ISSN 2308-0361

УДК 004;331.1;65.01

ВПЛИВ КІБЕРЗЛОЧИННОСТІ НА ЦИФРОВУ ЕКОНОМІКУ

Олександр Буров,
провідний науковий співробітник НДІ інтелектуальної власності НАПрН України,
доктор тенічних наук
ID ORCID: 0000-0003-0733-1120

У статті проведено аналіз чинників кібернебезпек для світової економічної системи, які проявилися за період пандемії та переходу економіки до «нової норми», в умовах розширення цифровізації за такими аспектами: цифровізація та нові умови праці, використання гібридної робочої сили, вплив біологічної пандемії та кіберпандемії на зміни в економіці, чинники кіберзагроз для бізнесу. Обґрунтовано виникнення гібридної робочої екосистеми, її переваги та недоліки. Проаналізовано виникнення кіберпандемії як результат стрімкої цифровізації внаслідок пандемії COVID-19 і переходу праці до дистанційної форми. Виділено найбільш вагомі чинники кібербезпеки для успішної діяльності компаній.

Ключові слова: людський капітал, дистанційна праця, кібербезпека, гібридна робоча сила, цифрова економіка

Вступ. За словами Клауса Шваба, засновника та виконавчого голови Всесвітнього економічного форуму, «після років зростаючої нерівності доходів, занепокоєння з приводу переміщення робочих місць, спричиненого технологіями, та зростання суспільного розладу в усьому світі, сукупні потрясіння в галузі охорони здоров'я та економіки 2020 року підштовхнули економіки до вільного падіння, порушили ринки праці та виявили повну неадекватність наших соціальних контрактів. … Настав вирішальний момент: рішення та вибір, які ми робимо сьогодні, визначатимуть життя та існування цілих поколінь. У нашому розпорядженні є інструменти. Щедрість технологічних інновацій, що визначають нашу теперішню епоху, можна використати для розкриття людського потенціалу. У нас є засоби для перепідготовки та підвищення кваліфікації осіб у безпрецедентній кількості, для розгортання точних мереж безпеки та для створення спеціальних карт, які орієнтують втрачаючих роботу працівників на працю завтрашнього дня, де вони зможуть процвітати» [1, 3].

Каталізатором цих процесів стали пандемія і глобальний перехід до дистанційної праці та освіти, що фактично привели людство до «нової норми» існування [2]. Після майже півтора року децентралізованої співпраці багато компаній у всьому світі переглядають своє бачення того, що означає бути «на роботі», що таке «робоче місце», як можна контролювати виробничий процес [3]. Хоча цифрові технології, такі як електронна пошта та смартфони, завжди стирали відмінність між роботою та перебуванням поза офісом, для багатьох «білих комірців» пандемія усунула будь-які розбіжності між домівкою та офісом, породивши нове бачення безпеки життя та діяльності [4].

Постановка проблеми. «*New normal*» теперішніх соціальних і економічних процесів супроводжується високою швидкістю трансформації об'єктів і

засобів виробництва [4], що повинно підвищити ефективність наукових парків як «конвеєрів інновацій» [5, 90]. Як наслідок, прискорилися зміни в економічній діяльності виробників і постачальників [6], вимоги до робочої сили та її кваліфікації [7], що, в свою чергу, прискорило вимоги до дослідницьких робіт та освіти [8], особливо загострivши необхідність навчання/перенавчання протягом життя [9]. Постійно з'являються і набувають нових рис виклики та загрози для інтелектуального капіталу на особистісному, корпоративному та державному рівні у традиційних і мережних формах.

Аналіз останніх досліджень і публікацій. Надзвичайні часи вимагають надзвичайних дій, попит на кваліфікованих і творчих працівників зростає швидше, ніж будь-коли раніше [10]. Згідно з результатами дослідження компанії Gartner багато організацій були змушені під час пандемії керувати розподіленою робочою силою, розкиданою за місцем розташування, яка потерпала від зовнішніх відволікань. Водночас гібридне планування робочої сили надає керівникам відділу кадрів та іншим діловим особам, — а також керівникам та працівникам, — засоби і можливість переосмислити організаційні структури, ролі та проєктування роботи абсолютно новими способами [11]. Цьому сприяє еволюція інформаційно-комунікаційних технологій (ІКТ) [12], у тому числі соціальних мереж [13], які посідають чільне місце в житті та освіті людини. Проте автори багатьох досліджень зауважують, що таке проникнення ІКТ у різні сфери нашого життя породжує нові ризики для працюючого населення [14], у сфері освіти [15] і в цілому впливає на різні аспекти національної безпеки, включаючи інтелектуальну власність [16]. За рекомендаціями дослідників, зниження ризиків при використанні ІКТ може бути досягнуте шляхом використання математичних моделей мереж в управлінні складними системами [17] та прогнозування ефективності навчання здобувачів знань [18].

