УДК 338.1: 303.71

Н. Ю. Вакшинська [1], О. Є. Шандрівська [2]
ORCID [2]0000– 0002– 4335– 2423
Національний університет "Львівська політехніка"

СПЕЦИФІКА РОЗВИТКУ РИНКУ BIG DATA ДЛЯ ПОТРЕБ ВІДНОВЛЕННЯ ЕКОНОМІКИ УКРАЇНИ В ПОСТВОЄННИЙ ПЕРІОД

https://doi.org/

Досліджено особливості та перспективи розвитку світового ринку Big Data до та під час війни. Ідентифіковано джерела витоку даних на ринку Big Data, виявлено вплив міжнародних інституцій на протидію кібератакам в умовах збурень. Сформовано напрями адаптації українського кіберпростору до функціонування в умовах війни, розроблено рекомендації щодо напрямів імплементації технологій Big Data після війни для забезпечення економічного зростання на прикладі воєнно-промислового комплексу. Проведено SWOT – аналіз ринку Big Data в частині оцінювання сили та слабкостей воєнно-промислового комплексу під впливом чинників зовнішнього середовища. Узагальнені результати дослідження специфіки функціонування та перспектив розвитку ринку Big Data рекомендовано для застосування представниками *Мінцифри* та Комітету цифрової трансформації України, Міністерства економічного розвитку і торгівлі України, а також керівникам інформаційних відділів/ відділів захисту персональних даних підприємств різних галузей економіки

Ключові слова: Big Data, персоналізовані дані, війна, кібератаки, SWOT-аналіз, воєнно-промисловий комплекс, національне господарство.

Постановка проблеми

Умови, в яких функціонує економіка України, відзначаються різкими деструктивними змінами, що призводять до появи нових викликів та проблем. Українська економіка зазнала впливу активних бойових дій та поширення пандемії COVID-19, що призвело у 2022 р. до падіння ВВП на 30,2 %, зростання кількості безробітних до 2,9 млн. осіб, зростання індексу інфляції до 126,6 % тощо [9].

Ці деструктивні наслідки можуть бути пом'якшені за допомогою технологій Big Data, які можуть стати корисним інструментом для урядових організацій та підприємств в Україні за для адаптації до сучасних реалій. Дослідження ринку Big Data допоможе знайти рішення, які враховуватимуть технологічні можливості та деструктивні впливи макроекономічного та геополітичного середовища.

Формулювання мети та завдань статті

Метою роботи є дослідження стану та перспектив розвитку ринку Big Data на світовому рівні та на рівні економіки України під час воєнних дій; розробка рекомендацій щодо економічних напрямів впровадження захисту персональних даних в умовах дії деструктивних чинників.

За для досягнення поставленої мети були сформовані та вирішені такі науково-методичні й практичні завдання:

-досліджено світову динаміку та тенденції розвитку ринку Big Data та проведена подальша структуризація ринку Big Data за ознаками типів та кількості даних, які створюються суб'єктами господарювання на досліджуваному ринку;

- ідентифіковано та проаналізовано хронологію кібератак України до та під час активної фази війни, що дозволило ідентифікувати ризики та небезпеки галузі Big Data;

- виявлено специфіку кон'юнктури українського ринку Big Data під час війни, що дозволило сформувати рекомендації щодо імплементації напрямів захисту персональних даних на різних ієрархічних рівнях.

Авторами висунуто гіпотезу щодо значних деструктивних впливів на економіку України у часі гібридної агресії з 2014 року та в період повномасштабної війни з 2022 року, що вимагає нагального реагування на деструктивні явища, домінантно учасниками ринку Big Data. Найбільшою загрозою на даному ринку постають кібератаки, які завдає РФ з метою витоку даних та маніпулювання ними для отримання неправомірних вигод та створення загального інформаційно-психологічного хаосу.

У роботі застосовані такі методи дослідження: статистичний, методи порівняльного аналізу та узагальнення - для ідентифікації особливостей розвитку ринку Big Data в умовах активізації деструктивного інформаційного впливу з боку РФ під час війни. SWOT – аналіз для ідентифікації внутрішніх та зовнішніх впливів на галузь Big Data у воєнно-промисловому комплексі в умовах війни.

Аналіз останніх досліджень і публікацій

В умовах глобалізації бізнесу та з огляду на широкий спектр деструктивних впливів активно досліджується ринок Big Data у зарубіжній та вітчизняній науковій літературі. Зокрема, у дослідженнях [9] Х. Сінгх описує напрями впливу Big Data у галузі охорони здоров'я, що сприяє застосуванням результатів його досліджень з метою підвищення точності отриманих діагнозів.

Джастін Лонго у роботі [20] досліджує реальні виклики та можливості, пов'язані з обробкою великих обсягів даних в сучасному глобалізованому світі. У роботі [16] К. Кук'єр описує проблематику та перспективи розвитку галузі Big Data в сучасних умовах господарювання.

Серед вітчизняних досліджень слід виділити наукові роботи, де розглядаються проблеми захисту персональних даних в Україні, зокрема, щодо порушення правил збору та зберігання даних, а також використання даних без згоди власника. Також обговорюється можливості шляхи вирішення цих проблем та перспективи розвитку ринку персональних даних в Україні.

Дослідження чинників впливу на динаміку розвитку ринку Big Data відображається у публікаціях аналітичних компаній, серед яких слід зазначити Gartner [18] та Statista [27].

Виклад основного матеріалу дослідження

Ринок Big Data є одним з найбільш динамічних ринків у світовій цифровій економіці. Розвиток цифрової економіки сприяє збільшенню кількості підприємств, які збирають та аналізують персональні дані користувачів, а також з'являються нові технології, які дозволяють обробляти та аналізувати великі обсяги даних.

