DOI: https://doi.org/10.12958/1817-3772-2024-3(77)-203-216

УДК 004.056:004.9

Д. В. Попова,
доктор філософії з економіки,
ORCID 0000-0001-5801-2950,
e-mail: Dianavpopova1995@gmail.com,
м. Київ, Україна,

С. В. Яременко,
доктор філософії з економіки,
ORCID 0000-0001-5805-953X,
м. Прага, Чехія

КІБЕРБЕЗПЕКА В ЕПОХУ ІНДУСТРІЇ 5.0: НОВІ ВИКЛИКИ ТА МОЖЛИВОСТІ

Постановка проблеми. У контексті Індустрії 5.0, де цифрові технології стають визначальними факторами у формуванні сучасних економічних та соціальних процесів, кібербезпека набуває особливої актуальності. Індустрія 5.0 передбачає глибоку інтеграцію фізичних, цифрових та біологічних систем, що створює унікальні можливості для інноваційного розвитку, але також і нові виклики, пов'язані з кіберзагрозами. Це включає зростання ризиків, таких як атаки на критичну інфраструктуру, промислове шпигунство та маніпуляції з даними на глобальному рівні.

Зважаючи на швидку трансформацію технологічного середовища та постійний розвиток кіберзагроз, питання кібербезпеки в епоху Індустрії 5.0 вимагає нових підходів до захисту інформації та систем. Сучасні методи кіберзахисту часто не відповідають новим ризикам, що постають в умовах цифрової трансформації, і тому необхідно розробляти більш адаптивні, інтегровані та гнучкі стратегії для забезпечення безпеки. Це дослідження ставить за мету розкрити ключові виклики та можливості в галузі кібербезпеки в умовах Індустрії 5.0, акцентуючи увагу на необхідності інноваційних рішень для ефективного захисту національних і міжнародних систем від кіберзагроз.

Аналіз останніх досліджень і публікацій. Тематика досліджень у сфері кібербезпека в епоху Індустрії 5.0 активно досліджується як зарубіжними, так і вітчизняними вченими: В. Андреев [1], Ю. Білявська [4], В. Болілий [3], А. Гевара [34], А О. Гуцалюк [4], А. Дегучі [32], Г. Дергачова [7], Б. Кормич [13], К. Краус [14], Н. Краус [14], Т. Ліма [38], Ю. Лісовська [15], О. Лунгол [3], Ю. Максименко [16], О. Ондей [37], В. Осецький [14], В. Остроухова [11], В. Петрик [11], А. Перейра [38], Б. Салгуес [40], Б. Степко [21], О. Стрижак [22], Л. Суховірська [3], Д. Терра [34], М. Фукуяма [33], К. Хіраї [32], В. Хорошко [1], Ю. Чалюк [25], Ф. Чарруа-Сантос [38], В. Чередниченко [1], М. Шелест [1] та інші. Загалом дослідження кібербезпеки та кіберзахисту в сфері «розумних» інформаційно-технологічних проєктів – це важливий аспект сучасного технологічного світу. Воно охоплює аналіз потенційних загроз для смарт-технологій, таких як Інтернет речей (IoT), штучний інтелект, автономні системи і розробку стратегій захисту від цих загроз [27-30; 39]. Хоча існує багато наукових робіт з кібербезпеки, проте деякі ключові виклики та можливості даної проблематики в аспекті Індустрії 5.0 потребують додаткового дослідження. Також, важливим є визначення ефективних методів захисту корпоративних систем і даних, що адаптуються до нових викликів і можливостей, що надає Індустрія 5.0. Особлива увага у цьому аспекті має бути спрямована на посилення кіберстійкості в умовах невпинної цифрової трансформації.

Метою статті є вивчення новітніх викликів і можливостей у сфері кібербезпеки в рамках Індустрії 5.0.

Викладення основного матеріалу дослідження. Ми живемо в епоху, коли на порозі стоїть нова технологічна революція. Це період, коли технології швидко змінюють наше життя, трансформуючи економічні та соціальні реалії. Згідно з доповіддю Римського клубу «Come on!» 2017 року, «старий світ приречений, новий світ неминучий». Сучасне індустріальне суспільство зіштовхується з величезними викликами, що випливають з цих змін. Радикальне оновлення глобальної соціотехнологічної структури призводить до повної перебудови звичних систем, створення нових соціокультурних патернів та економічних стратегій. Ці зміни охоплюють не лише технологічну парадигму, але й моделі управління та суспільні норми. Відбувається інтеграція виробництва з Інтернетом та інформаційними технологіями, переосмислюються суспільні цілі та глобальні досягнення. Все це ставить перед нами не

тільки нові можливості, але й серйозні виклики, з якими необхідно впоратися.

Наразі трансформація суспільства відбувається з неймовірною швидкістю, відмінною від тривалих процесів минулих епох. Якщо аграрні перетворення займали тисячоліття, а індустріальні зміни розгорталися протягом століття, то сучасний перехід до новітнього суспільства відбувається протягом лише декількох десятиліть. В центрі цієї метаморфози знаходиться концепція «Індустрії 4.0», яка зародилась у 2011 році на промисловій виставці у Ганновері [37]. «Індустрія 4.0» характеризується стрімким розвитком інформаційно-комунікаційних технологій, автоматизацією та роботизацією виробничих процесів. Ця модель швидко стала домінантною у глобальних дискусіях, набувши ключової ролі на Всесвітньому економічному форумі в Давосі, та стала основою національних стратегій країн, таких як США, Японія, Швеція, Китай, Південна Корея, Франція та Італія. Ці зміни відзначають новий напрямок в еволюції суспільства, де прогрес вимірюється не десятиліттями, а швидкістю технологічного інноваційного розвитку [40].

В Японії було засновано Національний інститут просування цифрової економіки та цифрового суспільства (JIPDEC), що свідчить про країнну відданість цифровізації. Паралельно, у США великі технологічні гіганти, такі як AT&T, Cisco, GE, IBM, та Intel, об'єдналися для створення Консорціуму промислового інтернету (IIC). Ця відкрита некомерційна група, станом на 2017 рік, налічувала 250 компаній з 30 країн. Протягом приблизно 15 років світ перебуває під впливом «Індустрії 4.0», цифрової революції, яка охопила виробничі галузі та сферу послуг, впливаючи на повсякденне життя країн з розвиненою виробничою структурою та потенціалом для її подальшого вдосконалення [25].

Варто відмітити, що Україна активно пристосовується до концепції «Індустрія 4.0», яка з часом стає важливою частиною стратегічного планування країни. З 2016 року країна ініціювала національний рух, до якого зараз входить понад 100 компаній, що демонструє її намір консолідувати головних стейкхолдерів та урядові структури. Зусилля також були направлені на залучення IT-сектору, створення інноваційних промислових сегментів та адаптацію освітніх програм до нових реалій [22]. Проте, плани України зіткнулися з рядом викликів, включаючи пандемію COVID-19, російську військову агресію, обмежене державне стимулювання цифровізації виробництва та брак навичок у громадян у сфері цифрових інновацій, що ускладнило реалізацію стратегічних планів. Втім, навіть попри воєнний стан та економічні труднощі, стрімкий розвиток цифрових технологій в країні продовжується, дозволяючи Україні наздоганяти глобальних лідерів та адаптуватися до новітніх технологічних трендів.

У сучасному світі економіка активно впроваджує п'яте покоління технологічних укладів, що базується на розвитку технологій для взаємодії між людиною та машиною через застосування штучного інтелекту та машинного навчання. Передбачається, що в недалекому майбутньому основою для взаємодії учасників економічних процесів стане цифровий обмін даними. Це сприятиме розвитку нейромереж і подальшому вдосконаленню систем на базі штучного інтелекту. За оцінками міжнародних дослідників, штучний інтелект стає ключовим елементом цифрової трансформації, який відіграє важливу роль у переході економіки до нового рівня взаємодії між людиною та машиною. Це, в свою чергу, сприяє розширенню цифрових платформ і загальному розвитку цифрової економіки [35].

В області Індустрії 5.0 сучасні дослідження висвітлюють передові практики у використанні штучного інтелекту, що ґрунтуються на двох ключових підходах. Один із цих підходів було представлено Брентом Кедзерським під час його виступу на круглому столі, що відбувся 17 червня 2021 року у Великій Британії. Виступ був присвячений питанням штучного інтелекту. Кедзерський аргументував, що основа Індустрії 5.0 вбачається у синергії технологічних можливостей Індустрії 4.0 та людиноцентричного підходу Індустрії 5.0. Він підкреслив, що таке поєднання відкриває перспективи для гармонійної взаємодії між людським інтелектом та когнітивними системами обчислень [25].

Другий підхід сформульовано Оздчан Сарітас, керівником дослідницької лабораторії Інституту статистичних досліджень та економіки знань, який був представлений на XXII Квітневій Міжнародній конференції з проблемам розвитку економіки та суспільства, що відбулася 13–30 квітня 2021 р. У рамках даного трактування Концепція 5.0 має на увазі «об'єднання людського та машинного інтелекту для створення колективного інтелекту, що дозволяє уникнути в майбутньому технологічної сингулярності, а також удосконалювати людину та розвивати технології одночасно» [25].

Таким чином, в Індустрії 5.0 буде сформовано нову модель людино-машинного інтерфейсу, що у свою чергу призведе до інтелектуальної цифровізації виробничо-економічних систем на вищому рівні, ніж у Індустрії 4.0.

Логічно, що сучасні розвинуті країни активно переходять від індустріальної до інтелектуальної моделі суспільства, яке в Японії відоме як «Суспільство 5.0» або Super Smart Society. Це нове суспільство інтегрує кібернетичні та фізичні простори, роблячи акцент на інноваціях у науці та технологіях як ключових елементах забезпечення економічного розвитку та вирішення соціальних проблем. «Суспільство 5.0» використовує технологічні досягнення епохи «Індустрії 4.0», але йде далі, прагнучи до синергії між людиною і штучним інтелектом. Основні завдання цього суспільства включають підвищення якості людського капіталу та звільнення людей від рутинної фізичної праці, надаючи ширші можли-

вості для самоактуалізації, самореалізації та самовираження [25].