З огляду на зазначені нові ризики в умовах прискореної цифровізації світової економіки суттєвого значення набуває моніторинг стану кібербезпеки у світі та визначення найбільш вагомих чинників кіберзагроз, що впливають на економічні та соціальні аспекти життя і діяльності людей.

Мета статті. Виконати аналіз чинників кібернебезпек для світової економічної системи, які проявилися за період пандемії та переходу економіки до «нової норми», тобто орієнтації на бізнес-моделі, що використовують розширення цифровізації та використання гібридної робочої сили, є метою цього дослідження.

Результати дослідження. Пандемія та стрибкоподібний перехід до використання дистанційних форм праці та навчання стали надзвичайними подіями у світі в останні два роки. Об'єктивною передумовою для такої зміни соціально-економічних і воєнних рис сьогодення була переорієнтація провідних економік світу (насамперед, США та Китаю) на потужну цифровізацію всіх сфер життя людини та, насамперед, створення нових технологій з орієнтацією на штучний інтелект. Зокрема у США за державної підтримки фінансувалися наукові та прикладні дослідження та освітні проєкти у трьох головних технічних галузях (антропоцентрична комп'ютеризація, інтеграція інформації та інформатика, робастний інтелект) і двох перехресних технічних галузях (взаємодія людей та/або роботів, безпека і захист інформації) [19]. Успішність цієї національної програми підтверджується успіхами США в багатьох сферах за 5 років після закінчення дослідницького етапу у 2016 році. Проте, за словами екс-першого керівника з програмного забезпечення Пентагону Ніколаса Шайлана, «Китай виграв битву зі Сполученими Штатами у сфері штучного інтелекту і рухається до глобального панування через свій технологічний прогрес» [20]. За оцінками західних спецслужб, Китай, друга за величиною економіка світу, протягом десятиліття або близько того, швидше за все, домінуватиме над багатьма ключовими новими технологіями, зокрема штучним інтелектом,

синтетичною біологією та генетикою, і зможе панувати над майбутнім світу, контролюючи все — від медіа до геополітики. Крім того, слід зазначити, що Китай більше інших країн (у т.ч. США) інвестує в передові технології та підготовку висококваліфікованих спеціалістів, особливо з науковим ступенем доктора, що потребує високого рівня володіння цифровими технологіями та забезпечує ефективну адаптацію до будь-яких умов праці, у тому числі гібридних.

Гібридна робоча сила та майбутнє праці. Дистанційна праця та необхідність зміни навіть парадигми організації робочих місць актуалізували нові поняття в управлінні виробництвом: «гібридна робоча сила», «гібридна праця» та «ліквідна робоча сила», які радикально змінюють уявлення щодо організації робочого місця та ставлення до працівників [21]. Керівники все більшої кількості компаній усвідомлюють, що здатність адаптуватися до нових і мінливих умов після кризи буде важливою для успіху, їм доведеться активно реагувати на зміну вподобань та проблем, щоб зберегти свої найкращі таланти, прийняти кращі програми для здоров'я та самопочуття своїх працівників у будь-якому місці, оскільки успіх компаній залежить від їх талантів і благополуччя. Для досягнення успіху на цьому шляху визначилися три значні цілі: 1) створити гібридну роботу, тобто навчитися планувати та організовувати роботу персоналу, який працює частково на формальному робочому місці, а частково — дистанційно; 2) розширити можливості та залучити працівників, де б вони не працювали; 3) керувати та підтримувати планування зайнятості в залежності від завдань і обставин.

Уже зрозуміло, що тенденція щодо гібридних робочих екосистем буде стрімко зростати і до 2025 року фахівці прогнозують світ, що характеризується розсіяною, ліквідною робочою силою з цифровими можливостями. «Робота — це не те, куди ви їдете, а те, чим ви займаєтесь» [21]. При цьому роботодавці повинні максимізувати гнучкість і стійкість робочої сили для подолання майбутніх збоїв та ризиків. Проте розуміння і прийняття моделі гібридної праці ускладнює менеджмент виробничого процесу, виникають не тільки переваги, а й недоліки такої організації праці, причому як для керівника, так і для працівника [22].

