого онлайн-ритейлера, де за замовчуванням мінімізується збір і використання персональних даних, а користувачеві пропонуються конфіденційні налаштування з самого початку. Принципи «privacy by design» та «privacy by default», сформульовані в галузі права даних та інженерії конфіденційності інтегрують безпеку даних у початкові етапи розробки систем, а не як вторинну опцію.

У таблиці 1 наведено узагальнені дані про оцінку глобальних витрат (ринкового розміру) у сфері бізнес-розвідки, взяті з відкритих джерел та аналітичних досліджень міжнародних агентств.

Право інтелектуальної власності у контексті BI охоплює захист алгоритмів, аналітичних методик, патентування новітніх рішень у сфері машинного навчання, а також авторське право на унікальні аналітичні панелі, процеси візуалізації та структурування даних. Наприклад, в IT-секторі нерідкими стають кейси патентування інноваційних алгоритмів, розроблених для прогнозування динаміки фондового ринку або оптимізації

логістичних ланцюгів. Питання власності алгоритмічних рішень, створених штучним інтелектом, активно вивчають науковці, зокрема Р. Кало та В. Гартцог, які досліджують етичні та правові аспекти діджиталізації й автоматизації [12].

Міжнародні стандарти та норми, розроблювані організаціями, такими як ISO, IEEE, WIPO, прагнуть узгодити регуляторні підходи у сфері кібербезпеки, захисту даних та інтелектуальної власності. Стандарти серії ISO/IEC 27000 спрямовані на впровадження систем керування інформаційною безпекою, а рекомендації IEEE орієнтовані на етичні та технічні аспекти використання штучного інтелекту [13]. Відповідна гармонізація правових норм сприяє уникненню фрагментації ринків, забезпечує інтероперабельність та підвищує загальну довіру до глобального обміну даними.

Корпоративні практики також трансформуються: великі міжнародні фінансові установи, технологічні компанії та виробничі гіганти інвестують в навчання персоналу, створення внутрішніх кодексів етики, призначення відповідальних офіцерів з питань захисту даних, а також ініціюють незалежні аудити безпеки. Такі дії сприяють формуванню зрілої корпоративної культури відповідального використання даних, про що свідчать численні кейси впровадження BI-рішень у транснаціональних корпораціях, задокументовані в звітах Deloitte, PwC [14] та KPMG [15].

На шляху становлення правового поля для BI постає й питання балансу між захистом споживачів, гарантуванням конфіденційності, інноваційністю та ефективною конкуренцією. У ЄС ухвалюються акти на кшталт Digital Markets Act [16] та Digital Services Act [17], спрямовані на прозорість алгоритмічних процесів, недопущення дискримінації та монопольних зловживань. Подібні тенденції відображені й у працях Ш. Зубофф, яка у книзі "The Age of Surveillance Capitalism" аналізує вплив масового збору даних, алгоритмічного прогнозування поведінки та монетизації приватності на суспільство, права людини та економіку [18].

Формування правового поля для BI – складний та багатовимірний процес, що відбувається на перетині інформаційного, інтелектуального, корпоративного, податкового та антимонопольного права. Успішна інтеграція правових норм, етичних стандартів та передових технічних рішень у BI-процеси дозволить знизити

Таблиця 1

Оцінки глобального ринку бізнес-розвідки за 2019–2027 роки

Рік/період	Джерело та назва звіту	Оцінка глобального ринку BI	Примітки
2019	Fortune Business Insights, "Business Intelligence Market Size, Share & COVID-19 Impact Analysis" (2020)	~22,26 млрд дол. США	Дані до пандемії, базовий рік оцінювання
2020	MarketsandMarkets, "Business Intelligence Market" (2020)	~23,1 млрд дол. США	Вплив віддаленої роботи та хмарних рішень
2021	Mordor Intelligence, "Business Intelligence Market – Growth, Trends, COVID-19 Impact, and Forecasts (2021–2026)"	~24 млрд дол. США	Стійке зростання через цифрову трансформацію
2025	MarketsandMarkets (2020)	~33,3 млрд дол. США	Прогнозований середньорічний приріст близько 7,6%
2027	Fortune Business Insights (2020)	~39,35 млрд дол. США	Прогнозований середньорічний приріст близько 8,1%

Джерело: складено за даними [10; 11]

юридичні, репутаційні та фінансові ризики, сприяти інноваціям, забезпечуючи сталий розвиток цифрового бізнес-середовища. Аналітичні центри, університети та міжнародні організації продовжують генерувати нові знання, розробляючи засади для гармонійної взаємодії між ринками, суспільством, наукою та правом.

