**УДК [(174.4+177.9):334.012.23]:(004.9+004.855)**

# АКТУАЛЬНІ ПРОБЛЕМИ ЦИФРОВОЇ ЕТИКИ БІЗНЕСУ

***Компанієць В.В., д.е.н., професор, (ХГУ НУА),***
***Крацер В.В., к.е.н., програміст (ТОВ «ГлобалЛоджик Україна»)***

*В статті наведено визначення сутності цифрової етики бізнесу, основних етичних дилем, проведено системний аналіз проблем та напрямів забезпечення цифрової етики бізнесу на платформі парадигми духовно-моральної та соціокультурної детермінації соціально-економічного розвитку. Розглянуто європейський досвід забезпечення цифрової етики економічних відносин, європейську та вітчизняну законодавчу базу у сфері захисту персональних даних. Висвітлено результати досліджень світових компаній у контексті глобальної кризи довіри до збирачів персональних даних, а також у напрямі забезпечення цифрової відповідальності бізнесу.*

*Сформовано рекомендації щодо посилення захисту прав людини в кіберпросторі та впровадження в освітянський простір та економічну практику етики економічних відносин та бізнесу в умовах цифровізації.*

***Ключові слова: цифрова економіка, цифрова етика, штучний інтелект, інтернет поведінки, кіберзагрози, захист персональних даних, права людини, конфіденційність, освіта.***

# ACTUAL PROBLEMS OF THE DIGITAL ETHICS OF BUSINESS

***Kompaniets V.V., Doctor of Economics, professor (Kharkiv Humanitarian University "People's Ukrainian Academy"),***
***Kratser V.V., Ph.D., Software Engineer (GlobalLogic Ukraine LLC)***

*New generation technologies (NBICS-technologies), which are based on digital technologies, give humanity new perspectives. They also pose huge problems and threats. In particular, there is an opportunity to use such technologies and arrays of personal data for selfish, destructive purposes to achieve profits or power and manage people's behaviour.*

*Another threat and problem is the significant gap in the assessment of the admissibility of the development of new technologies in terms of morality and law. As one of the answers to these threats and problems in the European scientific space, a separate area dedicated to digital ethics has been formed - business ethics.*

*In the article, the authors define the essence of digital business ethics and the main ethical dilemmas. The authors make a systematic analysis of the problems and directions of ensuring digital business ethics on the platform of the paradigm of spiritual, moral and socio-cultural determination of socio-economic development. The authors consider the European experience in ensuring digital ethics of economic relations, the European and domestic legal framework in the field of personal data protection and present the results of research of global companies in the context of the global crisis of trust in collectors of personal data, as well as in the direction of ensuring digital business responsibility. The authors provide recommendations for strengthening the protection of human rights in cyberspace and introducing the ethics of economic relations and business in the context of digitalization into the educational space and economic practice.*

*In conclusion, digital ethics has become a meeting place for the interests of various economic actors - the state, supranational government, large companies (especially high-tech), politicians*

*and ordinary consumers, so there is a threat of lobbying each of the strengths of its "beneficial digital ethics". In these conditions, it is difficult, but necessary to create a digital ethics of economics (business) and focused on the preservation of traditional values, and the tradition of humanism.*

***Key words: digital economy, digital ethics, artificial intelligence, internet of behaviour, cyber threats, personal data protection, human rights, privacy, education.***

**Постановка проблеми.** Функціонування соціально-економічних систем усіх рівнів сьогодні відбувається в умовах цифрової трансформації. Технології нового покоління (насамперед NBICS-технології), основою яких є цифрові, дають людству нові перспективи і, разом з тим, породжують величезні, досі небачені проблеми і загрози. Зокрема, виникла можливість використання таких технологій, а також масивів особистих даних в корисливих, руйнівних цілях для досягнення надприбутку або влади, управління поведінкою людей.

Іншою, одночасно і загрозою, і проблемою стало значне відставання оцінки допустимості розвитку нових технологій з точки зору норм моралі і розробки норм права. Як одна з відповідей на ці загрози і проблеми в європейському науковому просторі сформувався окремий напрямок, присвячений *цифровій етиці, в т.ч. етиці бізнесу*.