Відомо, що персональні дані збираються як комерційними, так і некомерційними організаціями. Домінантно, компанії, які працюють у сфері високих технологій, є основними збирачами даних, аби забезпечити надання широкого асортименту послуг своїм користувачам та отримання доходу за рахунок надання персоналізованої реклами. Технологія Big Data застосовується в різних галузях, таких як медицина, фінанси, транспорт, енергетика, телекомунікації та багато інших. Ці технології забезпечують зручний та ефективний доступ до великих обсягів даних на різних ієрархічних рівнях, що дозволяє приймати більш точні рішення та підвищувати ефективність бізнесу.

Розвиток ринку Big Data несе за собою певну низку загроз, найбільш поширеною з яких є кібершпигунство. У сучасному світі кібершпигунство набуло гострої актуальності, оскільки дає змогу збирати великі обсяги інформації віртуально без ризику бути ідентифікованим. Слід зазначити один з найбільш відомих прикладів кібершпигунства, яким є діяльність спецслужб РФ в Інтернеті: російська влада використовує кібершпигунство для збирання інформації про діяльність урядових та неурядових організацій, застосовує інформаційні кібератаки з метою впливу на виборчі процеси в інших країнах, здійснює викрадення інноваційних технологій виробничих підприємств, маніпулює даними у різних країнах, зокрема в Україні та США.

Незважаючи на загрози, щоденно світ створює величезну кількість даних. Великі обсяги даних утворюються завдяки розвитку сенсорних технологій, мереж Інтернету та мобільних пристроїв, що приводить до створення великої кількості структурованих і неструктурованих даних, які необхідно обробляти та аналізувати. Це можливо завдяки застосуванню спеціальних технологій та алгоритмів машинного навчання, що дозволяють автоматизувати та прискорювати аналіз даних. Як свідчить статистика, місткість світового ринку Dig Data зростає протягом 2018 - 2022 рр. (табл. 1).

Таблиця 1

Аналіз динаміки місткості світового ринку Big Data за період 2018 – 2023 рр.

Рік	2018	2019	2020	2021	2022	2023 (прогноз)	2023/ 2018
Місткість ринку Big Data, млрд. дол. США	42	49	56	64	70	77	1,83

Джерело: структуровано на основі [25; 27]

Глобальний ринок великих даних, згідно із даними Statista, зросте до першого кварталу 2027 р. до позначки у 103 млрд. дол. США., що понад двічі перевищує потенційну місткість ринку Big Data у 2018 р. [27]. Дана статистика вказує на різкий та неперервний зріст кількості даних у Інтернеті та їх вартості. Зауважимо, що цей зріст впродовж 2018 – 2022 рр. відбувся на 54,5 %.

За даними Forbes, у 2018 році увесь світ виробив близько 2,5 екзабайт (2,5 млрд. гігабайт) даних шляхом створення персоніфікованих даних від пристроїв Інтернету речей (IoT), сенсорів, соціальних мереж, веб-сайтів, електронної пошти та інших джерел інформації [22].

Кількість персоналізованих інформаційних даних щороку зростає, оскільки кінцеві споживачі та підприємства продовжують створювати нові масиви даних в Інтернет – просторі. За прогнозами Statista, протягом 2020-2025 рр. обсяг глобальних даних зросте до понад 180 зетабайт. У 2020 році кількість створених і відтворених інформаційних даних досягла нового максимуму. Зростання було вищим, ніж очікувалося раніше, через запровадження дистанційного типу роботи та навчання вдома внаслідок пандемії [29].

Відомо, шо кожна трансакція чи взаємодія в Інтернеті створює інформаційний слід. Так, у 2021 р. 3,7 млрд. чол. щодня здійснювали близько 5,6 млрд. пошукових запитів, і це лише за пошуками в Google. Найбільша пошукова система Google обробляє понад 63000 пошукових запитів щосекунди. Відповідно до звітів, в середньому щохвилини в Твіттері оопубліковується 456000 твітів, в Instagram створюється 46740 зображень, а на YouTube переглядається 4146600 відео. Щохвилини надсилається 156 мільйонів електронних листів та створюється 103447520 спам-повідомлень [29].

Зростаючий сплеск застосування інформаційних персоніфікованих даних зумовлений не лише тим, що все більше технологій використовується в процесі цифровізації, але й зростанням кількості вбудованих пристроїв. Зокрема, серед вбудованих пристроїв розрізняють фітнес трекери, аудіо системи, камери спостереження, електронні книжки і т. д.

Отже, за підсумками 2021 р., людство створило близько 59 зеттабайт (59 трлн гігабайт), за період 2018 - 2021 рр. цей показник у світі зріс на 61 % [19].

Засвідчено широке коло варіантів успішних випадків використання Big Data серед компаній. Зокрема, Netflix є прикладом того, наскільки потужним може бути використання Big Data. Медіакомпанія повідомляє, що її алгоритм рекомендацій впливає на близько 80 % усього контенту, який переглядається на платформі, що формує утримання та заощадження близько 1 млрд. дол. США [5].

Big Data приносить велику користь компаніям, модернізує та покращує такі процеси, як дослідження ринку та його окремих складових, оптимізація виробництва, покращення клієнтського сервісу, попередження шахрайства та крадіжок, удосконалення маркетингу, розробка нових послуг та продуктів, які сприяють комплементарному розвитку суміжних та дотичних галузей, сумарно дають поштовх розвитку економіці окремої країни [3]. Попри усі переваги Big Data, ця галузь пов'язана з різними ризиками та небезпеками, а саме:

- безпекою даних. Збір, збереження та обробка великих обсягів даних можуть створити загрозу для безпеки даних на різних ієрархічних рівнях: особистості, підприємства чи організації, окремих галузей економіки, громадянського суспільства та держави в цілому. Тому вкрай важливо забезпечити надійний захист інформаційних даних від несанкціонованого доступу та зламів систем безпеки;
- недостатня якість даних. У великих обсягах даних можуть бути помилки та неточності, що можуть призвести до невірних результатів аналізу та необґрунтованих висновків;
- питання етики. Великі обсяги даних можуть містити особисту інформацію, яка повинна бути захищена від несанкціонованого використання та зловживань. Крім того, використання персоніфікованих даних може піднімати питання етики та приватності;
- залежність від технологій. Стверджується, що великі обсяги інформаційних даних вимагають спеціальних технологій та відповідної інфраструктури для їх обробки та аналізу. Залежність від цих технологій може створювати додаткові ризики, які пов'язані з невідповідністю технологій, технічними несправностями, відмовою системи та іншими проблемами техніко-технологічного забезпечення;
- високі витрати. Робота з великими обсягами даних може вимагати значних фінансових витрат та витрат часу на створення інфраструктури (домінантно), технології, персонал та інші ресурси.