Концепція «Суспільства 5.0» розглядається як адаптація суспільства до сучасних технологій Індустрії 4.0. Ця ідея передбачає створення нової культури та цивілізації, де основними напрямками розвитку є інтеграція інноваційних технологій таких як штучний інтелект, блокчейн, інтернет речей та криптовалюти. Такий поступ технологій не лише змінює економічні умови, але й створює унікальну синергію між людським інтелектом та можливостями машин. В Індустрії 5.0 інновації виступають ключовим фактором, який сприяє переходу до більш стабільної та людиноцентричної промисловості, здатної задовольняти потреби сучасних поколінь без загрози для майбутніх.

Приходимо до висновку, що в Індустрії 5.0, що є еволюцією за четвертою промисловою революцією, де основний акцент був на комп'ютеризації виробництва та бізнесу, ключовим стає всеосяжне впровадження передових технологій у всі сфери суспільного життя. Технології такі як збір та аналіз великих даних, хмарні рішення, краудсорсинг, 3D-друк, біотехнології, безпілотні автомобілі та штучний інтелект мають не просто розвиватися окремо, але інтегруватися у кожен аспект економічної та соціальної діяльності. Таке інтегроване поєднання засобів вирішує складні проблеми сучасності, роблячи повсякденне життя комфортнішим і стійкішим [18].

Отже, Індустрія 5.0 ставить перед собою мету не лише викликати глобальний технологічний прогрес, але й відповісти на найнагальніші гуманітарні та техногенні виклики сьогодення. Це суспільство, яке називається людиноцентричним, визнає людський капітал як основну цінність і ставить технології на службу людині. Ціль полягає у створенні гармонійного співіснування між наукою та технологіями та реальними потребами людей, забезпечуючи стабільне економічне зростання і загальний добробут.

Цей перехід має значні наслідки для суспільства, особливо у контексті соціально-економічних викликів, пов'язаних з діджиталізацією виробництва. Цей процес може призвести до зменшення ролі людини в традиційних сферах, таких як промисловість, сільське господарство та сервісні послуги, що вимагає розроблення адаптаційних стратегій для мінімізації негативних наслідків. Існує ймовірність, що з розвитком автоматизації, процеси в майбутньому досягнуть такої точки, де для підтримання глобальної системи виробництва та логістики буде достатньо лише кількох мільйонів висококваліфікованих спеціалістів.

Для структурованого представлення відмінностей між Індустрією 4.0 та Індустрією 5.0 у формі табл. 1, можна використати такі основні ознаки для порівняння:

1. Основна ціль.
2. Роль людського фактору.
3. Технологічний фокус.
4. Підхід до інновацій.
5. Екологічна відповідальність.

Таблиця 1

Відмінності Індустрії 5.0 в порівнянні з Індустрією 4.0

№ з/п	Ознака	Індустрія 4.0	Індустрія 5.0
1	Основна ціль	Оптимізація та ефективність виробництва	Гармонізація технологій і людського потенціалу
2	Роль людського фактору	Мінімізація людської участі	Акцент на людській креативності та співпраці
3	Технологічний фокус	Автоматизація та Інтернет речей	Інтеграція когнітивних технологій та ШІ
4	Підхід до інновацій	Технологічні інновації	Соціально орієнтовані інновації
5	Екологічна відповідальність	Обмежена увага до екологічних факторів	Висока екологічна відповідальність та сталість

Розроблено авторами на основі [4; 7-9; 14; 18; 25; 36].

Як видно, Індустрія 5.0 представляє собою еволюційний крок від Індустрії 4.0, зосереджуючись на реінтеграції людського творчого потенціалу в автоматизовані процеси, що є ключовою відмінністю між цими двома стадіями технологічного розвитку. Індустрія 4.0 орієнтувалася переважно на максимізацію автоматизації, оптимізацію виробничих процесів через розгортання технологій Інтернету речей (IoT), штучного інтелекту (ШІ) та машинного навчання. Цей підхід прагнув забезпечити високу ефективність та зниження виробничих витрат. На противагу цьому, Індустрія 5.0 включає новий гуманістичний вимір, де основна увага приділяється взаємодії людини і машини з метою досягнення більш стійких та адаптивних виробничих систем. В цьому контексті, ключовими аспектами є впровадження технологій, які підтримують креативність та інноваційний потенціал людського фактору, що дозволяє не просто автоматизувати процеси, а зробити їх більш гнучкими та адаптованими до індивідуальних потреб.

Індустрія 5.0 також впроваджує концепцію стійкості та екологічної відповідальності на виробництво, акцентуючи на збалансованому використанні ресурсів, рециклінгу та мінімізації відходів, що відрізняє її від Індустрії 4.0, де головний акцент

робився на оптимізації та продуктивності без значної уваги до екологічних факторів. Таким чином, Індустрія 5.0 не просто продовжує тенденції Індустрії 4.0, а розвиває їх, вносячи стратегічні корективи з метою створення більш гармонійного та відповідального виробничого середовища.

На цьому етапі особливу увагу приділяється людиноцентричним підходам, збалансованому управлінню ресурсами та розширенні можливостей цифровізації. Цифровізація включає в себе комплексний аналіз та впровадження цифрових технологій у всі аспекти діяльності підприємств. Ми вважаємо, що індустрію 5.0 не слід сприймати як заміну попередній парадигмі – Індустрії 4.0, а радше як її розвиток та доповнення, яке вносить нові ключові аспекти:

– Людиноцентричний підхід. Індустрія 5.0 підкреслює значення створення безпечного та інклюзивного робочого середовища, де пріоритетом є здоров'я та благополуччя працівників, з метою досягнення не лише високої продуктивності, а й задоволення потреб кожного працівника.

– Стійкість. Здатність швидко адаптуватися до змін є критично важливою для підприємств, які прагнуть залишатися конкурентоспроможними в умовах невизначеності, включаючи нові технологічні розробки та зміни в ринкових потребах.

– Екологічний розвиток. Індустрія 5.0 наголошує на важливості циркулярних процесів, які сприяють переробці та повторному використанню природних ресурсів, зменшенню відходів та зниженню екологічного впливу, тим самим підвищуючи ефективність виробничих процесів.

З використанням цифрових технологій, компанії, які належать до Індустрії 5.0, мають змогу значно підвищити свою продуктивність та ефективність. Технології, такі як автоматизація, аналіз даних та штучний інтелект, дозволяють оптимізувати процеси, зменшити витрати та підвищити загальну продуктивність. Цифрова трансформація також сприяє адаптації компаній до змін у ринкових умовах, змінних вимогах споживачів та швидкому розвитку технологій. Одним з основних викликів є інтеграція сучасних технологій з застарілими системами, що може становити загрозу для безпеки та цілісності даних. Управління даними та кібербезпека є критично важливими компонентами в процесі цифрової трансформації, особливо з огляду на зростаючу залежність від рішень, прийнятих на основі даних, та використання штучного інтелекту і машинного навчання, що вимагає строгої відповідності до стандартів конфіденційності та безпеки даних.

У науковій спільноті поки що немає загальноприйнятого визначення терміну «кібербезпека». Це створює потребу в уточненні цього поняття, що допоможе краще зрозуміти її особливості в епоху індустрії 5.0, зокрема ідентифікувати виклики та можливості.

Б. Кормич вважає, що кібербезпека полягає у захисті правових норм, які регулюють інформаційні процеси в державі. Ці норми забезпечують умови для життя та розвитку людини, суспільства і держави, гарантовані Конституцією [13, с. 142].

Група дослідників під керівництвом В. Остроухова пропонує власне визначення терміну «кібербезпека». На їхню думку, це стан захищеності особи, держави та суспільства, за якого забезпечується інформаційний розвиток у технічному, інтелектуальному, соціально-політичному та морально-етичному аспектах, і при цьому зовнішні інформаційні впливи не завдають їм значної шкоди [11, с. 10]. Слід звернути увагу, що це визначення включає не лише пасивну складову, таку як «ступінь захищеності», але й активну – «інформаційний розвиток», який охоплює технічний, інтелектуальний, соціально-політичний та морально-етичний аспекти.

Українські науковці В. Андрєєв, В. Хорошко, В. Чередниченко та М. Шелест визначають кібербезпеку як захист інформації та інфраструктури, що її підтримує, від випадкових або цілеспрямованих впливів, як природного, так і штучного походження. Такі впливи можуть завдати неприпустимої шкоди учасникам інформаційних відносин, включаючи власників і користувачів інформації та інфраструктури, яка її забезпечує [1, с. 55].

В. Петрик визначає кібербезпеку як стан, при якому забезпечується захист об'єктів, таких як особистість, суспільство, держава та інформаційно-технічна інфраструктура. У цьому стані об'єкти можуть нормально функціонувати, незважаючи на внутрішні чи зовнішні інформаційні впливи. [19, с. 160-161].

О. Баранов визначає кібербезпеку як стан, що забезпечує захист життєво важливих інтересів особистості, суспільства та держави. У цьому стані мінімізуються ризики, пов'язані з неповнотою, несвоєчасністю або недостовірністю інформації, негативним інформаційним впливом, небажаними наслідками використання інформаційних технологій, а також несанкціонованим поширенням інформації [2, с. 134].

В. Цимбалюк визначає кібербезпеку як стан захищеності законодавчо встановлених норм та параметрів інформаційних процесів і відносин. Такий стан забезпечує необхідні умови для функціонування держави, суспільства та людини як суб'єктів цих процесів і відносин [24, с. 78-79].