Для керівника: 1) більш гнучкі відносини з працівниками, необхідність враховувати їхні конкретні потреби (наприклад, кожен працівник буде відрізнятися «гібридною компетентністю» і потребуватиме різної підтримки від начальника; деяким працівникам у дистанційному режимі може знадобитися допомога в отриманні ресурсів, а іншим може знадобитися відчувати себе більш пов'язаними з групою); 2) підвищена уважність і контроль щодо видимості результатів роботи працівників (не можна покладатися на лише тих співробітників, які разом з керівником в офісі; «дистанційні» менеджери повинні гарантувати, що вони доступні як віддаленим, так і сумісним працівникам, і не повинні втрачати поінформованість щодо людей або завдання, які виконуються віддалено, тому що «менеджери, які працюють далеко від своїх команд, завжди ризикують не знати, що відбувається»).

Для працівника: 1) зниження професійної віддачі може відбутися просто через особливості фізичного доступу до робочого місця (працівники на традиційному робочому місці можуть скористатися всіма ресурсами, наявними в офісі, незалежно від того, ресурси це чи люди; а співробітники в дистанційному режимі можуть зіштовхнутися як з особистими, так і з технічними комунікаціями, що ускладнює демонстрацію їхньої компетентності); 2) видимість результатів самої праці та взаємодії з колегами й іншими учасниками проєкту. «Якщо ви маєте більший доступ до ресурсів і більшу видимість, це робить вас потенційно більш могутньою, впливовою людиною у вашій команді або у вашій робочій групі».

Цифрова економіка має кілька нових аспектів у порівнянні з традиційною. Поява гібридної праці, відповідні зміни у

появі гібридної робочої сили та в організації управління виробництвом є найбільш динамічним складником змін. Проте ще більш швидкі зміни відбуваються в захищеності бізнесу, точніше — у зростанні його вразливості через швидкий розвиток кіберзагроз у цифровому середовищі, яке економіка лише почала активно опановувати, однак ще не встигла створити необхідну систему власного захисту (як це зроблено в середовищі виробництва матеріальних об'єктів, наприклад, фізичний, юридичний та економічний захист). Дистанційна форма роботи породила й нові форми бізнесу — створення та використання кіберзагроз.

Біологічна пандемія та кіберпандемія. Пандемія COVID-19 спровокувала швидкий і масштабний перехід людства до цифрового середовища, у якому загрози благополуччю людини почали еволюціонувати та поширюватися настільки ж активно, як і штами коронавірусу SARS-CoV-2. Проте якщо біологічні хвороби (у попередній історії) відступали навіть після пандемій, то пандемія кібернебезпек може існувати більш тривалий час [23].

Згідно з оцінками Всесвітнього економічного форуму (ВЕФ) виявилося, що у зв'язку зі швидким переходом на віддалену роботу працівники виконують свою професійну діяльність у поспішно зібраних домашніх офісах, не призначених для блокування сучасних загроз безпеці [23]. Дослідження показало, що 95 % фахівців з безпеки стикаються з додатковими проблемами безпеки IT через коронавірус.

Найбільш поширеними проблемами є такі: забезпечення безпечного віддаленого доступу для співробітників (56 %); необхідність використання масштабованих рішень для віддаленого доступу (55 %); працівники в дистанційному режимі знаходять і використовують неперевірене програмне забезпечення, інструменти та послуги (47 %). Такі зміни впливають на ризик організації, тобто на те, наскільки організація піддається кібератакам.

Дотримання попередньої політики безпеки компаній у нову епоху коронавірусу неможливе. Компанії повинні якомога швидше адаптувати свою IT-політику, щоб гарантувати безпеку своїх співробітників. У нещодавньому аналізі «Прогнози ризиків COVID-19: Попереднє зіставлення та його наслідки» Всесвітній економічний форум попереджає: «Ми повинні підготуватися до глобальної кіберпандемії, подібної до COVID-19, яка поширюватиметься швидше і далі, ніж біологічний вірус, з рівнозначним або більшим економічним впливом» [23].

За результатами опитування 350 провідних світових експертів з ризиків, проведеного ВЕФ, найбільшу стурбованість викликають у час розгортання кризи такі три чинники: тривала рецесія глобальної економіки (66,3 % опитаних), сплеск банкрутств як великих, так і малих компаній (52,7 %), кібератаки і втрата даних (50,1 %).