З огляду на поширення глобалізації та цифровізації бізнесу у світі загострюється проблема відсутності приватності та безпеки у Інтернеті, з огляду на появу нових технологій та способів крадіжки персональних даних. У сучасному цифровому світі кіберзлочинці можуть красти різноманітні дані з комп'ютерів та інших електронних пристроїв. Однак, деякі типи даних є більш привабливими для крадіжок, оскільки мають більший потенціал для зловживання. Найпоширенішими типами даних, які злочинці можуть красти, згідно експертних думок та за результатами досліджень авторів можуть бути такі.

1. Кредитні картки. Кредитні картки містять особисту інформацію про власника, зокрема, такі дані як ім'я, адреса, номер картки та код безпеки. Крадіжка цих даних може призвести до зловживань карткою та збитків для власника.

2. Персоніфіковані дані. Це можуть бути імена, адреси, номери телефонів, адреси електронної пошти та інші дані, що використовуються для ідентифікації особи. Крадіжка таких даних може призвести до шахрайства та ідентифікаційної крадіжки.

3. Медичні дані. Медичні дані містять приватну інформацію про стан здоров'я та історію лікування особи. Ці дані можуть використовуватися злочинцями для здійснення медичної крадіжки та випадкових терапевтичних процедур.

4. Банківські дані. Банківські дані містять інформацію про банківські рахунки та транзакції. Крадіжка таких даних може призвести до шахрайства та фінансової крадіжки.

5. Комерційна та конкурентна інформація. Це можуть бути торгові та бізнес-секрети, такі як патенти, розробки, технології, плани маркетингу тощо. Крадіжка таких даних може призвести до загострення конкуренції та втрати конкурентної переваги.

Динаміку кількості офіційно поданих скарг, пов'язаних з крадіжкою даних наведено у табл. 2.

Таблиця 2

Аналіз динаміки кількості скарг на крадіжки даних у США, 2018 – 2022 рр.

	Роки					2022/ 2018
Види скарг	2018	2019	2020	2021	2022	
Скарги про крадіжку особистих даних	444338	650523	1388539	1434693	1108609	2,49
Інши скарги	1203425	982142	1318247	1633677	1694993	1,41
Скарги компаній	1523295	1893941	2365362	2923941	2369527	1.56
Разом	3171058	3526606	5072148	5992311	5173129	3,9

Джерело: структуровано на основі [10]

Згідно з табл. 2, найбільшою категорією скарг є крадіжки даних та кібершахрайство на промисловому рівні, тобто ті випадки, коли дані викрадені або маніпульовані у межах компаній. У 2021 році спостерігається найбільше зростання цього показника, що пов'язано зі зростанням кількості працівників, які працюють здалеку, у зв'язку з пандемією COVID-19. Більша кількість даних стала доступною для крадіжок, оскільки більше інформації перейшло в цифровий простір. Загальний відсоток скарг з 2018 по 2022 рік збільшився на 61,2%. На таблиці2. можна побачити взаємозв'язок між кількістю створених та викрадених даних за цей період. У 2022 році у США було зафіксовано 1802 випадки витоку даних, а більше 422 млн. людей стали жертвами компрометації даних, включаючи виток та неправомірний доступ до даних [10].

Одним з найбільш популярних типів кібератак є програма - вимагач (ransomware). Програма-вимагач – це тип шкідливої програми, який злочинці встановлюють на комп'ютерах споживачів з метою їх блокування. Відновлення доступу вимагає грошової компенсації [30]. Злочинні групи програм-вимагачів здебільшого націлені на розвинені країни, щоб максимізувати прибутки. Країни, які найчастіше атакуються злочинними організаціями наведено на табл. 3.

Таблиця 3

Структура країн, які найчастіше атакуються групою програм-вимагачів

Місце	Країна	Кількість атак групою програм-вимагачів, %
1	США	51
2	Великобританія	10
3	Канада	5
4	Франція	3
5	Австралія	3
6	Японія	2.5
7	Бразилія	2
8	Німеччина	2
9	Решта світу	21,5
	Разом	100,0

Джерело: структуровано на основі [17;14-15]

Станом на 2021 р. США залишаються головною країною атак програм - вимагачів у світі, на які припадає понад 51 % інцидентів. Другою країною за масштабами кібератак є Великобританія, на яку припадає 10 % кіберзлочинів. Трійку лідерів країн, які атакують програми – вимагачі замикає Канада. На неї припадає 5 % кібератак до загалу. Найчастіше такі кібератаки здійснюються на такі сфери: юридичні, фінансові, охорона здоров'я та людські ресурси.

Отже, крадіжки мають вагомий деструктивний вплив на компанії, організації та індивідуальних користувачів, включаючи фінансові збитки, репутаційні збитки, правові наслідки, втрата конкурентоспроможності, зниження іміджу країни тощо [13].

В Україні галузь Big Data нова, але існують успішні випадки використання Big Data у веденні бізнесу, зокрема у фінансовому секторі.

Ще одним методом застосування є Мінцифри для аналізу даних з метою контролю кінцевих споживачів, які прибували з-за кордону, щоб відслідковувати дотримуванням ними режиму самоізоляції в період карантину. Частка підприємств, які виконують аналіз великих даних, в Україні у 2018 - 2020 рр. подано на табл. 4.

Таблиця 4

Аналіз динаміки частки підприємств, які виконують аналіз Big Data в Україні, 2018-2020 рр.