Успішне функціонування бізнес-розвідки у цифровому середовищі значною мірою залежить від комплексного правового, організаційного та технологічного підходу. На основі проведеного аналізу можна сформулювати низку рекомендацій, спрямованих на підвищення ефективності, безпечності та прозорості ВІ-систем, а також на забезпечення дотримання правових норм і стандартів етики. Рекомендації наведено в таблиці 2.

Загалом окреслені рекомендації вказують на нагальну потребу у комплексному підході до регулювання систем бізнес-розвідки. Ключовими завданнями постають гармонізація національних норм з міжнародними стандартами, визначення прозорих умов використання даних, впровадження етичних кодексів та посилення відповідальності за порушення правових норм. Це доповнюється посиленою увагою до кібербезпеки, формуванням правових рамок для застосування штучного інтелекту та стимулюванням міжнародної взаємодії та обміну передовим досвідом. Такий підхід забезпечить стійкість, довіру та безпеку в цифровому середовищі.

Висновки. Цифрова трансформація підприємств і поширення технологій бізнес-розвідки створюють

Таблиця 2

Рекомендації підвищення ефективності, безпечності та прозорості ВІ-систем

Напрямок	Методи	Опис
Удосконалення правового регулювання в національному та міжнародному контексті.	Гармонізація законодавства:	Необхідно забезпечити узгодження національних нормативно-правових актів зі світовими стандартами та директивами. Зокрема, важливо адаптувати локальне законодавство у сфері захисту персональних даних до вимог міжнародних документів (наприклад, GDPR) та створити правові бази, що враховують специфіку використання штучного інтелекту й алгоритмічних рішень
	Розробка прозорих ліцензійних умов для даних	Створення чітких інструкцій, які визначають умови використання відкритих даних, захищеної інформації, а також алгоритмічно згенерованих результатів дозволить знизити ризики правових колізій та сприятиме інноваційному розвитку
	Посилення відповідальності за порушення правил обробки інформації	Запровадження послідовної системи санкцій за незаконне використання або поширення конфіденційних даних стане важливим стимулом для суб'єктів господарювання дотримуватися встановлених норм
Впровадження етичних стандартів та саморегуляційних механізмів	Розробка етичних кодексів для аналітиків і фахівців з ВІ	Створення галузевих кодексів етики, що регламентують межі допустимого використання даних, особливо коли йдеться про персональні чи чутливі бізнес-дані, сприятиме підвищенню репутаційного капіталу організацій
	Інституціоналізація внутрішнього контролю	Призначення корпоративних омбудсменів з питань інформаційної безпеки та етики, а також впровадження незалежних аудиторських механізмів оцінки алгоритмічних процесів дозволять забезпечити прозорість та підзвітність
Зміцнення кібербезпеки та забезпечення конфіденційності.	Технічні стандарти безпеки	Визначення мінімальних вимог щодо шифрування, автентифікації, моніторингу та управління доступом до даних знизить вразливості систем ВІ до кібератак, несанкціонованого доступу та витоків інформації
	Інвестиції в кіберграмотність	Підвищення освітнього рівня персоналу та користувачів щодо методів захисту даних і безпечної поведінки в цифровому просторі матиме позитивний довгостроковий ефект. Інтеграція нових технологій та аналітичних інструментів
Інтеграція нових технологій та аналітичних інструментів.	Нормативна база для використання AI та ML	Розробка регламентів, які окреслюють межі використання штучного інтелекту для аналізу даних, допоможе мінімізувати ризики дискримінації, «чорних скриньок» та зловживань інсайдерською інформацією
	Стандартизація форматів даних	Уніфікація підходів до структурування і метаданих підвищить сумісність ВІ-платформ, полегшить обмін інформацією та її правомірне використання
Міжнародна координація та міжгалузева взаємодія	Створення транскордонних регуляторних платформ	Формування міжнародних робочих груп, які об'єднують юристів, технічних експертів, представників бізнесу та громадських організацій, сприятиме розробці глобальних стандартів і рекомендацій
	Популяризація «кращих практик»	Обмін досвідом та знаннями щодо ефективних підходів у сфері бізнес-розвідки дозволить швидше масштабувати інновації та посилить довіру між ринковими акторами

Джерело: складено за даними [10–12; 14; 15; 19]

багаторівневу екосистему, в якій аналітичні інструменти тісно переплітаються з правовими й етичними викликами. Ця екосистема динамічно реагує на нові можливості та загрози, пов'язані з інтенсивним використанням даних, штучного інтелекту та автоматизованих систем прийняття рішень. У таких умовах рівновага між потребою в інноваціях та необхідністю захисту прав суб'єктів цифрового ринку, конфіденційності та інтелектуальної власності набуває ключового значення.