О. Степко визначає кібербезпеку як стан захищеності життєво важливих інтересів особистості, суспільства та держави, за якого мінімізуються ризики, пов'язані з неповнотою, несвоєчасністю або недостовірністю інформації, негативним впливом інформаційних потоків, несприятливими наслідками використання інформаційних технологій, а також несанкціонованим поширенням даних [21].

Л. Харченко характеризує кібербезпеку як частину національної безпеки, що включає процес уп-

равління загрозами та небезпеками. Цей процес здійснюється як державними, так і недержавними інституціями, а також окремими громадянами, з метою забезпечення інформаційного суверенітету України [23, с. 46].

Ю. Максименко акцентує увагу на кібербезпеці як результаті управління реальними та/або потенційними загрозами з метою забезпечення національних інтересів особи, суспільства і держави у цифровій сфері [16, с. 52].

О. Олійник, О. Соснін та Л. Шиманський розглядають кібербезпеку через призму загроз як систему превентивних заходів, спрямованих на захист життєво важливих інтересів особистості, суспільства та держави від негативних інформаційних впливів.

Ці заходи охоплюють економічну сферу, внутрішню і зовнішню політику, науково-технологічну, соціокультурну і оборонну сфери, систему державного управління. Вони також забезпечують незалежний розвиток елементів національного інформаційного простору, інформаційний суверенітет країни та захист від маніпуляцій і дезінформації. Держава повинна мати здатність нейтралізувати або послаблювати внутрішні та зовнішні інформаційні загрози, що впливають на свідомість і підсвідомість як окремих осіб, так і суспільства в цілому [17, с. 540-541].

Отже, кібербезпека має системний характер, що робить її забезпечення складним і багатогранним процесом. Для визначення її структурних елементів зазвичай використовуються такі терміни, як «напрями», «механізми» та «шляхи» забезпечення. Аналіз різних джерел вказує на те, що структурні компоненти кібербезпеки залишаються недостатньо розробленими та систематизованими. Проте саме розгляд кібербезпеки як комплексної діяльності дозволяє не лише гармонізувати термінологію, але й здійснювати глибокий змістовний аналіз із використанням можливостей діяльнісного підходу [15].

Варто зазначити, що у сучасному інформаційному суспільстві система кібербезпеки України формується та розвивається на основі Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в електронній сфері. Основу цієї системи складають органи, сили та засоби забезпечення кібербезпеки, які використовують комплекс заходів, таких як адміністративно-правові, інформаційно-аналітичні, організаційно-управлінські тощо, з метою забезпечення стабільного функціонування державного управління. Відповідно до статті 2 Закону України «Про основи національної безпеки України», правову базу у сфері національної безпеки визначають Конституція, цей закон та інші закони України, міжнародні договори, ратифіковані Верховною Радою України, а також нормативно-правові акти, ухвалені для виконання цих законів [15].

Таким чином, кібербезпека є складним і багатогранним процесом, що включає різні аспекти забезпечення захисту, такі як напрями, механізми та шляхи. Хоча структура кібербезпеки ще не до кінця систематизована, її розгляд як комплексної діяльності дозволяє гармонізувати термінологію та глибше аналізувати змістовні аспекти цієї сфери.

На наш авторський погляд, кібербезпека – це система комплексних заходів, що забезпечують захист інформаційних ресурсів, технологій та інфраструктури від загроз будь-якого походження з метою забезпечення стійкості, надійності та безперервного розвитку держави, суспільства та окремих осіб в умовах цифрової трансформації та Індустрії 5.0.

Досліджуючи питання кібербезпеки, слід враховувати, що вона є невід'ємною частиною інформаційних технологій. У сучасному світі стрімкий розвиток та поширення нових інформаційних і телекомунікаційних технологій створюють умови для глобальної інформаційної революції. Цей процес має безпосередній вплив на всі аспекти діяльності держави, зокрема політику, економіку, управління, фінанси, культуру, науку та розвиток інформаційних відносин [15].

Кібербезпека в епоху Індустрії 5.0 має свої унікальні особливості, що зумовлені змінами в технологічному розвитку, інтеграцією штучного інтелекту, взаємодією людей і машин, а також зростаючою залежністю від цифрових технологій у всіх сферах життя. Індустрія 5.0 ставить акцент не лише на автоматизацію, як це було в Індустрії 4.0, але й на тісну співпрацю між людьми та технологіями, що вимагає нових підходів до кібербезпеки.

Основні особливості кібербезпеки в епоху Індустрії 5.0 представлені у табл. 2.

Таким чином, кібербезпека в епоху Індустрії 5.0 потребує нових підходів, що враховують інтеграцію людини та технологій, розвиток штучного інтелекту, захист кіберфізичних систем та етичні аспекти використання технологій. Це комплексний процес, який вимагає постійної адаптації до нових викликів у світі цифрових інновацій.

Кібербезпека відіграє ключову роль у захисті інформації та комп'ютерних систем від несанкціонованого доступу та кіберзлочинів. Ця область включає забезпечення конфіденційності, цілісності та доступності інформації на всіх етапах її життєвого циклу. В той час як фізична безпека охороняє людей і матеріальні активи, кібербезпека фокусується на захисті цифрових даних, користувацьких програм і серверів.

Заходи кібербезпеки, також відомі як кіберзахист, спрямовані на попередження атак, виявлення загроз та реагування на інциденти. Вони включають активні кроки для передбачення можливих атак і протидії потенційним кіберзагрозам. Це важливо, оскільки кіберзлочинці часто мотивовані

Таблиця 2

Основні особливості кібербезпеки в епоху Індустрії 5.0

№ з/п	Особливості	Змістовне наповнення
1	Взаємодія людини і машини	Індустрія 5.0 фокусується на інтеграції людських інтелектуальних та креативних здібностей із можливостями машин і штучного інтелекту. Це означає, що кібербезпека повинна охоплювати не лише технічний захист, але й забезпечувати захист від ризиків, пов'язаних із людським фактором. Необхідно створювати безпечні умови для роботи з технологіями, які враховують соціальні та психологічні аспекти.
2	Розширення можливостей штучного інтелекту (ШІ)	Зростаюча роль ШІ у прийнятті рішень та автоматизації бізнес-процесів вимагає нових стандартів кібербезпеки. Оскільки штучний інтелект активно використовується для аналізу даних, управління системами та взаємодії з людиною, кіберзагрози, спрямовані на алгоритми ШІ, можуть стати більш складними та небезпечними. Кібербезпека в цьому випадку має включати захист ШІ від маніпуляцій, несанкціонованих дій і зловмисного використання.
3	Захист персональних даних і конфіденційності	В епоху Індустрії 5.0 значно збільшується обсяг персональних даних, які збираються і обробляються. Високий рівень автоматизації та індивідуалізація процесів веде до нових ризиків у сфері конфіденційності. Тому кібербезпека повинна включати вдосконалені механізми захисту даних, дотримання етичних стандартів щодо використання інформації та управління доступом до конфіденційних даних.
4	Кіберфізичні системи	Індустрія 5.0 все більше покладається на кіберфізичні системи, які інтегрують фізичні об'єкти з віртуальними системами. Це вимагає захисту від загроз не лише в цифровій сфері, але й у фізичному просторі. Наприклад, атаки на промислові роботи або дрони можуть мати серйозні наслідки для безпеки людей та інфраструктури. Тому кібербезпека повинна забезпечувати захист цих систем від вторгнень та саботажу.
5	Підвищення ролі етичних аспектів кібербезпеки	Оскільки Індустрія 5.0 тісно пов'язана з персоніфікацією технологій та їхнім впливом на суспільство, етичні аспекти кібербезпеки стають все більш важливими. Відповідальне використання технологій, запобігання дискримінації, дотримання прав людини в цифровій сфері - все це має бути враховано при створенні політик кібербезпеки.
6	Постійна адаптація до нових загроз	Індустрія 5.0 характеризується швидким впровадженням інноваційних рішень, що створює нові виклики для кібербезпеки. Злочинці також адаптуються до нових технологій, розробляючи нові типи атак. Кібербезпека в цій епохі потребує динамічних та адаптивних систем, які можуть швидко реагувати на зміни у загрозах і забезпечувати надійний захист.
7	Глобалізація та мережеві загрози	У світі, де більшість процесів глобалізовані і взаємопов'язані, мережеві загрози стають ще більш небезпечними. Індустрія 5.0 використовує величезні обсяги даних і технологій, що взаємодіють через глобальні мережі. Кібербезпека повинна бути орієнтована на захист від масштабних атак, які можуть вплинути на міжнародні процеси, економіку та безпеку держав.

Розроблено авторами на основі [8-11; 14; 18; 20; 25; 33-34; 37; 40].

фінансовими, політичними або соціальними інтересами і використовують новітні технології для атак на критичну інфраструктуру, включаючи охорону здоров'я, фінансові установи та урядові організації.

Отже, захист кіберпростору сьогодні є життєво важливим, оскільки у кіберзлочинців з'являється все більше можливостей для атак. Протягом останніх двох десятиліть критична інфраструктура у багатьох розвинених країнах стикалася з кібератаками, що призвело до значних фінансових втрат для численних підприємств [26].

Щороку у світі реєструються понад 2000 підтверджених випадків витоку даних, кожен з яких завдає збитків на суму близько 3,9 мільйона доларів. З початку 2000-х років кіберзлочинці вкрали особисті дані понад 3,5 мільярда людей, що складає приблизно половину населення планети. Відтак, на сьогоднішній день експерти в області кібербезпеки перебувають у великому попиті. Ось чому набуває актуальності знання про запобіжні заходи, про які ми розповімо далі [26].

Вважаємо, що необхідно розглянути основні види кібератак для чіткого розуміння захисту від них в контексті кібербезпеки. Отже, основні їх види:

1. Фішинг. Це тактика, за якою зловмисники відправляють жертвам електронні листи або повідомлення, які виглядають як законні, з метою виманювання грошей чи конфіденційних даних. Вони можуть також маскувати шкідливі URL-адреси під легітимні.