Рік	2018	2019	2020	2020/ 2018
Частка компаній, %	12,5	11,9	12,7	1,016

Джерело: структуровано на основі [24]

Аналіз табл. 4 свідчить, що частка підприємств, які використовували аналіз великих даних в Україні у 2020 році становить 12,7 %, що є найбільшим показником за період 2018 - 2020 рр. У 2019 р. ця частка знизилася до 11,9 %, тобто в України на цей період немає стрімкого зросту застосування технологій Big Data серед підприємств, проте частка цих підприємств є стабільною.

Вплив гібридної агресії з боку РФ засвідчив, домінантно з 2014 року, що урядові організації в Україні та її сайти зазнають кібератак. Серед масованих кібератак, які відбулися до 24 лютого 2022 року, слід виділити:

- 27 червня 2017 року відбулася кібератака на державні установи, об'єкти фінансового, енергетичного та транспортного сектору, а також приватні підприємства, за допомогою шкідливого програмного продукту Petya-A, який паралізує комп'ютерні системи. Цей вірус-блокувальник шифрує дані на комп'ютері та вимагає викуп. Засвідчено та доведено причетність спецслужб РФ до цієї кібератаки [10];
- протягом вересня 2020 року компанія "Нафтогаз України" щодня стикнулася з близько 800 кібератаками в кіберпросторі, які їй вдалося зупинити [1];
- станом на серпень 2021 р. СБУ перешкодила 43 кібератакам на інформаційні системи органів державної влади. Також було виявлено понад 36 тисяч потенційних кіберінцидентів. Найбільш поширеними типами виявлених кіберзагроз були: підключення до командно-контрольних серверів, намагання отримати несанкціонований доступ до інформаційних сайтів підприємств, атаки на вебдодатки та шкідливе програмне забезпечення. Співробітники СБУ встановили причетність спецслужб РФ до здійснення цих кібератак [12];
- станом на 13-14 січня 2022 року відбулася хакерська атака на кілька урядових веб-сайтів, включаючи Міністерство закордонних справ, Міністерство освіти і науки України, Державну службу з надзвичайних ситуацій та інші. Була доведена причетність спецслужб РФ. На цих веб-сайтах були розміщені провокаційні повідомлення. Більшість пошкоджених державних ресурсів було відновлено. За даними Держспецзв'язку, за час цих злочинів постраждали близько 70 сайтів центральних і регіональних органів влади [12];

- станом на 15 лютого 2022 р. була здійснена DDoS-атака на урядові сайти Міністерства оборони та Збройних сил України, а також банківський сектор веб-сервісів державних Банку АТ «Ощадбанку» і Банку АТ «ПриватБанку». DDOS-атака на державні ресурси України була виключно інформаційно-психологічною, жодних втрат не виявлено [2];
- 27 червня 2017 року відбулася кібератака на державні установи, об'єкти фінансового, енергетичного та транспортного сектору, а також приватні підприємства, за допомогою шкідливого програмного продукту Petya-A, який паралізував комп'ютерні системи. Відомо, що цей вірус-блокувальник шифрує дані на комп'ютері та вимагає викуп. За цією кібератакою була доведена причетність спецслужб РФ [10].

За період 2017 - 2022 рр. доведено причетність спецслужб РФ до даних кібератак. Ці атаки мали фокус на урядові органи влади України для шантажу та створення інформаційного хаосу. Дані кібератаки мали глобальні наслідки щодо безпеки та ефективності роботи економічного сектору України, вплинули на зниження ВВП України та принесли збитки окремим підприємствам енергетичного сектору та іншим підприємствам критичної інфраструктури України. .

У час повномасштабної війни число кібератак збільшилося на 50 %, щодо галузей економіки, то це число в середньому становить до 605 разів на день. Найчастіше цілями атак є державний, фінансовий та медіа сектори – близько 2600 атак кожного дня, що у 2022 році склало на 44 % більше, ніж у 2021 році [7].

За час з 24 лютого 2022 р. по початок січня 2023 р. здійснено близько 4500 кібератак з боку РФ, середньодобово зроблено 10 кібернападів [8]. Найчастіше ці кіберзлочини сфокусовано на критичну інфраструктуру, виявлено узгодженість у часі між ракетними ударами та кібератаками ворога. Наприклад, 1 березня 2022 року ракетний удар по київській телевежі призвів до зупинки телевізійного мовлення, паралельно з ракетним ударом здійснювалася кібератака на Концерн радіомовлення, радіозв'язку і телебачення. Такий сценарій застосовується також при ракетних ударах на українські об'єкти енергетики, які супроводжуються кібератаками. Росія планує використовувати витоки даних для шпіонажу, маніпуляцій та створення загального інформаційно-психологічного хаосу. Ці дії спецслужб РФ суперечать міжнародним правилам у кіберпросторі щодо України.

У 2015 році Генеральна Асамблея ООН прийняла резолюцію 70/237, яка закликає держави розробляти та застосовувати міжнародні закони, стандарти та норми для протидії кіберзагрозам, включаючи кіберзлочинність та кібертероризм. РФ, яка прийнята до Організації Об'єднаних Націй у 1945 році, офіційно підтримує але не виконує цю резолюцію.

Виявлено такі основоположні принципи, в переліку резолюції 70/237, які мають такі вимоги щодо держав:

- дотримування міжнародного права, а саме універсально визнаних принципів і норм поведінки в кіберпросторі;
- захист критичної інфраструктури від кібератак на енергетичні мережі, транспортні системи та фінансові установи;
- співпраця в досудовому розслідуванні та притягнення до відповідальності кіберзлочинців та кібертерористів;
- співпраця в обміні інформацією та взаємодопомога в захисті від кіберзагроз [5; 11].

Тож, окрім територіальної агресії та активних воєнних дій, РФ веде наступ в кіберпросторі. Рекомендовано Раді безпеки ООН притягнути до міжнародної відповідальності РФ за здійснення кібератак на критичні об'єкти України через те, шо РФ розглядає та використовує кібератаки як політичний інструмент впливу та тиску на суверенітет України.