Визначено основні елементи, що впливають на кіберризик організації компанії, які слід урахувати:

1) соціально-інженерні атаки, що використовують страх, невпевненість та сумніви;
2) поверхня атаки (кількість та поширення точок ураження) зростала в геометричній прогресії;
3) співробітник стає «CISO» власного помешкання (CISO, англ. Chief Information Security Officer — керівник відділу IT-безпеки).

Автори дослідження підкреслюють: «Тенденції коронавірусу кардинально змінили нашу роботу, і ці зміни залишаються на місці. Прискорені темпи цифрової трансформації, інфраструктура віддаленого доступу та швидкий перехід до хмари — відомі тенденції дій кіберзлочинців. Коли ми змінюємо спосіб роботи, ми повинні змінити спосіб забезпечення своєї роботи. Стратегії кібербезпеки повинні бути оновлені відповідно до нашої нової реальності» [23]. Насамперед це стосується таких змін роботи компаній, що відбулися за час пандемії: праця з дому, швидкий перехід до використання хмарних технологій, критична інфраструктура, збільшена продуктивність мережі.

Важливою особливістю переходу до дистанційної праці є його усвідомлене по-

зитивне, як правило, сприйняття всіма віковими групами. За даними компанії Perimeter 81, що спеціалізується на питаннях кіберзахисту, не тільки молодь (вікова група 18–34 роки) віддає перевагу дистанційній формі праці (70 % опитаних), а й старше покоління (45–60 років) переважно вважає таку форму покращенням балансу «праця – життя» (51 %) [24]. У результаті такого переходу компанії вказують на зменшення часу перебування своїх працівників на лікарняному на 13 %, що дасть змогу компаніям США заощадити до 2030 року понад 4,5 млрд дол. і зменшити плинність кадрів на 10 %.

Ураховуючи зазначені тенденції, бізнес вкладає значні кошти у вирішення питань безпеки. За прогнозами дослідницького та консультативного гіганта компанії Gartner, світові витрати на безпеку та управління ризиками у 2021 році перевищать 150 млрд дол., причому майже половина загальної суми (приблизно 72 млрд дол.) буде витрачена на послуги безпеки, включаючи консультації, технічну підтримку та послуги з упровадження та аутсорсингу. Значні кошти також будуть вкладені в захист інфраструктури (24 млрд), обладнання для захисту мережі (17 млрд) та управління доступом до ідентифікаційних даних (14 млрд) [25]. Компанія вважає, що слід очікувати найбільший приріст витрат на хмарну безпеку (41,2 % порівняно з 2020 р.), яку вона назвала «найменшим, але найшвидшим сегментом ринку».

Чинники кіберзагроз для бізнесу. Нове дослідження NortonLifeLock показало, що майже 330 млн людей у 10 країнах стали жертвами кіберзлочинності за останні 12 місяців, витративши 2,7 млрд годин на боротьбу з наслідками, а понад 55 млн людей стали жертвами крадіжки особистих даних [26].

Зважаючи на те що наразі організації повинні забезпечувати швидкий і безпечний доступ своїх працівників до корпоративних ресурсів, забезпечення захисту своїх мереж, бізнес-даних і персональних даних працівників стає їх усе важливішим завданням, особливо з огляду на перенесення бізнес-діяльності у хмари. За оцінками компанії Perimeter 81, понад 84 % компаній пов'язують хоча б одну критичну функцію діяльності з хмарними сервісами, а 58 % використовують гібридні хмарні моделі [24]. Відповідної уваги потребують пов'язані з цим ризики, хоча самі хмарні технології частково вирішують і ці питання.

Спільне дослідження компаній Fidelis Cybersecurity Company та Security Insiders встановило, що у 2021 році 95 % компаній приділяють увагу безпеці бізнесу у хмарах [27], причому найбільшу стурбованість викликають такі ризики: небезпечний інтерфейс (54 %), неавторизований доступ (52 %) і зовнішній обмін даними (44 %). Серед чинників платформ хмарної безпеки індустріальні лідери на перше місце ставлять ефективність витрат (66 %), визначаючи таким чином важливість і необхідність збалансованого прийняття рішень з цих питань.