2. Автоматичні атаки та боти. Більшість кібератак виконуються за допомогою автоматизованих ботів, які сканують системи на предмет вразливостей, намагаються зламати паролі, а також заражають системи шкідливими програмами.

3. DDoS-атаки. Це атаки, під час яких систему бомбардують великою кількістю фальшивого трафіку до того моменту, коли система не може впоратися з навантаженням, блокуючи доступ законним користувачам.

4. Шкідливе програмне забезпечення. Створене спеціально для заподіяння шкоди комп'ютерним системам або допомоги у проведенні кібератак, таке програмне забезпечення може поширюватися та заражати інші комп'ютери [26].

Розуміння цих загроз є ключовим кроком у розробці ефективної стратегії кібербезпеки.

Як вже було визначено, кібербезпека, хоч і не має єдиного визначення, стосується нових викликів у сфері безпеки, які торкаються як окремих організацій, так і суспільства загалом. Ці виклики зростають разом із цифровою трансформацією та збільшенням нашої залежності від взаємопов'язаних цифрових систем і послуг. Кібербезпека включає заходи, які компанії можуть застосовувати для захисту своїх важливих бізнес-систем, програмного забезпечення, пристроїв та мереж передачі даних від кіберзагроз. Ці загрози, що включають шкідливі події чи процеси, можуть серйозно вплинути на діяльність організації, її фінанси, дані та репутацію, а в гіршому випадку - і на безперервність її діяльності [12].

Кібербезпека в рамках Індустрії 5.0 розкривається на декількох важливих рівнях, кожен з яких має свої специфіки та вимоги. На фізичному рівні безпека забезпечується через захист пристроїв промислового інтернету речей, таких як датчики, часто встановлені в місцях, недоступних для постійного контролю. Захист цих пристроїв може включати в себе як прості рішення – наприклад, замкнені шафи для устаткування – так і більш складні, як системи сигналізації на панелі управління, що сповіщають про несанкціоновані спроби доступу, або системи відеоспостереження з функцією розпізнавання осіб. Людський фактор становить другий рівень кібербезпеки. Він акцентує на вразливості, що виникає через недостатню обізнаність або увагу працівників. Хакери часто використовують методи соціальної інженерії для отримання конфіденційної інформації від співробітників, підрядників та замовників, використовуючи їх некомпетентність як засіб доступу до корпоративних мереж. Третій рівень – організаційний, який раніше характеризувався розділенням обов'язків між різними командами, не завжди включаючи IT-безпеку в обов'язки кожної з них. Сучасні підходи вимагають інтегрованого захисту, який об'єднує кібербезпеку, забезпечення надійності систем та фізичний захист для створення більш безпечного виробничого середовища. Четвертий рівень кібербезпеки – технологічний, має свої особливості. З одного боку, інтелектуальніші технології сприяють стримуванню, запобіганню та виявленню кібератак. Проте, з іншого боку, кіберзагрози також стають складнішими та розвиненішими. Це означає, що старі технологічні системи, які раніше вважалися безпечними та надійними, тепер можуть стати вразливими точками, через які хакери можуть отримати доступ до виробничих систем компанії [10].

Ми вважаємо, що при забезпеченні кібербезпеки в умовах Індустрії 5.0, необхідно звертати увагу не тільки на технологічні аспекти. Важливо також опрацювати операційні складові процесів, які включають ретельне планування бізнес-процесів, чітке визначення зон відповідальності підрозділів і окремих працівників. Такий комплексний підхід дозволяє не тільки ліквідувати існуючі уразливості в системах, але й забезпечити міцнішу загальну структуру кіберзахисту підприємства.

Важливо визначити пріоритети кібербезпеки в епоху Індустрії 5.0, що відіграють ключову роль у формуванні стійких та безпечних виробничих середовищ, адаптованих до швидкого розвитку технологій та постійно змінюваних загроз. Основні напрямки включають:

1. Інтеграція з ШІ та автоматизацією. Індустрія 5.0 зосереджена на оптимізації взаємодії людей і машин. Пріоритетом є захист систем, які управляють цими взаємодіями, забезпечуючи безпеку даних і процесів, контрольованих штучним інтелектом.

2. Розширене забезпечення прозорості і простежуваності. Важливо забезпечити прозорість усіх процесів і даних у мережі, дозволяючи оперативно виявляти і реагувати на кіберзагрози.

3. Проактивний захист. Передбачення можливих кібератак та розробка методів їх попередження стає необхідністю, а не вибором. Це включає аналіз загроз та оновлення безпеки в реальному часі.

4. Підвищення обізнаності і навчання співробітників. Навчання співробітників основам кібербезпеки та найкращим практикам для мінімізації ризиків від людського фактору.

5. Забезпечення сталості та екологічної безпеки. Врахування екологічних аспектів та впливів у стратегії кібербезпеки, забезпечуючи таким чином не тільки безпеку даних, але й відповідальне використання ресурсів.

Ці пріоритети створюють основу для забезпечення цифрової безпеки в епоху Індустрії 5.0, підкреслюючи важливість інтегрованого та багаторівневого підходу до кіберзахисту (рис. 1).

Національний інститут стандартів і технологій США (NIST) розробив комплексну Структуру кібербезпеки, яка спрямована на ефективне управління ризиками для організацій (рис. 2).

Ця структура включає п'ять ключових функцій: ідентифікація, захист, виявлення, реагування та відновлення. Ідентифікація полягає у глибокому розумінні бізнес-контексту, управлінні активами і оцінці ризиків. Функція захисту передбачає розробку безпечної інфраструктури, контроль доступу та навчання персоналу. Виявлення зосереджено на моніторингу систем та виявленні загроз. Реагування включає в себе розробку планів реакції на інци-

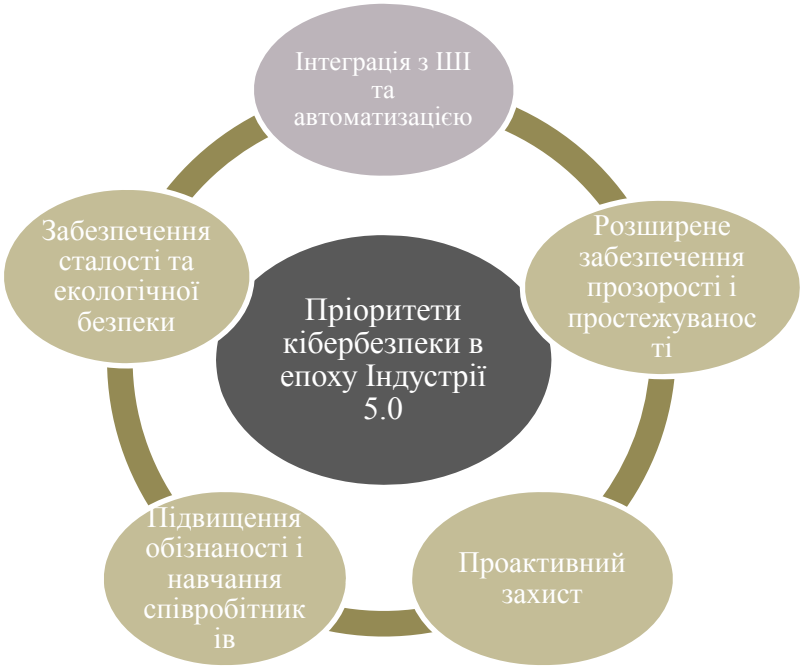

Рис. 1. Пріоритети кібербезпеки в епоху Індустрії 5.0

Побудовано авторами.

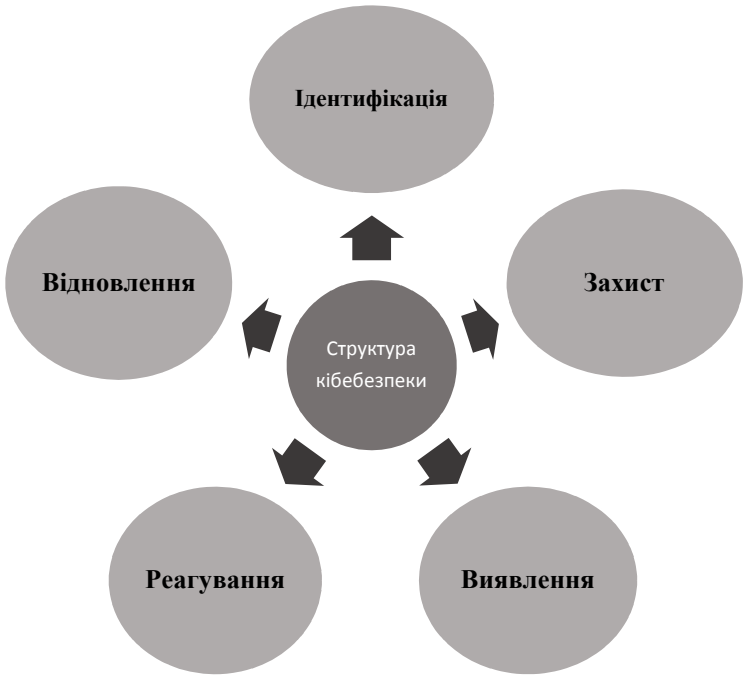

Рис. 2. Структура кібербезпеки, розроблена Національним інститутом стандартів і технологій

денти, аналіз подій і управління змінами. Відновлення має на увазі розробку планів безперервності бізнесу і методів відновлення систем після аварій. Реалізація цих функцій здійснюється через різноманітні технічні, управлінські та операційні заходи. Структура NIST служить надійною основою для створення комплексних програм кібербезпеки, що інтегрують людські, процесуальні та технологічні компоненти, адаптуючись до специфічних потреб кожної організації і зменшуючи ризики кіберінцидентів [22]. Структура кібербезпеки NIST, що охоплює п'ять ключових функцій – ідентифікація, захист, виявлення, реагування та відновлення – становить суттєвий фундамент для ефективного управління кіберризиками в організаціях. У контексті Індустрії 5.0, де взаємодія між людьми та машинами досягає нового рівня інтеграції за допомогою передових технологій, ця структура набуває ще більшого значення.