Попри спроби РФ дестабілізувати кіберпростір України, жодна з даних спроб не була успішною. Значний досвід схожих злочинів надав Україні можливість бути підготовленій до таких маніпуляцій. Крім того, після спроб у 2017 році задіяно інвестиції у розмірі 265 млрд. дол. США [6] для

убезпечення кіберпростору нашої держави. Після 24 лютого 2022 р. була створена «ІТ армія», яка складається близько з 175 тис. добровольців.

Ефективне технологій застосування Big Data показує покращення функціонування не лише економіки України, але військово - промислового комплексу, надто, в умовах війни. Використаємо такий інструментарій дослідження, як SWOT - аналіз для визначення сильних та слабких сторін розвитку та можливостей і загроз застосування технологій Big Data у воєнний період.

Сильні сторони. Дані, зібрані від сенсорів, аналізів соціальних мереж, зображень з дронів та інших джерел, можуть допомогти представникам воєнно-промислового комплексу зібрати інформацію про противника, його стратегії, розміщення військ, зброю та інші фактори. Аналіз даних також може допомогти виявити закономірності у поведінці противника та зрозуміти, які дії можуть бути взяті для зниження ефективності його дій. Big Data можуть бути використані в логістичних цілях для моніторингу бойових дій, контролю за розміщенням військ та зброї, для координування дій між військовими підрозділами. Аналіз отриманих даних може допомогти зрозуміти ефективність дій та знайти нові способи боротьби з противником. Big Data використовується у нових моделях дронів, які використовуються для аналізу та розвідки нової території. Також Big Data можуть допомогти визначити оптимальні логістичні маршрути та сприяти забезпеченню доставки потрібних ресурсів в зони бойових дій.

Слабкі сторони. Потрібну інформацію слід шукати не лише у великих наборах даних, але і у інших джерелах, наприклад, звітах військових доповідачів, звітах з місць подій та інших джерел. Без правильного аналізу всіх цих джерел може бути критично залежати лише від Big Data. Обробка великої кількості даних створює великі ризики для конфіденційності та безпеки даних, а саме якщо вони мають особисту інформацію про військових, розміщення військових баз, їх аналітику, або інші конфіденційні дані.

Можливості. Технології Big Data зможуть покращити та осучаснити військові можливості держави, в тому числі для потреб логістичного забезпечення тилу та передової лінії. Можуть розроблятися системи військового управління на основі аналізу даних. Війна завжди була рушійною силою у створенні інновацій, тому і зараз є велика потреба у розвитку нових алгоритмів та технологій. Ця необхідність створює поле для її розвитку. Для України існує багато програм, грантів для допомоги, в тому числі і в ІТ - секторі.

Загрози. Системи Big Data можуть бути ціллю кібератак з боку супротивника, які можуть спричинити крадіжку даних, порушення конфіденційності, превентивного впливу на хід активних бойових дій. Також ці дані можуть бути ціллю для шпигунства, можуть нести компроментацію, що призведе до витоку важливої військової інформації. З використанням даних про психологічний стан та поведінку населення в зонах активних бойових дій можуть бути проведені психологічні атаки, інформаційно - гібридний вплив та адаптування пропаганди під цілі супротивника.

Після проведеної оцінки всіх складових, варто розглянути потенційні стратегії для мінімізації загроз та слабких сторін у вигляді матриці (табл. 5).

Отже, для збалансованого та безпечного розвитку ринку Big Data під час війни необхідні інвестиції у фінансовий та ресурсний потенціал. В України є великі можливості для розвитку цієї галузі, оскільки війна диктує свої нові правила та потреби, які пов’язані з технологіями Big Data, Після завершення війни ці технології можуть бути використані іншими державами та адаптовані до застосування у цивільному секторі. Також варто пам’ятати про безпеку даних у поствоєнний період, тому уряду України слід збільшити кількість заходів забезпечення кібербезпеки для захисту військових систем, економіки України та цивільного населення.

Таблиця 5

Матриця SWOT – аналіз ринку Big Data в умовах війни

	Можливості	Загрози
Сильні сторони	Наявні технології становлять основу для створення більш вдосконалених систем аналізу воєнних дій, тоді як перекваліфікація фахівців сектору Big Data може задовольнити потреби військово-промислового комплексу в захисті військової інформації.	Досвід, набутий у боротьбі з кіберзагрозами, а також інвестиції у цифрову технологізацію країни, сприяють зменшенню загроз, пов'язаних з втратою та крадіжкою даних. Контроль та обмеження розповсюдження контенту з РФ допомагає уникнути наслідків інформаційного впливу на суспільство та військово-промисловий комплекс.
Слабкі сторони	Інвестування у сектор Big Data та надання можливостей отримання грантів сприятимуть підготовці нових фахівців в галузі ІТ для задоволення потреб військово-промислового комплексу. Можливе відкриття спеціалізованих напрямків з кіберзахисту в навчальних закладах, що належать до Міністерства оборони України, також може стати сприятливим кроком у цьому напрямку.	Нестабільні інформаційні умови можуть призвести до зупинки та зниження розвитку в економічних та військово-промислових галузях. Недостатня захищеність даних може призвести до їх витоку та використання для шпигунства та маніпуляцій, що особливо небезпечно в умовах війни.

Джерело: власна розробка

У поствоєнний період продукція ринку Big Data буде корисною для розвитку та відбудови держави та нейтралізації наслідків війни. Також, використання технологій Big Data після війни може бути необхідним для відновлення та підтримки руйнівних наслідків війни на зруйнованих територіях, зокрема:

- відновлення критичної та інших видів інфраструктури. Big Data може допомогти зібрати інформацію про пошкодження об’єктів логістичної інфраструктури, наприклад, про стан доріг, мостів і інших об'єктів. Ця інформація може використовуватися для планування та порівняння відновлення об’єктів інфраструктури після війни;
- забезпечення безпеки населення. Big Data може бути задіяна для моніторингу і аналізу злочинності в постконфліктних зонах, щоб влада могла застосувати обґрунтовані дії з питань безпеки населення, об’єктів інфраструктури тощо;
- медична допомога. Big Data може використовуватися для збору даних про стан здоров'я населення на територіях активних бойових дій. Ці дані можуть застосуватися для планування та здійснення медичної допомоги для тих, хто її потребує;
- розвиток секторів економіки. Big Data може бути важливою для віднови економіки після війни, збираючи дані про бізнес-середовище та економічну активність в зоні конфлікту. Ця інформація може використатися для розробки ефективних стратегій відновлення та розвитку бізнесу;
- культурна спадщина. Big Data може бути корисною для збору даних про культурну спадщину в зонах конфлікту, щоб відновлювати та зберегти культурні пам'ятки та історичні об'єкти;
- військові злочинці. Використання Big Data може допомогти в ідентифікації злочинців, оскільки великі обсяги даних, що збираються і обробляються за допомогою різних технологій, можуть дати інформацію, яка дозволить знайти злочинців та розкрити їхні злочинні дії.