*Процес цифровізації бізнесу в усьому світі, в т.ч. в Україні, значно прискорили, події, пов'язані з глобальною короно-кризою і масовим вимушеним переходом безлічі компаній в цифрове середовище. Це актуалізувало дослідження в області цифрової етики для вітчизняних вчених і представників бізнесу.*

**Аналіз останніх досліджень і публікацій. Виділення невирішених частин загальної проблеми.** Потрібно відзначити, що в Європі проблеми, пов'язані із забезпеченням цифрової етики економічних відносин розглядаються вже кілька років і досить активно. Вітчизняні вчені даною проблемою поки не цікавилися. Публікацій вітчизняних вчених, присвячених питанням цифровізації економіки і бізнесу, досить багато, але вони не мають зв’язків із етичними проблемами. Серед них можна виділити роботи Кіндзерського Ю., Шраменко О., Пантєлєєвої Н., Романовської Л. та ін. [1, 3]. В окремому циклі статей розглядаються етичні і правові питання забезпечення безпеки особистості в Інтернет-просторі, зокрема, це публікації Войтович О., Ткаченко О., Карпенко Ю., Хрущ С. [4-8] , але вони не пов'язані з економікою і бізнесом.

Тому в межах цієї публікації ми будемо звертатися до робіт найбільш відомих зарубіжних професіоналів в даній області, зокрема Грі Хассельбалч і Пернілль Транбе, Френка Байтендейк, Дейва Ярдлі та ін. [9-17], доповнюючи їх дослідженнями, проведеними світовою аудиторською компанією PwC, Всесвітньою незалежною мережею з маркетингових досліджень і опитувань громадської думки (WIN), а також глобальною торговою асоціацією для галузі даних та аналізу (ESOMAR) [18-21]. *При цьому усі зазначені та інші, використані при підготовці публікації матеріали, ми будемо аналізувати на платформі парадигми духовно-моральної та соціокультурної детермінації соціально-економічного розвитку в межах якої працюють автори.*

**Метою нашої публікації** буде: *визначення сутності цифрової етики бізнесу та її основних напрямів; якісний системний аналіз основних проблем цифрової етики та деяких напрямів її забезпечення на платформі парадигми духовно-моральної та соціокультурної детермінації соціально-економічного розвитку. Також ми з’ясуємо, які первинні кроки зроблені в українському науково-освітньому просторі, що можливо хоча б опосередковано використовувати для певного поштовху в розвитку науково-*

*освітнього і практико-орієнтованого напряму «цифрова етика бізнесу» в Україні.*

**Виклад основного матеріалу.** В останні роки в розвинених країнах Заходу спостерігається процес активного використання різних даних про населення в комерційних і політичних цілях. Виникли навіть такі поняття як *«економіка даних» або «платформний капіталізм»* Загальна суть цих двох понять зводиться до того, що *головним «фактором виробництва», який дозволяє забезпечувати економічне зростання і прибуток в умовах цифровізації, стають дані про населення (групи населення) як потенційних покупців*. Такі «великі дані» обробляються за допомогою певних методів, а результати аналізу використовуються власниками або замовниками такої аналітики для управління поведінкою покупців і обігравання конкурентів. *Зрозуміло, що і сам збір конфіденційної інформації про людину, і спроба управляти її поведінкою на основі цього, викликає багато суперечок і в області права, і в області етики.*

*Та й самі люди, які активно «живуть в цифровому світі» і залишають в ньому свої «цифрові сліди», останнім часом дуже стривожені можливістю використання даних про них в корисливих цілях.*

Це доводить, опитування понад 25 тис. осіб у 40 країнах світу, проведене у липні 2020 року Всесвітньою незалежною мережею з маркетингових досліджень і опитувань громадської думки (WIN), а також глобальною торговою асоціацією для галузі даних та аналізу (ESOMAR) [21]. Воно, зокрема показує, що 7 з 10 опитаних у всьому світі стурбовані обміном особистою інформацією, при цьому двом третинам опитаних не подобається поточна практика використання конфіденційної інформації, що демонструється більшістю збирачів даних.