Варто визнати, що наведені дані вказують на значні витрати компаній на захист свого бізнесу на організаційному та виконавчому рівнях, розуміючи, що кібербезпека стала не додатковими видатками для виробництва, а безпосереднім складником самого бізнесу, суттєво впливаючи на макро- та мікроекономічні показники. Відповідно, діяльність з питань кіберзахисту та кібербезпеки сформувалась як самостійний вид економічної діяльності і цей факт є природним, оскільки будь-яка діяльність (економічна, соціальна, воєнна тощо) переміщується з середовища матеріальних об'єктів у середовище інформаційне, яке реалізується на сьогодні у кіберпросторі, цифрових мережах, де тільки починається розгалуження економічної діяльності за сферами, специфічними для цифрового середовища.

Наразі безпека мереж складається з таких чинників:

1) перехід від периметр-центричних засобів безпеки до користувач-центричних;
2) безпечна мережа як сервіс;

3) підхід, що базується на «дружніх» хмарах (за аналогією з дружнім інтерфейсом);
4) 2- або 3-рівнева аутентифікація;
5) урахування підходу BYOD (Bring You Own Device);
6) легка адаптація до IT;
7) бездоганний логін;
8) безагентне віддалене робоче місце.

Безмовно, найбільш важливим нині стало правило безпеки Zero Trust («нульова довіра»), тобто модель безпеки, розроблена колишнім аналітиком Forrester Джоном Кіндервагеном у 2010 році, що стала найбільш популярною концепцією у сфері кібербезпеки, оскільки практика довела, що довіри не може бути нікому, жодній програмній розробці.

Висновки і подальші перспективи дослідження. Цифровізація всіх сфер діяльності людини веде до зміни сутності та форм бізнес-діяльності, впливаючи як на організацію виробничих процесів, так і на розвиток робочої сили. Розширення економічних процесів на цифрове середовище викликало появу нових загроз для бізнесу та окремих людей. Кібербезпека змінила статус додаткових видатків виробництва на безпосередній складник бізнесу, суттєво впливаючи на макро- та мікроекономічні показники підприємства. Відповідно, діяльність з питань кіберзахисту та кібербезпеки сформувалась як самостійний вид економічної діяльності і цей факт є природним, оскільки будь-яка діяльність (економічна, соціальна, воєнна тощо) переміщується з середовища матеріальних об'єктів у середовище інформаційне, яке реалізується на сьогодні у кіберпросторі, у цифрових мережах.

Подальші дослідження потребують моніторингу стану кібербезпеки віддаленої праці, у тому числі із застосуванням систем штучного інтелекту, який пропонують використовувати і для виявлення кіберзагроз, але він і сам використовується все ширше як засіб для кіберзлочинів і діяльність якого слід ураховувати як можливе джерело загроз [28].

Список використаних джерел / List of references

1. *Schwab K., Zahidi S. The Future of Jobs Report, October 2020. 2020 World Economic Forum. 163 pp. URL: www.weforum.org.*
2. *Manavi J. The Next Normal: Building resilience in the post-COVID-19 workspace. Observer research foundation. Oct 20. 2020. URL: https://www.orfonline.org/expert-speak/next-normal-building-resilience-post-covid19-workspace.*
3. *Shaping the Future of Digital Economy and New Value Creation. 2020 World Economic Forum. URL: https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation.*
4. *Resetting the Future of Work Agenda: Disruption and Renewal in a Post-COVID World. WHITE PAPER, October 2020. 2020 World Economic Forum. URL:http://www3.weforum.org/docs/WEF_NES_Resetting_FOW_Agenda_2020.pdf.*
5. *Бутнік-Сіверський О. Б. Економіко-правові перспективи активізації діяльності наукових парків на шляху до неоекономіки. Теорія і практика інтелектуальної власності. 2020. № 3. 82–96.*
6. *Javed N. Future Economy: Upskilling Exporters & Reskilling Manufacturers. Modern Diplomacy. October 18. 2020. URL: https://moderndiplomacy.eu/2020/10/18 /future-economy-upskilling-exporters-reskilling-manufacturers/*
7. *Gratton L. An Emerging Landscape of Skills for All. MIT Sloan Management Review. March 08, 2021. URL:https://sloanreview.mit.edu/article/an-emerging-landscape-of-skills-for-all.*
8. *Kozák, S., Ružický, E., Štefanovič, J., & Schindler, F. Research and education for industry 4.0: Present development. Cybernetics & Informatics (K&I). 2018. P.1–8.*