В умовах війни за даними напрямами активізується робота з Big Data, як на безпечних територіях, територіях активних бойових дій, так і деокупованих територіях. Прогнозується, що після закінчення війни, ринок Big Data зможе більше сфокусуватися на потребах для відбудови та відновлення України.

Висновки

Світ щороку демонструє збільшення місткості ринку Big Data. Обробка великих обсягів даних має потенціал для розвитку різних галузей та покращення якості життя людей. Застосування Big Data дозволяє здійснювати ефективний моніторинг різних сфер, включаючи економіку, медицину, науку, соціальні процеси та здійснювати аналіз даних, виявляти тенденції, прогнозувати події та приймати обґрунтовані рішення на основі точних даних.

Однак, разом з можливостями, використання Big Data з'являються і загрози. Однією з найбільших проблем сучасного світу є брак приватності. Розвиток всіх позитивних і негативних аспектів цієї галузі вимагає більшої уваги для забезпечення захисту персональних даних. Слід пам'ятати, що в умовах розвитку інформаційно-комунікаційних технологій створюється нові методи для витоку даних. В сучасному світі незаконно отримуються майже усі дані, які у майбутньому використовуються проти власників. Під загрозою витоку даних можуть були не лише індивідуальні особи, але й великі компанії та уряди країн.

Розвиток Big Data в Україні є активним та перспективним напрямком. Україна має потужний IT-сектор та висококваліфікованих спеціалістів, що може стати суттєвим фактором у розвитку Big Data для окремих галузей, в тому числі, військово-промислового комплексу під час війни.

До початку повномасштабного вторгнення українські сектори економіки вже успішно застосовували аналітичні інструменти Big Data для збору, аналізу та використання великих обсягів даних. Зокрема, використання Big Data дозволяє підвищити ефективність діяльності у сферах банківської справи та фінансів, медицини, виробництва та логістики, енергетики, телекомунікацій тощо.

Починаючи з 2014 року, українські державні системи активно піддавалися кібератакам з боку Росії. Ці атаки були спрямовані на різні ієрархічні рівні, але головною ціллю були і залишаються об'єкти критичної інфраструктури. Після 24 лютого 2022 року кількість кібератак, які не були замасковані за походженням з Росії, зросла втричі. Існує кореляція між часом ракетних обстрілів та кібератак.

Перспективи подальших досліджень

Перспективами подальших досліджень є розробка маркетингових стратегій для імплементації технологій Big Data щодо розбудови України та розвитку економіки у післявоєнний період.

Список літератури

1. "Нафтогаз" щодня зазнає близько 800 кібератак. (2020). Уніан. URL: https://www.unian.ua/economics/energetics/zahist-danih-naftogaz-shchodnya.html.

2. Андаліцька І. (2022). Масова кібератака на Україну: СБУ розслідує причетність спецслужб РФ. Уніан. URL: https://www.unian.ua/economics/telecom/masova-kiberataka-na-ukrajinu-sbu-rozsliduye-prichetnist-specsluzhb-rf-novini-11672053.html.

3. Вакшинська Н. Захист персональних даних. Тези 79 Студентської науково-технічної конференції, 28 жовтня 2021 р., Львів, Видавництво Львівської політехніки, 89.

4. Shvarts D. A. (2022). Кібератака в Україні 15 лютого була найбільшою в історії держави. Уніан. URL: https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html.

5. Камчатий М. (2017). Заборонені засоби ведення кібервійни, Підприємництво, господарство і право, 9, 211 - 217 с.

6. Капінвестиції в українські IT-компанії зросли у 3,3 рази за 2017 рік. Mind. (2018).URL: https://mind.ua/news/20182572-kapinvesticiyi-v-ukrayinski-it-kompaniyi-zrosli-u-33-raza-za-2017-rik.

7. Курочко Н. (2022). Як росія та Україна воюють на кіберфронті. Економічна Правда. URL: https://www.epravda.com.ua/columns/2022/09/28/691925/.

8. Лисогор. І. (2023). Росія щоденно здійснює близько 10 кібератак проти України. Дорослий погляд на світ. LB.ua URL: https://lb.ua/society/2023/02/28/547362_rosiya_shchodenno_zdiysnyuie_blizko_10.html.

9. НАБУ. ВВП України. URL : https://nabu.ua/ua/vvp-2.html.

10. СБУ встановила причетність спецслужб РФ до масштабної кібератаки вірусу-блокувальника (2017). Уніан. URL: https://www.unian.ua/politics/2005644-sbu-vstanovila-prichetnist-spetsslujb-rf-do-masshtabnoji-kiberataki-virusu-blokuvalnika.html.

11. Сироїд. Т. (2017). Діяльність Генеральної Асамблеї ООН. URL: https://legalactivity.com.ua/index.php?option=com_content&view=article&id=1445%3A31-0117-16&catid=173%3A2-0217&Itemid=216&lang=ru.

12. У серпні було здійснено понад 40 кібератак на ресурси органів влади (2021). Уніан. URL: https://www.unian.ua/science/u-serpni-bulo-zdiysneno-ponad-40-kiberatak-na-resursi-organiv-vladi-sbu-novini-11531968.html.