Понад дві третини опитаних розуміють, що їх особиста інформація цінна для збирачів даних (і, підкреслимо, що вона використовується в бізнес, чи в політичних цілях), це особливо усвідомлюють в Європі (74% опитуваних) та в Азіатсько-Тихоокеанському регіоні (75%). При цьому менше половини опитаних в світі і менше третини у Латинській Америці та США, вважають надання особистої інформації життєво важливою і необхідною процедурою. Тобто, багато опитуваних упевнені у тому, що збір даних є однобічною угодою: це цінно для бізнесу, але в цілому не потрібно. Цей крах довіри між громадськістю та компаніями, коли йдеться про збір даних, найімовірніше, випливає з широкого негативного досвіду зловживання даними (спам, фішинг, зловживання електронною поштою, надокучлива контекстна реклама, витік особистих даних або злом банківського рахунку / кредитної картки).

У Північній Америці, Латинській Америці, Європі та країнах Близького (Середнього) Сходу та Північної Африки *менше половини споживачів знають про те, що відбувається з їхньою особистою інформацією після того, як вони поділилися нею зі збирачем даних.*

*До того ж більше половини населення світу стало жертвою зловживання даними.* В Європі це більше двох третин, в Латинській Америці та Африці жертвами стали приблизно три з п'яти осіб, тоді як у Північній Америці жертвами певного зловживання даними стало 80% населення.

Результати цього опитування – це один з багатьох доказів необхідності ретельного вивчення основних проблем етики економічних відносин та бізнесу в умовах цифровізації.

*Як же розуміють цифрову етику в європейському науковому просторі?* Єдиного визначення не існує. На нашу думку, досить ємко сутність цього поняття висловила *Грі Хассельбалч* - незалежний старший науковий співробітник і радник з

етики даних і штучного інтелекту (ШІ), прав людини, співавтор першого системного Європейського дослідження в області етики даних. На її думку *«цифрова етика» - це етичне управління наслідками цифрових розробок для людини і суспільства* [10].

На наш погляд, *більш розгорнуто економічну етику в т. ч. етику бізнесу в цифровому середовищі (скорочено - «цифрову етику») можна визначити як* мультидисциплінарну, інтегровану галузь науки і практики соціально-економічних відносин, яка, аналізує, створює і використовує інструменти і механізм прийняття суб'єктами економічної діяльності морально виправданих рішень, а також моделі поведінки осіб, які приймають рішення, в умовах роботи в цифровому середовищі, з цифровими даними і новітніми технологіями.

*В європейському просторі можна виділити три головних напрями цифрової етики:*

- *етика даних*, яка вивчає питання дослідження та забезпечення етики та прав людини в цифровому просторі, зокрема, збереження конфіденційності інформації та використання цифрових даних поза межами прав та етичних принципів;

- *етика використання штучного інтелекту* (ШІ), яка стосується питань дослідження та забезпечення етики та прав людини в умовах застосування новітніх технологій (ШІ), вивчає питання меж та наслідків їх використання для людини, суспільства, економіки;

- *цифрова етика ведення бізнесу і цифрової трансформації*, яка стосується безпосередньо компаній (організацій), у т.ч. поведінки так званих цифрових монополій.

Зрозуміло, що *цей науково-практичний напрям є складним і синтетичним* за своєю природою, адже стосується широкого кола *етичних, правових, суспільно-економічних, технологічних питань і знань* у відповідних галузях.