В Індустрії 5.0 кібербезпека перестає бути лише технічним завданням; вона вимагає глибокого розуміння взаємозв'язків між технологічними, процесуальними та людськими аспектами. Ідентифікація ризиків та управління активами стають складнішими з огляду на зростаючу коннектованість та автоматизацію, що властиві Індустрії 5.0. Тому захист інфраструктури, контроль доступу та навчання персоналу повинні бути адаптовані до нових реалій, де кіберзагрози стають все більш складними та різноманітними.

Функція виявлення, яка зосереджена на моніторингу систем, вимагає новітніх технологій для виявлення загроз в реальному часі, що є критично важливим у світлі швидких змін в технологічному ландшафті. Реагування на інциденти та відновлення після кібератак також потребують нових підходів, зорієнтованих на мінімізацію перерв у роботі та забезпечення бізнес-стійкості.

Завдяки своїй гнучкості та орієнтації на комплексне розуміння кібербезпеки, структура NIST забезпечує ідеальну основу для адаптації до нових викликів та можливостей Індустрії 5.0, що дозволяє організаціям не лише захищати свої активи, а й ефективно реагувати на кіберзагрози, враховуючи постійно змінювані умови та потреби сучасного промислового середовища [22].

Отже, у світлі невпинного розвитку Індустрії 5.0, де передові технології та штучний інтелект все більше інтегруються у всі аспекти виробництва, питання кібербезпеки набувають особливої актуальності. Ця нова ера технологічних інновацій вносить як низку нових викликів, так і відкриває перед організаціями численні можливості для забезпечення безпеки своїх систем і даних. Розглянемо докладніше, як саме еволюція кіберпростору в контексті Індустрії 5.0 впливає на зміну парадигми кібербезпеки, ідентифікуємо ключові виклики та можливості, що стоять перед сучасними підприємствами (табл. 3).

Таблиця 3

Ключові виклики та можливості в контексті кібербезпеки в епоху Індустрії 5.0

№ з/п	Виклики	Можливості
1	Збільшення взаємозв'язків систем. Індустрія 5.0 характеризується розширеною інтеграцією цифрових технологій у всіх аспектах виробництва, що створює складніші мережі та збільшує потенційні вектори атак	Розумні системи виявлення загроз. Розвиток технологій дозволяє створювати більш розвинуті системи моніторингу і виявлення, які можуть передбачати і нейтралізувати загрози до того, як вони спричинять шкоду
2	Автоматизація та автономні системи. Посилення використання автономних роботів і систем управління, керованих штучним інтелектом, вносить додаткові ризики, пов'язані з ненавмисними помилками в програмному забезпеченні та можливими зловмисними маніпуляціями	Захист інтеграції з блокчейн-технологіями. Блокчейн може забезпечити вищий рівень захисту даних через децентралізовану та незмінну структуру записів
3	Загрози штучного інтелекту. Інтелектуальні системи можуть бути вразливими до атак з використанням даних, що вводяться (data poisoning), що може призвести до некоректного прийняття рішень	Штучний інтелект у кібербезпеці. AI може бути використаний для автоматизації складних процесів виявлення і реагування на кіберзагрози, значно підвищуючи ефективність кібероборони
4	Кібер-фізичні системи та IoT. Широке впровадження кібер-фізичних систем та інтернету речей в промисловості створює великі виклики для забезпечення конфіденційності, цілісності та доступності критично важливих даних	Адаптивні системи безпеки. Розвиток технологій дозволяє створювати системи безпеки, які можуть адаптуватися до змін у загрозах і виробничих умовах в реальному часі
5	Комплексність даних та їх захист. Ріст обсягів даних, їх різноманітність і швидкість обробки потребують вдосконалення методів захисту і зберігання	Освіта та навчання. Підвищення обізнаності та кваліфікації працівників у галузі кібербезпеки може значно знизити людські помилки і підвищити загальний рівень захищеності

Розроблено авторами.

Ці виклики та можливості є важливими аспектами для врахування при розробці стратегій кібербезпеки в епоху Індустрії 5.0, дозволяючи організаціям не лише відповідати на нові виклики, але й використовувати нові можливості для покращення своєї кіберстійкості.

Також важливо, на наш погляд, провести аналіз впливу покращення кіберстійкості економічних систем на людські можливості. Аналіз впливу покращення кіберстійкості на людські можливості в економічних системах може бути розглянутий через декілька ключових аспектів. Вдосконалення кіберстійкості не тільки захищає інформаційні ресурси і критичну інфраструктуру, але й сприяє економічному розвитку, соціальній стабільності, та розширенню людських можливостей.

1. Забезпечення довіри в цифровому просторі. Висока кіберстійкість збільшує довіру споживачів і бізнесів до електронної комерції, онлайн банкінгу та інших цифрових сервісів. Це, в свою чергу, підвищує використання цих послуг, сприяє інноваціям і веде до росту економіки. Коли користувачі відчува-

ють, що їхні дані безпечні, вони активніше використовують цифрові технології, що відкриває нові можливості для навчання, роботи та соціальної взаємодії.

2. Захист від інформаційних загроз. Підвищення кіберстійкості зменшує ризики від кіберзлочинності, такі як крадіжка особистих даних, фішинг, шахрайство з платіжними картками, що забезпечує більший захист особистих і корпоративних фінансів. Зменшення економічних втрат від кіберзлочинів позитивно впливає на економічну стабільність і збереження ресурсів, необхідних для розвитку людського потенціалу.

3. Стимулювання інновацій. Безпечне цифрове середовище стимулює бізнеси до впровадження нових технологій, сприяючи технологічному прогресу. Інновації у сфері кібербезпеки можуть також створити нові робочі місця і сприяти професійному розвитку в області IT-безпеки, збільшуючи кількість висококваліфікованих фахівців.

4. Забезпечення доступу до інформації. Покращення кіберстійкості забезпечує більший доступ до інформації, що є важливим для освіти та самоосвіти. В захищеному онлайн середовищі люди можуть безпечно доступатися до освітніх ресурсів, що покращує загальний рівень освіченості населення та підвищує культурний розвиток.

5. Підтримка соціальної справедливості. Кіберстійкість може також сприяти соціальній справедливості, захищаючи чутливі дані і запобігаючи дискримінації. Надійні механізми захисту даних дозволяють захистити інформацію про вразливі групи населення, сприяючи їхньому захисту та підтримці.

6. Збільшення економічної ефективності Підвищення кіберстійкості дозволяє підприємствам зменшити витрати, пов'язані з відновленням систем після кібератак. Це також зменшує простої у роботі, підвищуючи загальну продуктивність бізнесу.

7. Покращення корпоративного управління Компанії, які активно інвестують у кібербезпеку, демонструють вищий рівень відповідальності та прозорості. Це зміцнює довіру інвесторів та партнерів, сприяючи стабільнішому бізнес-середовищу.

8. Зміцнення національної безпеки Забезпечення кіберстійкості є критично важливим для національної безпеки, оскільки захищає від кібератак, які можуть бути спрямовані на дестабілізацію уряду чи критичної інфраструктури країни.

Разом ці аспекти створюють комплексне розуміння того, як покращення кіберстійкості впливає на економічні системи та розвиток людських можливостей в різних сферах життя в епоху Індустрії 5.0 (рис. 3).

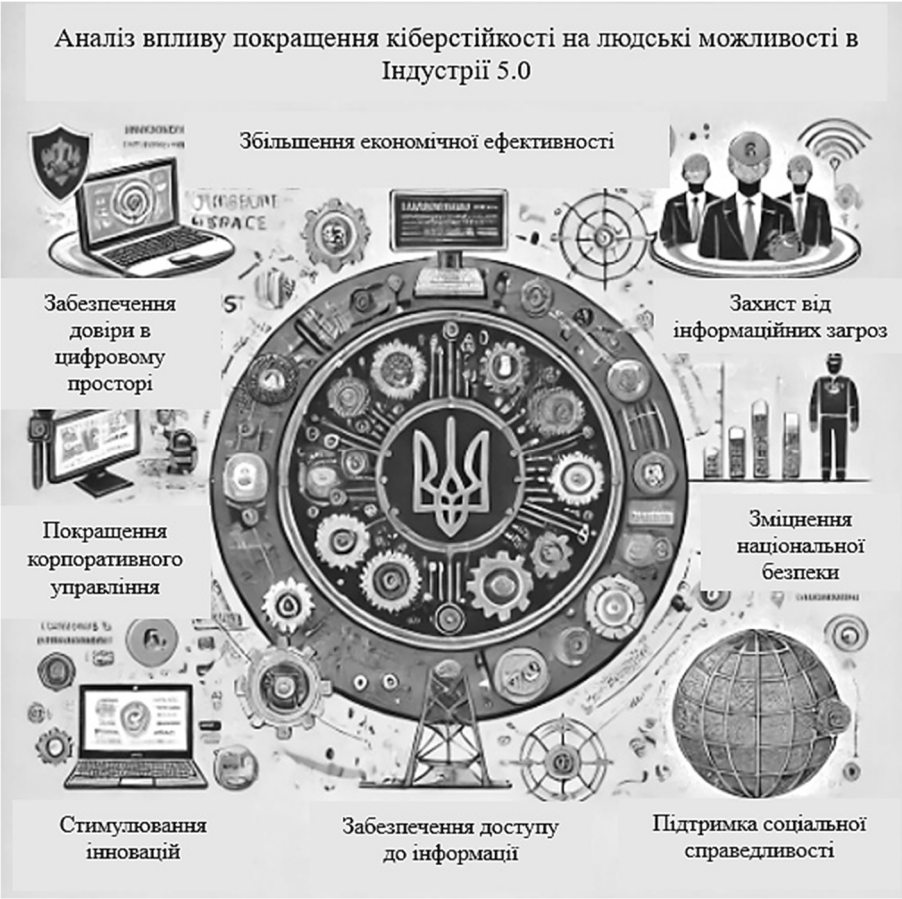

Рис. 3. Аналіз впливу покращення кіберстійкості на людські можливості в Індустрії 5.0

Авторська розробка.