9. *Kim Jinyoung and Park Cyn-Young: Education, Skill Training, and Lifelong Learning in the Era of Technological Revolution. Asian Development Bank Economics Working Paper Series. # 606, (January 2020).*
10. *Jesuthasan R., Chan Q. What talent means in the post-COVID-19 workplace. World Economic Forum. URL: https://www.weforum.org/agenda/2020/08/work-talent-human-capital-covid-19.*
11. *Wiles J. Hybrid Workforce Models Speed Digital Transformation. 2020. https://www.gartner.com/smarterwithgartner/hybrid-workforce-models-speed-digital-transformation.*
12. *Burov O., Bykov V., Lytvynova S. ICT evolution: from single computational tasks to modeling of life. In: Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications, Integration, Harmonization and Knowledge Transfer, Vol-2393, 2020, pp. 170-177. http://ceur-ws.org/Vol-2393/paper_353.pdf.*
13. *Lytvynova S., Burov O. Methods, forms and safety of learning in corporate social networks. ICTERI 2017 - Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer".- CEUR-WS.-2017.-V.1844.-406-413.*
14. *Vigliarolo B. Employees new to working remotely are a security risk. Security, June 22, 2020. URL: https://www.techrepublic.com/article/employees-new-to-working-remotely-are-a-security-risk.*
15. *Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019. 2(70). С. 313–331. URL:https://journal.iitta.gov.ua/index.php/itlt/article/view/2876 (https://doi.org/10.33407/itlt.v70i2.2876).*
16. *Зайківський О., Оністрат О. Система національної безпеки та питання інтелектуальної власності. Теорія і практика інтелектуальної власності. 2021. № 3. 39–47.*
17. *Lavrov, E., Pasko, N., Siryk, O., Burov, O., Natalia, M. Mathematical Models for Reducing Functional Networks to Ensure the Reliability and Cybersecurity of Ergatic Control Systems. Proceedings - 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2020, 2020, pp. 179–184.*
18. *Spirin O., Burov O. Models and applied tools for prediction of student ability to effective learning. 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. CEUR-WS. 2018. V. 2104. 404–411.*
19. *Буров О. Ю. Технології й інновації в діяльності людини ери інформації: людина та ІКТ. Інформаційні технології і засоби навчання. 2015. № 6 (50). С. 1–13.*
20. *"China has won AI battle with U.S., Pentagon's ex-software chief says". Reuters. - October 12, 2021. https://www.reuters.com/technology/united-states-has-lost-ai-battle-china-pentagons-ex-software-chief-says-2021-10-11/?utm_source=sfmc&utm_medium=email&utm_campaign=2759998_Agenda_weekly-15October2021&utm_term=&emailType=Agenda%20Weekly.*
21. *Puybaraud M. Could 'hybrid working' usher in a golden age for workers? 2021 World Economic Forum. https://www.weforum.org/agenda/2021/01/hybrid-working-golden-age-of-the-worker.*
22. *Are you ready for hybrid workplaces? 2021 World Economic Forum. URL: https://knowledge.wharton.upenn.edu/article/are-you-ready-for-the-hybrid-workplace.*
23. *Sagey M. Remote work carries massive cyber risks. These top IT tips can help keep your workers secure. 2021 World Economic Forum. URL: https://www.weforum.org/agenda/2020/09/remote-work-cyber-risks-top-it-tips-keep-your-workers-secure.*

24. *The Rise of Remote Workers: A Checklist for Securing Your Network. URL: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/2020/Perimeter81_RemoteAccessChecklist_Showcase.pdf.*
25. *Kovacs E. Gartner: Global Security Spending Will Reach $150 Billion in 2021. SecurityWeek. 25.05.2021. URL: https://www.securityweek.com/gartner-global-security-spending-will-reach-150-billion-2021.*
26. *2021 Norton Cyber Safety Insights Report. https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report.*
27. *2021 AWS Cloud Security Report. https://connect.fidelissecurity.com/rs/884-ZRZ-648/images/2021-AWS-Security-Report-CloudPassage-Final.pdf?mkt_tok=ODg0LVpSWi02NDgAAAGAKIUMbWC6Vd1WHctdFLm5fSnZNg9rQlroP_zZsDK2IDYsjQ7RGZEYwibqq9aCsWN7f6LFaiISy2hs93ogEgiY4JpnKagJfBxVuaqq8uS-ycO.*
28. *Андрощук Г. Штучний інтелект: економіка, інтелектуальна власність, загрози. Теорія і практика інтелектуальної власності. 2021. № 2. С. 56–74. DOI: https://doi.org/10.33731/22021.236555.*