Одна із важливих *проблем і практичних завдань цифрової етики* - це виявлення *окремих дилем з якими стикається особа, що приймає бізнес-рішення в цифровому середовищі або з використанням інструментів ШІ.*

Підприємці та менеджери, що діють в рамках ринкової моделі економіки, приймаючи рішення, завжди керувалися не тільки прагненням до прибутковості, а й певними етичними нормами. І цілком закономірно, що реалії роботи в цифровому середовищі з новими технологіями, великими масивами конфіденційної інформації (даними), сформували нові варіації дилеми «мораль або прибуток», з якими зіткнулися представники бізнесу. *Ці дилеми в соціокультурному плані універсальні і тому важливі для розуміння вітчизняним бізнесом, який можливо поки не стикався з необхідністю їх вирішення.*

*Френк Байтендейк*, віце-президент і аналітик компанії *Gartner*, виходячи з аналізу практики функціонування безлічі компаній, вказує на *чотири етичні дилеми, що виникають у бізнесу в умовах цифровізації* [14]. Сформулюємо їх розгорнуто, в авторській редакції.

*Перша: «конфіденційність або прибуток».*

Деякі компанії, наприклад, компанії громадського транспорту, отримуючи з метою збільшення свого прибутку і поліпшення обслуговування клієнтів певну особисту інформацію про них, можуть продавати ці дані третім особам. Чи є це етичним? Очевидно - ні, оскільки дані повинні використовуватися тільки для заявленої мети (подорожі).

*Друга: «отримувати поточну вигоду і ігнорувати можливості неетичного використання або зробити правильно і забезпечити постійний моніторинг продукту (технології ШІ)».*

Багато хто мав досвід у використанні таких цифрових помічників як Siri, Cortana або Google Now. Ця

технологія, як і інші, можуть бути використані не за призначенням (аморальним чином, в аморальному контексті)

Будь-які технології штучного інтелекту (ШІ) можуть бути недосконалими з точки зору можливості їх неетичного використання з метою отримання вигоди. У цьому випадку величезна відповідальність стосується виробників таких технологій і відповідних продуктів. Тому вони повинні подбати про те, щоб не тільки виконати поточне тестування технології, але і вбудувати програми, які дозволять постійно контролювати ШІ на предмет непередбачених наслідків.

*Третя: «передбачити можливі порушення конфіденційності інформації про споживача при проектуванні продукту і забезпечити захист даних або ігнорувати і отримувати поточну вигоду».*

Смарт-телевізори зазвичай відстежують поведінку телеглядачів при перегляді і відправляють інформацію про неї виробнику для персоналізації реклами. В європейській практиці були випадки, коли відбувались відправки конфіденційних даних з особистих файлів на USB-накопичувачах, підключених до телевізора. Використання такої інформації є юридично неприйнятним і може завдати репутаційної шкоди виробнику. Проблема полягає в більш якісному проектуванні програмного забезпечення, в процесі якого будуть зіставлятися питання конфіденційності з необхідністю майбутніх функцій пристрою.

*Четверта: «забезпечувати колективну відповідальність учасників виробництва та забезпечення функціонування «розумних машин» або уникати відповідальності за наслідки рішень, прийнятих «ШІ - розумними машинами»».*

На нашу думку, це одна з найбільш складно вирішуваних позитивно дилем. Сучасні «розумні машини «можуть приймати» самостійні рішення», які можуть привести до негативних наслідків, навіть до смертного результату. До таких машин можна віднести, наприклад, військові дрони або безпілотні автомобілі. Хто несе відповідальність за наслідки таких рішень: програміст, виробник або оператор? Зрозуміло, що всі учасники виробництва та забезпечення функціонування «розумних машин» несуть певну відповідальність. І їх обов'язок полягає в забезпеченні ретельного тестування і постійного моніторингу непередбачених результатів. Але питання реалізації колективної відповідальності в юридичній практиці досить складне.

*Як ми зазначали, всі ці чотири дилеми за своєю внутрішньою суттю зводяться до однієї «мораль або прибуток».* Якісне проектування і тестування технологій, їх постійний моніторинг і доведення – вимагають значних ресурсів, в т.ч. часу. Цього ж потребує навчання кадрів та залучення талановитих і свідомих фахівців. *Однак сучасні виробники, особливо в умовах наростання конкуренції, прагнуть до швидких результатів і не хочуть вкладати додаткові кошти в забезпечення більш якісного проектування систем ШІ. Тим більше, що багато юридичних питань регулювання систем ШІ залишаються відкритими.*

У цих умовах найбільш значущий збиток, який можуть отримати компанії, що вибирають «прибуток», це збиток репутаційний. І навпаки, *дотримуючись етики бізнесу в цифровому середовищі*, перш за все етики даних, як справедливо стверджують Грі Хассельбалч і Перніль Транбе, *компанії можуть отримати нову конкурентну перевагу* [11]. І до цього питання ми ще повернемося.