13. Шандрівська О. Є., Кириленко А. А. (2021). Особливості ідентифікації ризиків ринку BIG DATA. Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку, 3 (1), 82 – 95.

14. Cortez A.,P. Rita., Moro S.(2018). Researchtrendson Big Data in Marketing: A text mining and topic modeling based literature analysis. European Researchon Managementand Business Economics, 24, 1-7. DOI: https://doi.org/10.1016/j.iedeen.2017.06.002

15. Ahmadi M., Dileepan P. (2016). A SWOT-analysis of big data. TheJournal of Education for Business., 18, (5). DOI: https://doi.org/10.1080/08832323.2016.1181045

16. Cukier K. (2018). TheRise of Big Data: How It's Changing the Way We Think About the World. JSTOR, (58-65) URL: https://www.jstor.org/stable/23526834.

17. Fedor O. (2022). Ransomware Statistics. Antivirus Guide. URL: https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gc_BwE.

18. Gartner. Головна сторінка. URL: https://www.gartner.com/en.

19. Johnson C. (2019). How much Data is Produced every Day 2021? The next tech. URL: https://www.the-next-tech.com/blockchain-technology/how-much-data-is-produced-every-day-2019/#:~:text=of%20data%20usage.

20. Longo, J., Kuras, E., Smith, H., Hondula, D. M. andJohnston, E. (2017).Technology Use, Exposure to Natural Hazards, and Being Digitally Invisible. URL: https://jlphd.wordpress.com/category/papers/.

21. Lunter J. (2018). How Netflix Uses Big Data to Drive Success. Inside Big DataURL: https://inside Big Data.com/2018/01/20/netflix-uses-big-data-drive-success/.

22. Mar B. (2018). How Much Data Do We Create Every Day? Forbes. URL: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=3981732a60ba.

23. Petrosyan A. (2023). Annual number of data compromises. Statista. URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

24. Share of enterprises (2023). Statbsta URL: https://www.statista.com/statistics/1271855/enterprise-share-performing-big-data-analysis-ukraine/.

25. Shinichi K., Jun-Koo K., Jungmin K. at al.(2018). What is the Impact of Successful Cyber attack son Targe tFirms? NBER Working Paper, 24409. URL: https://www.nber.org/papers/w24409.pdf

26. Singh H. (2016).How Big Data is Revolutionizing Healthcare. LinkedIn. URL: https://www.linkedin.com/pulse/how-big-data-revolutionizing-healthcare-harpreet-singh/.

27. Statista. Головна сторінка URL: https://www.statista.com/.

28. Taylor P. (2022). Global Big Data industry market size 2011-2027. Statista. URL: https://www.statista.com/statistics/254266/global-big-data-market-forecast/#:~:text=The%20global%20big%20data%20and,billion%20U.S.%20dollars%20in%202022.

29. Taylor P. (2022). Volume of data information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. Statista. URL: https://www.statista.com/statistics/871513/worldwide-data-created/.

30. What is Ransomware (2023). Trellix. URL: https://uk.wikipedia.org/wiki/Ransomware#:~:text.

References

1. "Naftohaz" shchodnia zaznaie blyzko 800 kiberatak. [«Naftogaz» is subjected to about 800 cyberattacks every day] (2020). Unian.[Union]. Retrieved from: https://www.unian.ua/economics/energetics/zahist-danih-naftogaz-shchodnya.html.

2. Andalitska I. (2022). Masova kiberataka na Ukrainu: SBU rozsliduie prychetnist spetssluzhb RF. [Massive cyber-attack on Ukraine: the SBU is investigating the involvement of the special services of the Russian Federation]. Unian. [Union]. Retrieved from: https://www.unian.ua/economics/telecom/masova-kiberataka-na-ukrajinu-sbu-rozsliduye-prichetnist-specsluzhb-rf-novini-11672053.html.

3. Vakshynska N. Zakhyst personalnykh danykh. [Protection of personal data]. Tezy 79 Studentskoi naukovo-tekhnichnoi konferentsii, [Abstracts of the 79th Student Scientific and Technical Conference], 28 zhovtnia 2021 r., Lviv, Vydavnytstvo Lvivskoi politekhniky, 89.

4. Shvarts D.A. (2022). Kiberataka v Ukraini 15 liutoho bula naibilshoiu v istorii derzhavy. [The cyberattack in Ukraine on February 15 was the largest in the history of the country].Unian. [Union]. Retrieved from: https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html.

5. Kamchatyi M. (2017). Zaboroneni zasoby vedennia kiberviiny, Pidpryiemnytstvo, hospodarstvo i pravo, [Prohibited means of conducting cyber warfare, Entrepreneurship, economy and law], 9, 211 - 217 s.

6. Kapinvestytsii v ukrainski IT-kompanii zrosly u 3,3 raza za 2017 rik. [Capital investments in Ukrainian IT companies increased 3.3 times in 2017]. Mind. (2018). Retrieved from: https://mind.ua/news/20182572-kapinvesticiyi-v-ukrayinski-it-kompaniyi-zrosli-u-33-raza-za-2017-rik.

7. Kurochko N. (2022). Yak rosiia ta Ukraina voiuiut na kiberfronti. [How Russia and Ukraine are fighting on the cyber front]. Ekonomichna Pravda.[Economictruth]. Retrieved from: https://www.epravda.com.ua/columns/2022/09/28/691925/.

8. Lysohor. I. (2023). Rosiia shchodenno zdiisniuie blyzko 10 kiberatak proty Ukrainy. Doroslyi pohliad na svit. [Russia carries out about 10 cyberattacks against Ukraine every day. An adult view of the world].LB.ua Retrieved from: https://lb.ua/society/2023/02/28/547362_rosiya_shchodenno_zdiysnyuie_blizko_10.html.