1. *Schwab K., Zahidi S. The Future of Jobs Report, October 2020. 2020 World Economic Forum. 163 pp. URL: www.weforum.org.*
2. *Manavi J. The Next Normal: Building resilience in the post-COVID-19 workspace. Observer research foundation. Oct 20. 2020. URL: https://www.orfonline.org/expert-speak/next-normal-building-resilience-post-covid19-workspace.*
3. *Shaping the Future of Digital Economy and New Value Creation. 2020 World Economic Forum. URL: https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation.*
4. *Resetting the Future of Work Agenda: Disruption and Renewal in a Post-COVID World. WHITE PAPER, October 2020. 2020 World Economic Forum. URL:http://www3.weforum.org/docs/WEF_NES_Resetting_FOW_Agenda_2020.pdf.*
5. *Butnik-Siverskyi O. B. Ekonomiko-pravovi perspektyvy aktyvizatsii diialnosti naukovykh parkiv na shliakhu do neoekonomiky. Teoriia i praktyka intelektualnoi vlasnosti. 2020. № 3. 82–96.*
6. *Javed N. Future Economy: Upskilling Exporters & Reskilling Manufacturers. Modern Diplomacy. October 18. 2020. URL: https://moderndiplomacy.eu/2020/10/18 /future-economy-upskilling-exporters-reskilling-manufacturers/*
7. *Gratton L. An Emerging Landscape of Skills for All. MIT Sloan Management Review. March 08, 2021. URL:https://sloanreview.mit.edu/article/an-emerging-landscape-of-skills-for-all.*
8. *Kozák, S., Ružický, E., Štefanovič, J., & Schindler, F. Research and education for industry 4.0: Present development. Cybernetics & Informatics (K&I). 2018. P.1–8.*
9. *Kim Jinyoung and Park Cyn-Young: Education, Skill Training, and Lifelong Learning in the Era of Technological Revolution. Asian Development Bank Economics Working Paper Series. # 606, (January 2020).*
10. *Jesuthasan R., Chan Q. What talent means in the post-COVID-19 workplace. World Economic Forum. URL: https://www.weforum.org/agenda/2020/08/work-talent-human-capital-covid-19.*
11. *Wiles J. Hybrid Workforce Models Speed Digital Transformation. 2020. https://www.gartner.com/smarterwithgartner/hybrid-workforce-models-speed-digital-transformation.*
12. *Burov O., Bykov V., Lytvynova S. ICT evolution: from single computational tasks to modeling of life. In: Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications, Integration, Harmonization and Knowledge Transfer, Vol-2393, 2020, pp. 170-177. http://ceur-ws.org/Vol-2393/paper_353.pdf.*