Загалом, покращення кіберстійкості сприяє створенню стійкішої, справедливішої і інноваційної економіки, де людські можливості можуть розширюватися на фоні захищеного та стабільного цифрового простору.

У контексті кібербезпеки в епосі Індустрії 5.0, яка характеризується широким впровадженням автоматизації, штучного інтелекту та зв'язку між машинами, покращення кіберстійкості відіграє надзвичайно важливу роль у розширенні людських можливостей.

По-перше, значне зростання використання цифрових технологій та даних в Індустрії 5.0 посилює потребу в надійному захисті цих даних. Покращення кіберстійкості не тільки запобігає ризикам, таким як втрата даних, шахрайство або кібератаки, але й забезпечує неперервність бізнесу і знижує потенційні збитки.

По-друге, збільшення довіри до цифрових систем сприяє ширшому впровадженню інноваційних технологій. Коли компанії та споживачі впевнені у безпеці своїх даних, вони активніше включаються в цифрову економіку, що веде до зростання економічної активності та відкриває нові можливості для розвитку бізнесу та особистісного зростання.

По-третє, кіберстійкість сприяє створенню більш інклюзивного суспільства. Захист чутливих даних забезпечує, що інформація про вразливі групи населення захищена від зловживань, сприяючи рівності та соціальній справедливості.

На завершення, покращення кіберстійкості є фундаментом для безпечного використання та розвитку технологій Індустрії 5.0. Воно не тільки знижує ризики, пов'язані з новими технологіями, але й підкреслює роль кібербезпеки як важливого елемента стратегічного планування для будь-якої організації, прагнучої до інновацій та довгострокового розвитку.

Висновки. У статті було розглянуто ключові виклики та можливості кібербезпеки в епоху Індустрії 5.0. Основним висновком є те, що стрімка інтеграція фізичних, цифрових та біологічних систем створює нові можливості для розвитку, однак одночасно підвищує ризики кіберзагроз, що вимагають перегляду традиційних підходів до кіберзахисту.

Інтеграція штучного інтелекту та людиноцентричних технологій створює нові виклики для кібербезпеки, зокрема в аспектах захисту від загроз, пов’язаних з людським фактором та маніпуляціями ШІ. Це вимагає нових стратегій захисту, що охоплюють як технічні, так і етичні аспекти. Захист кіберфізичних систем набуває все більшого значення, оскільки критично важливі системи все більше залежать від взаємодії фізичних та цифрових компонентів. Це створює додаткові загрози не тільки в цифровому, але й у фізичному просторі. Постійна адаптація до нових загроз є критично важливою для забезпечення безпеки в умовах швидкої технологічної трансформації. Сучасні системи кібербезпеки повинні бути динамічними та здатними до самонавчання. Етичні аспекти кібербезпеки в Індустрії 5.0 набувають все більшої важливості. Використання штучного інтелекту та персоналізація технологій повинні враховувати права людини, запобігати дискримінації та забезпечувати прозорість. Кібербезпека як частина національної безпеки підкреслює необхідність розробки глобальних та міжнаціональних стандартів для боротьби з кіберзагрозами, що мають міжнародний характер.

Таким чином, для ефективного захисту в умовах Індустрії 5.0 необхідний інтегрований, адаптивний та проактивний підхід до кібербезпеки, який враховує як технічні, так і соціально-етичні аспекти.

Література

1. Андреев В. І., Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи кібербезпеки / за ред. проф. В. О. Хорошка. 2 вид., доп. і перероб. Київ: ДУІКТ, 2009. 292 с.

2. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи. Київ: ВД «СофтПрес», 2005. 316 с.

3. Болілий В. О., Гуцалюк О. М., Суховірська Л. П., Лунгол О. М. Розробка та впровадження програмного продукту «Автоматизована система обліку «АХІМ» на підприємствах малого бізнесу в системі формування аналітичного забезпечення. *Економічні інновації.* 2021. Т. 23. № 3 (80). С. 33-40. DOI: https://doi.org/10.31520/ei.2021.23.3(80).33-40.

4. Білявська Ю., Шестак Я. Кібербезпеки та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. №3. С. 47-59. DOI: https://doi.org/10.31617/2.2022(43)04.

5. Hutsaliuk O. M., Bondar Iu. A., Kotsiurba O. Y. Formation of analytical provision of sustainable functioning of service enterprises. *Вісник післядипломної освіти. Серія «Соціальні та поведінкові науки»*. 2022. Вип. 20 (49). С. 81-102. DOI: https://doi.org/10.32405/2522-9931-2022-20(49)-81-102.

6. Гуцалюк О. М., Бондар Ю. А., Цатурян Р. О. Особливості формування системи реінжинірингу бізнес-процесів підприємств з використанням цифрових технологій. *Економічний вісник Донбасу*. 2023. № 2 (72). С. 40-47. DOI: https://doi.org/10.129 58/1817-3772-2023-2(72)-40-47.

7. Дергачова Г. М., Колешня Я. О. Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології. *Економічний вісник НТУУ "КПІ"*. 2020. № 17. С. 280-290. DOI: https://doi.org/10.20535/2307-5651.17.2020.216367.

8. Індустрія 5.0: напрями дій та шляхи розвитку. URL: https://www.clusters.org.ua/blog-single/industry-5-0-napriamy-diy/.

9. Індустрія 5.0: бачення трансформацій від Європейської комісії. URL: https://www.clusters.org.ua/blogsingle/industry-5-0/.

10. Кібербезпека: як захистити підприємство в епоху Індустрії Х.0. URL: https://www.telesphera.net/blog/kiberbezpeka-indystrii-x-0.html.

11. Кібербезпека держави: підручник / В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.; в 2 т. Т. 2. / за заг. ред. В. В. Остроухова. К.: ДНУ «Книжкова палата України», 2016. 328 с.

12. Коваленко Н. В., Панасюк І. В. Управління ризиками транснаціональних корпорацій. *Економіка та менеджмент кораблебудування*. 2020. №4. С. 103-109. DOI: https://doi.org/10.15589/znp2020.4(482).12.

13. Кормич Б. А. Кібербезпека: організаційно-правові основи: навч. посіб. Київ: Кондор, 2008. 382 с.
14. Краус К., Краус Н., Осецький В. Суспільство 5.0 на базі розвитку інноваційного університету та цифрового підприємництва. *Економіка та суспільство.* 2021. Вип. 28. DOI: https://doi.org/10.32782/2524-0072/2021-28-37.
15. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.
16. Максименко Ю. Є. Теоретико-правові засади забезпечення кібербезпеки України : дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 186 с.
17. Олійник О. В., Соснін О. В., Шиманський Л. Є. Політикоправові аспекти формування інформаційного суспільства суверенної і незалежної України. *Держава і право: Збірник наукових праць*. 2001. Вип. 13. С. 534–541.
18. Петренко А. І. Неминучі зміни ІТ індустрії. Підготовка кадрів в умовах п'ятої промислової революції (Індустрія 5.0). *Системні дослідження та інформаційні технології*. 2022. №1. С. 27. DOI: https://doi.org/10.20535/SRIT.2308-8893.2022.1.02.
19. Петрик В. М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: навч. посіб. Київ: Росава, 2006. 208 с.
20. Про Індустрію 5.0 – чому це стає актуальним для України. URL: https://www.industry4ukraine.net/publications/pro-industriyu5-0-chomu-cze-staye-aktualnym-dlya-ukrayiny/.
21. Степко О. М. Аналіз головних складових кібербезпеки держави. Інститут міжнародних відносин Національного авіаційного університету. *Науковий вісник. Економіка, право, політологія, туризм*. 2011. Т. 1. № 3. С. 83-92
22. Стрижак О. Особливості взаємозв'язку рівня розвитку людського капіталу й цифрових технологій у контексті формування суспільства 5.0. *Agricultural and Resource Economics.* 2022. Vol. 8(3). P. 224–243. DOI: https://doi.org/10.51599/are.2022.08.03.11.
23. Харченко Л. С. Кібербезпека України: глосарій / за заг. ред. Р. А. Калюжного. Київ: Текст, 2004. 136 с.
24. Цимбалюк В. С. Інформаційне право (основи теорії і практики): монографія. Київ: «Освіта України», 2010. 388 с.
25. Чалюк Ю. О. Суспільство 5.0 у Японській концепції Кейданрен. *Міжнародний науковий журнал «Механізм регулювання економіки».* 2023. №1(99). С. 65-74. DOI: https://doi.org/10.32782/mer.2023.99.11.
26. Що таке кібербезпека? Заходи забезпечення кібербезпеки. URL: https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/.
27. Critical Infrastructure Security and Resilience. URL: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical infrastructure-sectors/chemical-sector.
28. Critical Infrastructure. URL: https://www.techtarget.com/whatis/definition/critical-infrastructure.
29. Critical Infrastructure. URL: https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en.
30. Defining critical infrastructure. URL: https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-securitycentre/defining-critical-infrastructure.
31. What is network functions virtualization nfv. URL: https://www.juniper.net/ru/ru/research-topics/what-is-networkfunctions-virtualization-nfv.html.
32. Deguchi A., Hirai C., Matsuoka H., Nakano T., Oshima K., Tai M., Tani S. What Is Society 5.0? 2018. Singapore: Hitachi and The University of Tokyo Joint Research Laboratory. 177 p.
33. Fukuyama M. Society 5.0: Aiming for a New Human-centered Society. URL: https://www.hitachi.com/rev/archive/2017/r2017_06/trends/index.html.
34. Guevara A., Terra D., Portes J., Alves da Silva J., Magalhaes K. A Ranking of countries concerning progress towards o Society 5.0. *Journal on Innovation and Sustainability*. 2020. V. 11(4). P. 188–199. DOI: https://doi.org/10.23925/2179-3565.2020v11i4p188-199.
35. Magistretti S., Dell'Era C., Petruzzelli A. M. How Intelligent is Watson? Enabling Digital Transformation through Artificial Intelligence. *Business Horizons.* 2019. Vol. 62. N 6. P. 819–829. DOI: https://doi.org/10.1016/j.bushor.2019.08.004.
36. Miraz, Mahadi & Hasan, Mohammad Tariq & Sumi, Farhana & Sarkar, Shumi & Hossain, Mohammad. Industry 5.0: The Integration of Modern Technologies. 2022. DOI: https://doi.org/10.1201/9781003122401-14.
37. Onday O. Japan's Society 5.0: Going Beyond Industry 4.0. *Business and Economics Journal.* 2019. Vol. 10(2). DOI: https://doi.org/:10.4172/2151-6219.1000389.
38. Pereira A., Lima T., Charrua-Santos F. Industry 4.0 and Society 5.0: Opportunities and Threats. URL: https://www.ijrte.org/wp-content/uploads/papers/v8i5/D8764118419.pdf.
39. Almeida, F. Prospects of Cybersecurity in Smart Cities. *Future Internet.* 2023. Vol. 15(9). P. 285. DOI: https://doi.org/10.3390/fi15090285.
40. Salgues B. Society 5.0: Industry of the Future, Technologies, Methods and Tools (Technological Prospects and Social Applications). 2018. London: Wiley-ISTE. 304 p. DOI: https://doi.org/10.1002/9781119507314.