9. NABU. VVP Ukrainy. [GDP of Ukraine]. Retrieved from: https://nabu.ua/ua/vvp-2.html.

10. SBU vstanovyla prychetnist spetssluzhb RF do masshtabnoi kiberataky virusu-blokuvalnyka. [The SBU established the involvement of the special services of the Russian Federation in a large-scale cyberattack of the blocker virus]. (2017). Unian. [Union]. Retrieved from: https://www.unian.ua/politics/2005644-sbu-vstanovila-prichetnist-spetsslujb-rf-do-masshtabnoji-kiberataki-virusu-blokuvalnika.html

11. Syroid. T. (2017). Diialnist Heneralnoi Asamblei OON. [Activities of the UN General Assembly]. Retrieved from: https://legalactivity.com.ua/index.php?option=com_content&view=article&id=1445%3A31-0117-16&catid=173%3A2-0217&Itemid=216&lang=ru.

12. U serpni bulo zdiisneno ponad 40 kiberatak na resursy orhaniv vlady. [In August, more than 40 cyberattacks were carried out on government resources]. (2021). Unian. [Union]. Retrieved from: https://www.unian.ua/science/u-serpni-bulo-zdiysneno-ponad-40-kiberatak-na-resursi-organiv-vladi-sbu-novini-11531968.html.

13. Shandrivska O. Ye., Kyrylenko A. A. (2021). Osoblyvosti identyfikatsii ryzykiv rynku BIG DATA. Menedzhment ta pidpryiemnytstvo v Ukraini: etapy stanovlennia i problemy rozvytku, [Features of BIG DATA market risk identification. Management and entrepreneurship in Ukraine: stages of formation and problems of development], 3 (1), 82 – 95.

14. Cortez A.,P. Rita., Moro S.(2018). Research trends on Big Data in Marketing: A text mining and topicmodeling based literature analysis. European Research on Management and Business Economics, 24, 1-7. DOI: https://doi.org/10.1016/j.iedeen.2017.06.002

15. Ahmadi M., Dileepan P. (2016). A SWOT-analysis of big data. The Journal of Education for Business., 18, (5). DOI: https://doi.org/10.1080/08832323.2016.1181045

16. Cukier K. (2018). The Rise of Big Data: How It's Changing the Way We Think About the World. JSTOR, (58-65) URL: https://www.jstor.org/stable/23526834.

17. Fedor O. (2022). Ransomware Statistics. AntivirusGuide. Retrieved from: https://www.antivirus-guide.com/cybersecurity/ransomware-statistics/?gc_BwE

18. Gartner. Holovna storinka. URL: https://www.gartner.com/en.

19. Johnson S. (2019). How much Data is Produced every Day 2021? The next tech. Retrieved from: https://www.the-next-tech.com/blockchain-technology/how-much-data-is-produced-every-day-2019/#:~:text=of%20data%20usage.-

20. Longo, J., Kuras, E., Smith, H., Hondula, D. M. and Johnston, E. (2017). Technology Use, Exposure to Natural Hazards, and Being Digitally Invisible. Retrieved from: https://jlphd.wordpress.com/category/papers/.

21. Lunter J. (2018). How Netflix Uses Big Data to Drive Success. Inside Big Data Retrieved from: https://inside Big Data.com/2018/01/20/netflix-uses-big-data-drive-success/.

22. Mar B. (2018). How Much Data Do We Create Every Day? Forbes. Retrieved from: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=3981732a60ba.

23. Petrosyan A. (2023). Annual number of data compromises. Statista. Retrieved from: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

24. Share of enterprises (2023). Statbsta Retrieved from: https://www.statista.com/statistics/1271855/enterprise-share-performing-big-data-analysis-ukraine/.

25. Shinichi K., Jun-Koo K., Jungmin K. at al. (2018). What is the Impact of Successful Cyberattacks on Target Firms? NBER Working Paper, 24409. Retrieved from: https://www.nber.org/papers/w24409.pdf

26. Singh H. (2016). How Big Data is Revolutionizing Healthcare. LinkedIn. Retrieved from: https://www.linkedin.com/pulse/how-big-data-revolutionizing-healthcare-harpreet-singh/.

27. Statista. Holovna storinka Retrieved from : https://www.statista.com/.

28. Taylor P. (2022). Global big data industry market size 2011-2027. Statista. Retrieved from: https://www.statista.com/statistics/254266/global-big-data-market-forecast/#:~:text=The%20global%20big%20data%20and,billion%20U.S.%20dollars%20in%202022.

29. Taylor P. (2022). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. Statista. Retrieved from: https://www.statista.com/statistics/871513/worldwide-data-created/.

30. What is Ransomware (2023). Trellix. URL: https://uk.wikipedia.org/wiki/Ransomware#:~:text

N. Yu. Vakshynska, O. Ye. Shandrivska
Lviv Polytechnic National University

SPECIFICS OF BIG DATA MARKET DEVELOPMENT FOR THE NEEDS OF UKRAINIAN ECONOMIC RECOVERY IN THE POST-WAR PERIOD

This article analyses the characteristics and prospects of the global big data market, and identifies the sources of data leakage in the global big data market. A study of the peculiarities of the development of the big data market in Ukraine in the economic context before and during the war was conducted, which revealed the influence of international institutions in the fight against cyber-attacks in the context of disturbances.

The directions of adaptation of the Ukrainian cyberspace to functioning in the conditions of war are identified, and recommendations are made on the directions of implementation of Big Data technologies in the post-war period for the needs of economic growth. The results of the study of the big data market are summarized. Recommendations on the directions of implementation of big data technologies in the post-war period for the needs of economic growth are given.

The purpose of the study is to research and analyse trends, development prospects and threats to the big data market at the global level and at the level of the Ukrainian economy during military operations; to develop recommendations on economic directions to implement the protection of personal data in the context of disruptive factors.

The results of the study show that the big data market in Ukraine is operating in a disruptive environment, but this does not prevent its development for the benefit of Ukraine's infrastructure and economy. The biggest threat to this infrastructure is cyber-attacks from the Russian Federation. The aim of these actions is to steal data in order to manipulate it and to destabilise the Ukrainian population and its government institutions.

The perspectives for further research are the development of strategies for the implementation of big data technologies for the development of Ukraine and the economy in the post-war era.

Key words: Big Data, personalized data, war, cyber attacks, SWOT analysis, military-industrial complex, national economy