13. *Lytvynova S., Burov O. Methods, forms and safety of learning in corporate social networks. ICTERI 2017 - Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. CEUR-WS.2017. V. 1844. 406–413.*
14. *Vigliarolo B. Employees new to working remotely are a security risk. Security, June 22, 2020. URL: https://www.techrepublic.com/article/employees-new-to-working-remotely-are-a-security-risk.*
15. *Bykov V. Yu., Burov O. Yu., Dementiievska N. P. Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi. Informatsiini tekhnolohii i zasoby navchannia. 2019. 2(70). S. 313–331. URL:https://journal.iitta.gov.ua/index.php/itlt/article/view/2876 (https://doi.org/10.33407/itlt.v70i2.2876).*
16. *Zaikivskyi O., Onistrat O. Systema natsionalnoi bezpeky ta pytannia intelektualnoi vlasnosti. Teoriia i praktyka intelektualnoi vlasnosti. 2021. № 3. 39–47.*
17. *Lavrov, E., Pasko, N., Siryk, O., Burov, O., Natalia, M. Mathematical Models for Reducing Functional Networks to Ensure the Reliability and Cybersecurity of Ergatic Control Systems. Proceedings - 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2020, 2020, pp. 179–184.*
18. *Spirin O., Burov O. Models and applied tools for prediction of student ability to effective learning. 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. CEUR-WS. 2018. V. 2104. 404–411.*
19. *Burov O. Yu. Tekhnolohii y innovatsii v diialnosti liudyny ery informatsii: liudyna ta IKT. Informatsiini tekhnolohii i zasoby navchannia. 2015. № 6 (50). S. 1–13.*
20. *"China has won AI battle with U.S., Pentagons ex-software chief says". Reuters. - October 12, 2021. https://www.reuters.com/technology/united-states-has-lost-ai-battle-china-pentagons-ex-software-chief-says-2021-10-11/?utm_source=sfmc&utm_medium=email&utm_campaign=2759998_Agenda_weekly-15October2021&utm_term=&emailType=Agenda%20Weekly.*
21. *Puybaraud M. Could hybrid working usher in a golden age for workers? 2021 World Economic Forum. https://www.weforum.org/agenda/2021/01/hybrid-working-golden-age-of-the-worker.*
22. *Are you ready for hybrid workplaces? 2021 World Economic Forum. URL: https://knowledge.wharton.upenn.edu/article/are-you-ready-for-the-hybrid-workplace.*
23. *Sagey M. Remote work carries massive cyber risks. These top IT tips can help keep your workers secure. 2021 World Economic Forum. URL: https://www.weforum.org/agenda/2020/09/remote-work-cyber-risks-top-it-tips-keep-your-workers-secure.*
24. *The Rise of Remote Workers: A Checklist for Securing Your Network. URL: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/2020/Perimeter81_RemoteAccessChecklist_Showcase.pdf.*
25. *Kovacs E. Gartner: Global Security Spending Will Reach $150 Billion in 2021. SecurityWeek. 25.05.2021. URL: https://www.securityweek.com/gartner-global-security-spending-will-reach-150-billion-2021.*
26. *2021 Norton Cyber Safety Insights Report. https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report.*
27. *2021 AWS Cloud Security Report. https://connect.fidelissecurity.com/rs/884-ZRZ-648/images/2021-AWS-Security-Report-CloudPassage-Final.pdf?mkt_tok=ODg0LVpSWi02NDgAAAGAKIUMbWC6Vd1WHctdFLm5fSnZNg9rQlroP_zZsDK2IDYsjQ7RGZEYwibqq9aCsWN7f6LFaiISy2hs93ogEgiY4JpnKagJfBxVuaqq8uS-ycO.*
28. *Androshchuk H. Shtuchnyi intelekt: ekonomika, intelektualna vlasnist, zahrozy. Teoriia i praktyka intelektualnoi vlasnosti. 2021. № 2. S. 56–74.*

DOI: https://doi.org/10.33731/22021.236555.

Надійшла до редакції 21.09.2021 року

Буров А. Влияние киберпреступности на цифровую экономику. В статье проведен анализ таких факторов киберрисков для мировой экономической системы: цифровизация и новые условия труда, использование гибридной рабочей силы, влияние киберпандемии на изменения в экономике, факторы киберугроз для бизнеса. Обоснованы преимущества и недостатки гибридной рабочей экосистемы. Проанализированы факторы возникновения киберпандемии. Выделены наиболее значимые факторы кибербезопасности для успешной деятельности компаний.

Ключевые слова: человеческий капитал, дистанционная работа, кибербезопасность, гибридная рабочая сила, цифровая экономика

Burov O. The impact of cybercrime on the digital economy. The article considers factors of cyber hazards for the world economic system that appeared during the pandemic COVID-19, as well as transition of the economy to the «new normal», in the context of digitalization in the following aspects: digitalization and new working conditions, use of hybrid work, biological pandemic and cyber-pandemic and their influence on changes in the economy, factors of cyber threats to business. It is highlighted that the pandemic and the abrupt transition to the use of remote forms of work have become extraordinary events in the world over the past two years. The objective precondition for such a change in the socio-economic and military features was the reorientation of the world's leading economies (primarily the United States and China) to the powerful digitalization of all spheres of human life and, above all, the creation of new technologies. It is noted that China invests more than other countries (including the United States) in advanced technology and training of highly qualified specialists, especially with a doctor degree that requires a high level of digital technology and appropriate literacy, and provides effective adaptation to any working conditions including hybrid.

The emergence of a hybrid working ecosystem and hybrid workforce is analysed, as well as their advantages and disadvantages are substantiated. It is noted that the digital economy has several new aspects compared to the traditional one. The emergence of hybrid work, the corresponding changes in the emergence of hybrid workforce and in the organization of production management are the most dynamic components of change. However, even faster changes are taking place in the security of business, more precisely — in the growth of its vulnerability due to the rapid development of cyber threats in the digital environment, which the economy has only begun to actively master, but has not yet created the necessary system of self-defence. Remote form of work has given rise to new forms of business — the creation and use of cyber threats. The emergence of a cyber-pandemic as a result of rapid digitization due to the COVID-19 pandemic and the transition of labour to remote form is analysed. The most important factors of cybersecurity for the successful operation of companies are highlighted.

Keywords: human capital, remote work, cybersecurity, hybrid workforce, digital economics