Проведений аналіз свідчить про нагальну потребу гармонізації правових норм, впровадження етичних стандартів, вдосконалення внутрішньокорпоративних політик і процедур контролю. Без належних правових рамок бізнес-розвідка може стати джерелом ризиків:

від юридичних суперечок і санкцій до значних репутаційних втрат. З іншого боку, чітка правова база, доповнена технічними стандартами безпеки, етичними принципами використання даних та ефективними механізмами саморегуляції, створить фундамент для сталого розвитку ВІ-практик.

Врешті-решт, цілісний, багатовимірний підхід до регулювання бізнес-розвідки в цифровому середовищі забезпечить оптимальні умови для інноваційного зростання, підвищення конкурентоспроможності й посилення довіри між усіма учасниками цифрового ринку. Це, у свою чергу, сприятиме формуванню більш стабільної, прозорої та передбачуваної бізнес-екосистеми, здатної генерувати цінність для суспільства, економіки та державних інституцій у довгостроковій перспективі.

Список використаних джерел:

1. Усов Д. С. Конкурентна розвідка як інструмент формування стратегії компанії. *Регіональні студії*, 2024. № 32. С. 48–52.
2. Mayer-Schönberger V., Padova Y. Regime Change? Enabling Big Data through Europe's New Data Protection Regulation. *Science and Technology Law Review*, 2016. № 17(2). С. 315–335.
3. Solove D. J. The limitations of privacy rights. *Notre Dame L. Rev.* 2022. № 98. С. 975.
4. Varian H. R. Beyond big data. *Business Economics*, 2014. № 49(1). С. 27–31.
5. Acquisti, Alessandro; Taylor, Curtis; Wagman, Liad. The economics of privacy. *Journal of Economic Literature*, 2016. № 54(2). С. 442–492.
6. Дикань В. Л., Куркін М. В. Роль конкурентної розвідки у боротьбі із недружніми поглинаннями в Україні. *Вісник економіки транспорту і промисловості*, 2009. № 28. С. 28–32.
7. Ronald S. R. National Institute of Standards and Technology. Special Publication 1500-4: Guide for Conducting Risk Assessments. 2013. 95 p. URL: <https://www.nist.gov/publications/guide-conducting-risk-assessments>
8. Otto M. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation–GDPR). *International and European Labour Law. Nomos Verlagsgesellschaft mbH & Co. KG*, 2018. PP. 958–981.
9. Harry L. Size, Hydrogen Peroxide Market. Share & COVID-19 Impact Analysis, 2021. *Fortune Business Insights*, 2020. URL: <https://solutions.trustradius.com/vendor-blog/business-intelligence-statistics-and-trends/>
10. Business Intelligence Market – Global Growth Trends, COVID-19 Impact and Forecasts 2021–2026. *MarketsandMarkets*, 2024. URL: <https://www.marketsandmarkets.com/PressReleases/social-business-intelligence-bi.asp>
11. Content Intelligence Market – Global Growth Trends, COVID-19 Impact and Forecasts 2021–2026. *ResearchAndMarkets.com*, 2024. URL: <https://www.businesswire.com/news/home/20210422005513/en/Content-Intelligence-Market---Global-Growth-Trends-COVID-19-Impact-and-Forecasts-2021-2026---ResearchAndMarkets.com>
12. Riek L. D., et al. The Emerging Policy and Ethics of Human Robot Interaction. *HRI (Extended Abstracts)*, 2015. С. 247–248.
13. Носок С. О.; Фаль, О. М.; Ткач, В. М. Управління інформаційною безпекою. Конспект лекцій: навчальний посібник для студентів спеціальності 125 «Кибербезпека». КПІ ім. Ігоря Сікорського, 2021. 258 с.
14. Cybersecurity and Data Protection. *PwC*. URL: <https://www.pwc.com/gx/en/services/legal-business-solutions/cybersecurity-and-data-protection.html>
15. Culture and Conduct Assurance Framework. *KPMG*. URL: <https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2020/01/kpmg-s-culture-and-conduct-assurance-framework.pdf>
16. Digital Markets Act: Ensuring Fair and Open Digital Markets. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
17. Digital Services Act. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (дата звернення: 10.12.2024).
18. Zuboff S. The Age of Surveillance Capitalism. *Social Theory Re-wired. Routledge*, 2023. С. 203–213.
19. Мірошниченко О., Боденчук П., Григор'єва Ю. Оптимізація операційної діяльності підприємств через застосування систем business intelligence. *Підприємство та інновації*, 2024. №31. С. 43–48. DOI: <https://doi.org/10.32782/2415-3583/31.7>