References

1. Andreev, V. I., Khoroshko, V. O., Cherednychenko, V. S., Shelest, M. E. (2009). Osnovy kiberbezpeky [Fundamentals of Cybersecurity]. 2nd ed. Kyiv, Publishing house of DUKIT. 292 p. [in Ukrainian].
2. Baranov, O. A. (2005). Informatsiine pravo Ukrainy: stan, problemy, perspektyvy [Information Law of Ukraine: State, Problems, and Perspectives]. Kyiv, «SoftPres». 316 p. [in Ukrainian].
3. Bolily, V. O., Hutsaliuk, O. M., Sukhovirska, L. P., Luhnol, O. M. (2021). Rozrobka ta vprovadzhennia prohramnoho produktu «Avtomatyzovana systema obliku «AXIM» na pidpryiemstvakh maloho biznesu v systemi formuvannia analitychnoho zabezpechennia [Development and implementation of a software product "Automated accounting system "AXIM" for small businesses in the system of formation of analytical support]. *Ekonomichni innovatsii – Economic Innovations,* Vol. 23, No. 3 (80), pp. 33-40. DOI: https://doi.org/10.31520/ei.2021.23.3(80).33-40 [in Ukrainian].
4. Biliavska, Yu., Shestak Ya. (2022). Kiberbezpeky ta kiberhihiiena: nova era tsyfrovykh tekhnolohii [Cyber security and cyber hygiene: the new era of digital technologies]. *Tovary i rynky – Goods and Markets*, No. 3, pp. 47-59. DOI: https://doi.org/10.31617/2.2022(43)04 [in Ukrainian].
5. Hutsaliuk, O. M., Bondar, Iu. A., Kotsiurba, O. Y. (2022). Formation of analytical provision of sustainable functioning of service enterprises. V*isnyk pisliadyplomnoi osvity. Seriia «Sotsialni ta povedinkovi nauky» – Bulletin of Postgraduate Education. Series "Social and Behavioral Sciences"*, No. 20(49), pp. 81-102. DOI: https://doi.org/10.32405/2522-9931-2022-20(49)-81-102 [in Ukrainian].

6. Hutsaliuk, O. M., Bondar, Iu. A., Tsaturyan, R. O. (2023). Osoblyvosti formuvannia systemy reinzhynirynhu biznes-protsesiv pidpryiemstv z vykorystanniam tsyfrovykh tekhnolohii [Peculiarities of Forming a System of Reengineering Business Processes of Enter-prises Using Digital Technologies]. *Ekonomichnyi visnyk Donbasu – Economic Herald of the Donbas,* Vol. 2 (72), pp. 40-47. DOI: https://doi.org/10.129 58/1817-3772-2023-2(72)-40-47 [in Ukrainian].

7. Derhachova, H. M., Koleshnia, Ya. O. (2020). Tsyfrova transformatsiia biznesu: sutnist, oznaky, vymohy ta tekhnolohii [Digital Transformation of Business: Essence, Features, Requirements, and Technologies]. *Ekonomichnyi visnyk NTUU "KPI" – Economic Bulletin of NTUU "KPI"*, No. 17, pp. 280-290. DOI: https://doi.org/10.20535/2307-5651.17.2020.216367 [in Ukrainian].

8. Industriia 5.0: napriamy dii ta shliakhy rozvytku [Industry 5.0: Directions and Paths of Development]. Retrieved from https://www.clusters.org.ua/blog-single/industry-5-0-napriamy-diy/ [in Ukrainian].

9. Industriia 5.0: bachennia transformatsii vid Yevropeiskoi komisii [Industry 5.0: Vision of Transformations from the European Commission]. Retrieved from https://www.clusters.org.ua/blog-single/industry-5-0/ [in Ukrainian].

10. Kiberbezpeka: yak zakhystyty pidpryiemstvo v epokhu Industrii X.0 [Cybersecurity: How to Protect an Enterprise in the Era of Industry X.0]. Retrieved from https://www.telesphera.net/blog/kiberbezpeka-indystrii-x-0.html [in Ukrainian].

11. Petryk, V. M., Prysiazhniuk, M. M., Melnyk, D. S. et al. (2016). Kiberbezpeka derzhavy [Cybersecurity of the State]. Vol. 2. Kyiv, DNU «Knyzhkova palata Ukrainy». 328 p. [in Ukrainian].

12. Kovalenko, N. V., Panasiuk, I. V. (2020). Upravlinnia ryzykamy transnatsionalnykh korporatsii [Risk Management of Transnational Corporations]. *Ekonomika ta menedzhment korablebuduvannia – Economics and Management of Shipbuilding*, No. 4, pp. 103-109. DOI: https://doi.org/10.15589/znp2020.4(482).12 [in Ukrainian].

13. Kormych, B. A. (2008). Kiberbezpeka: orhanizatsiino-pravovi osnovy [Cybersecurity: Organizational and Legal Foundations]. Kyiv, Kondor. 382 p. [in Ukrainian].

14. Kraus, K., Kraus, N., Osetskyi, V. (2021). Suspilstvo 5.0 na bazi rozvytku innovatsiinoho universytetu ta tsyfrovoho pidpryiemnytstva [Society 5.0 Based on the Development of an Innovative University and Digital Entrepreneurship]. *Ekonomika ta suspilstvo – Economy and Society*, Issue 28. DOI: https://doi.org/10.32782/2524-0072/2021-28-37 [in Ukrainian].

15. Lisovska, Yu. P. (2019). Kiberbezpeka: ryzyky ta zakhody [Cybersecurity: Risks and Measures]. Kyiv, Kondor. 272 p. [in Ukrainian].

16. Maksymenko, Yu. E. (2007). Teoretyko-pravovi zasady zabezpechennia kiberbezpeky Ukrainy [Theoretical and Legal Foundations of Ensuring Cybersecurity in Ukraine]. *Candidate's thesis*. Kyiv. 186 p. [in Ukrainian].

17. Oliinyk, O. V., Sosnin, O. V., Shymans'kyj, L. E. (2001). Politykopravovi aspekty formuvannia informatsiinoho suspilstva suverennoi i nezalezhnoi Ukrainy [Political and Legal Aspects of Forming an Information Society of a Sovereign and Independent Ukraine]. *Derzhava i pravo – State and Law*, Issue 13, pp. 534-541 [in Ukrainian].

18. Petrenko, A. I. (2022). Nemynuchi zminy IT industrii. Pidhotovka kadriv v umovakh piatoi promyslovoi revoliutsii (Industriia 5.0) [Inevitable Changes in the IT Industry. Training Personnel in the Context of the Fifth Industrial Revolution (Industry 5.0)]. *Systemni doslidzhennia ta informatsiini tekhnolohii – Systems Research and Information Technologies,* No. 1, p. 27. DOI: https://doi.org/10.20535/SRIT.2308-8893.2022.1.02 [in Ukrainian].

19. Petryk, V. M. (2006). Suchasni tekhnolohii ta zasoby manipuliuvannia svidomistiu, vedennia informatsiinykh viin i spetsialnykh informatsiinykh operatsii [Modern Technologies and Means of Manipulating Consciousness, Conducting Information Wars and Special Information Operations]. Kyiv, Rosava. 208 p. [in Ukrainian].

20. Pro Industriiu 5.0 – chomu tse staie aktualnym dlia Ukrainy [About Industry 5.0 – Why It Is Becoming Relevant for Ukraine]. Retrieved from https://www.industry4ukraine.net/publications/pro-industriyu5-0-chomu-cze-staye-aktualnym-dlya-ukrayiny/ [in Ukrainian].