References:

1. Usov D. C. (2024) Konkurentna rozvidka yak instrument formuvannya strategiyi kompaniyi [Competitive intelligence as a tool for company strategy formation]. *Rehionalni studii – Regional Studies*, no. 32, pp. 48–52. (in Ukrainian)
2. Mayer-Schönberger V., Padova Y. (2016) Regime Change? Enabling Big Data through Europe's New Data Protection Regulation. *Science and Technology Law Review*, vol. 17(2), pp. 315–335.
3. Solove D. J. (2022) The limitations of privacy rights. *Notre Dame L. Rev.*, vol. 98, pp. 975.
4. Varian H. R. (2014) Beyond big data. *Business Economics*, vol. 49(1), pp. 27–31.
5. Acquisti A., Taylor C., Wagman L. (2016) The economics of privacy. *Journal of Economic Literature*, vol. 54(2), pp. 442–492.
6. Dikan V. L., Kurkin M. V. (2009) Rol konkurentnoyi rozvidky u borotbi iz nedruzhnim poglynannamy v Ukraini [The role of competitive intelligence in countering hostile takeovers in Ukraine]. *Visnyk ekonomiky transportu i promyslovosti – Bulletin of Transport and Industry Economics*, no. 28, pp. 28–32. (in Ukrainian)

7. Ronald S. R. (2013) National Institute of Standards and Technology. Special Publication 1500-4: Guide for Conducting Risk Assessments. Available at: <https://www.nist.gov/publications/guide-conducting-risk-assessments>
8. Otto M. (2018) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation–GDPR). International and European Labour Law, Nomos Verlagsgesellschaft mbH & Co. KG, pp. 958–981.
9. Harry L. (2020) Size, Hydrogen Peroxide Market. Share & COVID-19 Impact Analysis, 2021. Fortune Business Insights. Available at: <https://solutions.trustradius.com/vendor-blog/business-intelligence-statistics-and-trends/>
10. Business Intelligence Market – Global Growth Trends, COVID-19 Impact and Forecasts 2021–2026. (2024) MarketsandMarkets. Available at: <https://www.marketsandmarkets.com/PressReleases/social-business-intelligence-bi.asp>
11. Content Intelligence Market – Global Growth Trends, COVID-19 Impact and Forecasts 2021–2026. (2024) ResearchAndMarkets.com. Available at: <https://www.businesswire.com/news/home/20210422005513/en/Content-Intelligence-Market---Global-Growth-Trends-COVID-19-Impact-and-Forecasts-2021-2026---ResearchAndMarkets.com>
12. Riek L. D., et al. (2015) The Emerging Policy and Ethics of Human Robot Interaction. HRI (Extended Abstracts), pp. 247–248.
13. Nosok S. O.; Fal, O. M.; Tkach, V. M. (2021) Upravlinnya informatsiynoyu bezpekoyu [Management of information security]: konspekt leksii. KPI im. Ihorya Sikorskoho, 258 p. (in Ukrainian)
14. Cybersecurity and Data Protection. PwC. Available at: <https://www.pwc.com/gx/en/services/legal-business-solutions/cybersecurity-and-data-protection.html>
15. Culture and Conduct Assurance Framework. KPMG. Available at: <https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2020/01/kpmg-s-culture-and-conduct-assurance-framework.pdf>
16. Digital Markets Act: Ensuring Fair and Open Digital Markets. European Commission. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
17. Digital Services Act. European Commission. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
18. Zuboff S. (2023) The Age of Surveillance Capitalism. Social Theory Re-wired. Routledge, pp. 203–213.
19. Miroshnichenko O., Bodenchuk P., Grigoryev Y. (2024) Optymizatsiya operatsiynoyi diyalnosti pidpryyemstv cherez zastosuvannya system business intelligence [Optimization of enterprise operational activities through the application of business intelligence systems]. *Pidpryyemnytstvo ta innovatsiyi – Entrepreneurship and Innovation*, no. 31, pp. 43–48. DOI: <https://doi.org/10.32782/2415-3583/31.7> (in Ukrainian)