21. Stepko, O. M. (2011). Analiz holovnykh skladovykh kiberbezpeky derzhavy. Instytut mizhnarodnykh vidnosyn Natsionalnoho aviatsiinoho universytetu [Analysis of the main components of state cybersecurity. Institute of International Relations of the National Aviation University]. *Naukovyi visnyk. Ekonomika, pravo, politolohiia, turyzm – Scientific Bulletin. Economics, Law, Political Science, Tourism*, Vol. 1, No. 3, pp. 83-92 [in Ukrainian].

22. Stryzhak, O. (2022). Osoblyvosti vzaiemozviazku rivnia rozvytku liudskoho kapitalu y tsyfrovykh tekhnolohii u konteksti formuvannia suspilstva 5.0 [Features of the Relationship Between the Level of Human Capital Development and Digital Technologies in the Context of Forming Society 5.0]. *Agricultural and Resource Economics,* Vol. 8(3), pp. 224–243. DOI: https://doi.org/10.51599/are.2022.08.03.11 [in Ukrainian].

23. Kharchenko, L. S. (2004). Kiberbezpeka Ukrainy: hlosarii [Cybersecurity of Ukraine: Glossary]. Kyiv, Tekst. 136 p. [in Ukrainian].

24. Tsymbaliuk, V. S. (2010). Informatsiine pravo (osnovy teorii i praktyky) [Information Law (Foundations of Theory and Practice)]. Kyiv, «Osvita Ukrainy». 388 p. [in Ukrainian].

25. Chaliuk, Yu. O. (2023). Yaponskii kontseptsii Keidanren [Society 5.0 in the Japanese Concept of Keidanren]. *Mizhnarodnyi naukovyi zhurnal «Mekhanizm rehuliuvannia ekonomiky» – International Scientific Journal "Mechanism of Economic Regulation"*, No. 1(99), pp. 65-74. DOI: https://doi.org/10.32782/mer.2023.99.11 [in Ukrainian].

26. Shcho take kiberbezpeka? Zakhody zabezpechennia kiberbezpeky [What is Cybersecurity? Measures for Ensuring Cybersecurity]. Retrieved from https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/ [in Ukrainian].

27. Critical Infrastructure Security and Resilience. Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/chemical-sector.

28. Critical Infrastructure. Retrieved from https://www.techtarget.com/whatis/definition/critical-infrastructure.

29. Critical Infrastructure. Retrieved from https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en.

30. Defining Critical Infrastructure. Retrieved from https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/defining-critical-infrastructure.

31. What is Network Functions Virtualization (NFV). Retrieved from https://www.juniper.net/ru/ru/research-topics/what-is-networkfunctions-virtualization-nfv.html.

32. Deguchi, A., Hirai, C., Matsuoka, H., Nakano, T., Oshima, K., Tai, M., Tani, S. (2018). What Is Society 5.0? Singapore, Hitachi and The University of Tokyo Joint Research Laboratory. 177 p.

33. Fukuyama, M. (2017). Society 5.0: Aiming for a New Human-centered Society. Retrieved from https://www.hitachi.com/rev/archive/2017/r2017_06/trends/index.html.

34. Guevara, A., Terra, D., Portes, J., Alves da Silva, J., Magalhaes, K. (2020). A Ranking of Countries Concerning Progress Towards Society 5.0. *Journal on Innovation and Sustainability,* Vol. 11(4), pp. 188-199. DOI: https://doi.org/10.23925/2179-3565.2020v11i4p188-199.

35. Magistretti, S., Dell'Era, C., Petruzzelli, A.M. (2019). How Intelligent is Watson? Enabling Digital Transformation through Artificial Intelligence. *Business Horizons,* Vol. 62, No. 6, pp. 819–829. DOI: https://doi.org/10.1016/j.bushor.2019.08.004.

36. Miraz, M., Hasan, M.T., Sumi, F., Sarkar, S., Hossain, M. (2022). Industry 5.0: The Integration of Modern Technologies. DOI: https://doi.org/10.1201/9781003122401-14.

37. Onday, O. (2019). Japan's Society 5.0: Going Beyond Industry 4.0. *Business and Economics Journal*, Vol. 10 No. 2. DOI: https://doi.org/10.4172/2151-6219.1000389.

38. Pereira, A., Lima, T., Charrua-Santos, F. (n.d.). Industry 4.0 and Society 5.0: Opportunities and Threats. Retrieved from https://www.ijrte.org/wp-content/uploads/papers/v8i5/D8764118419.pdf.

39. Almeida, F. (2023). Prospects of Cybersecurity in Smart Cities. *Future Internet,* 15(9), 285. DOI: https://doi.org/10.3390/fi15090285.

40. Salgues, B. (2018). Society 5.0: Industry of the Future, Technologies, Methods and Tools (Technological Prospects and Social Applications). London, Wiley-ISTE. 304 p. DOI: https://doi.org/10.1002/9781119507314.

Попова Д. В., Яременко С. В. Кібербезпека в епоху Індустрії 5.0: нові виклики та можливості

У статті розглядаються основні виклики та можливості кібербезпеки в контексті Індустрії 5.0, яка передбачає глибоку інтеграцію фізичних, цифрових і біологічних систем. Основна увага приділена проблемам, пов'язаним із розвитком штучного інтелекту, кіберфізичних систем та автоматизації процесів, що зумовлює необхідність перегляду існуючих підходів до кіберзахисту. Автори обґрунтували, що Індустрія 5.0 є еволюцією за четвертою промисловою революцією, де основний акцент був на комп'ютеризації виробництва та бізнесу, натомість у Індустрії 5.0 ключовим стає всеосяжне впровадження передових технологій у всі сфери суспільного життя. Було структуровано представлено відмінності між Індустрією 4.0 та Індустрією 5.0 з виокремленням основних ознак для порівняння. Визначено на основі аналізу вітчизняних і зарубіжних публікацій, що кібербезпека має системний характер, що робить її забезпечення складним і багатогранним процесом.

Сформульовано авторське визначення поняття «кібербезпека», як складного і багатогранного процесу, що включає різні аспекти забезпечення захисту, такі як напрями, механізми та шляхи, системи комплексних заходів, що забезпечують захист інформаційних ресурсів, технологій та інфраструктури від загроз будь-якого походження з метою забезпечення стійкості, надійності та безперервного розвитку держави, суспільства та окремих осіб в умовах цифрової трансформації та Індустрії 5.0. Визначено основні особливості кібербезпеки в епоху Індустрії 5.0. Розглянуті і обґрунтовані основні види кібератак для чіткого розуміння захисту від них в контексті кібербезпеки. Також було сформульовано пріоритети кібербезпеки в епоху Індустрії 5.0, що відіграють ключову роль у формуванні стійких та безпечних виробничих середовищ, адаптованих до швидкого розвитку технологій та постійно змінюваних загроз.

Авторами розглянути яким чином еволюція кіберпростору в контексті Індустрії 5.0 впливає на зміну парадигми кібербезпеки, зокрема ідентифіковано ключові виклики та можливості, що стоять перед сучасними підприємствами. Також проведений аналіз впливу покращення кіберстійкості економічних систем на людські можливості. Аналіз впливу покращення кіберстійкості на людські можливості в економічних системах був розглянутий через декілька ключових аспектів. Обґрунтовано, що саме визначені аспекти разом створюють комплексне розуміння того, як покращення кіберстійкості впливає на економічні системи та розвиток людських можливостей в різних сферах життя в епоху Індустрії 5.0.

Ключові слова: Індустрія 5.0, кібербезпека, штучний інтелект, кіберфізичні системи, автоматизація, цифрова трансформація, кібератаки, кіберстійкість, захист інформаційних ресурсів, технології, інфраструктура, економічні системи, людські можливості.

Popova D., Yaremenko S. Cyber Security in the Age of Industry 5.0: New Challenges and Opportunities

The article examines the main challenges and opportunities of cybersecurity in the context of Industry 5.0, which involves the deep integration of physical, digital, and biological systems. The focus is on the issues related to the development of artificial intelligence, cyber-physical systems, and process automation, which necessitate a revision of existing approaches to cyber protection. The authors argue that Industry 5.0 is an evolution following the Fourth Industrial Revolution, where the primary emphasis was on computerization of production and business, while in Industry 5.0, the key focus is on the comprehensive implementation of advanced technologies in all areas of societal life. The differences between Industry 4.0 and Industry 5.0 are structurally presented, highlighting key features for comparison. Based on the analysis of domestic and foreign publications, it has been determined that cybersecurity is systemic, making its provision a complex and multifaceted process.

The authors have formulated an original definition of the concept of "cybersecurity" as a complex and multifaceted process that includes various aspects of protection, such as directions, mechanisms, and methods, as well as systems of comprehensive measures that ensure the protection of information resources, technologies, and infrastructure from threats of any origin to ensure the resilience, reliability, and continuous development of the state, society, and individuals in the conditions of digital transformation and Industry 5.0. The main features of cybersecurity in the era of Industry 5.0 have been identified. The main types of cyberattacks are considered and substantiated to provide a clear understanding of how to protect against them in the context of cybersecurity. The priorities of cybersecurity in the era of Industry 5.0, which play a key role in the formation of resilient and secure production environments adapted to the rapid development of technologies and constantly changing threats, have also been formulated.

The authors examine how the evolution of cyberspace in the context of Industry 5.0 affects the paradigm shift in cybersecurity, identifying key challenges and opportunities faced by modern enterprises. The analysis of the impact of improved cyber resilience on human capabilities in economic systems has been conducted. The analysis of the impact of improving cyber resilience on human capabilities in economic systems was considered through several key aspects. It is substantiated that these defined aspects together create a comprehensive understanding of how enhancing cyber resilience affects economic systems and the development of human capabilities in various spheres of life in the era of Industry 5.0.

Keywords: Industry 5.0, cybersecurity, artificial intelligence, cyber-physical systems, automation, digital transformation, cyberattacks, cyber resilience, protection of information resources, technologies, infrastructure, economic systems, human capabilities.

Стаття надійшла до редакції 02.09.2024