В цілому, аналізуючи проблематику європейських публікацій в області цифрової етики економіки (бізнесу) [9-17], і доповнюючи їх авторським поглядом *на платформі парадигми духовно-моральної та*

*соціокультурної детермінації соціально-економічного розвитку*, *ми прийшли до певних висновків щодо актуальних проблем цифрової етики бізнесу*, деякі з яких прокоментуємо.

*Перше - перераховані дилеми в умовах глобалізації стають актуальними для бізнесу незалежно від його географічного місця розташування, але реакція на дилеми і їх рішення багато в чому залежить від «культурного поля»* - на нашу думку, від ступеня прихильності традиційним цінностям і населення, і бізнесу, і осіб, які приймають рішення.

Друге - незважаючи на відмінності в сприйнятті і вирішенні дилем, які детерміновані «культурним полем», *існує кілька універсальних рекомендацій, якими можуть скористатися при бажанні, особи, які приймають рішення в сфері бізнесу та економіки в цифровому середовищі. Перш за все, це використання золотого правила моралі.*

*До речі, в авторському підручнику «Моральні основи економіки та підприємницької діяльності»* [22]*, на основі багатьох досліджень, ми довели, що рішення дилеми «мораль або прибуток» у користь морального вибору завжди залежало від соціокультурних, інституційних та індивідуальних факторів. А також те, що існує позитивна залежність між дотриманням норм моралі в економіці та економічним розвитком.*

*Третє - забезпечення цифрової етики економічних відносин і бізнесу - це проблема комплексна і багаторівнева, що вимагає участі держави, компаній, осіб, які приймають рішення в галузі права і бізнесу, а також громадян.* Зупинимося на цьому пункті більш детально.

У цьому сенсі позитивним для України може бути *досвід європейських держав і бізнесу.*

У країнах Європейського Союзу докладається максимум зусиль, як в галузі розробки відповідних нормативних актів, так і в відповідній роз'яснювальній роботі аби населення, державні служби, муніципалітети, бізнес розуміли норми закону, що регулюють обробку даних, кібербезпеку та електронну комунікацію, знали практичні аспекти впровадження та ризики, пов'язані з невиконанням цих положень.

До того ж *вивченням питань цифрової етики займаються не тільки офіційні державні інституції чи державні фахівці, але й широке коло небайдужих професіоналів з різних сфер* (право, етика, економіка, технології), які створюють відповідні науково-професійні спільноти, проводять дослідження та активні професійні обговорення в реальному та віртуальному просторі.

Велика увага приділяється підвищенню обізнаності та розширенню знань про правила захисту персональних даних серед громадян та інституцій у державах – членах Європейського Союзу та Ради Європи, випускаються та популяризуються спеціальні тематичні посібники [23].

Починаючи з часів прийняття Загальної декларація прав людини Організації Об'єднаних Націй (ООН) 1948 року Європейське законодавство вже декілька десятиліть удосконалює й систему захисту персональних даних. останні суттєві зрушення - це прийняття 14 квітня 2016 року *Загального регламенту про захист даних (GDPR)* [24], який діє у межах Європейського Союзу (ЄС) та Європейської економічної зони (ЄЕЗ). Він також стосується експорту персональних даних за межі ЄС і ЄЕЗ. GDPR покликаний насамперед надати громадянам та резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання в межах ЄС. 25 травня 2018 цей регламент вступив в силу та став ще більш жорстким щодо регуляторних вимог в області інформаційної безпеки і відповідальності за їх дотримання (зарегламентовані

безпрецедентні штрафні санкції за порушення вимог закону, а також встановлена можливість здійснювати вплив на міжнародну діяльність недобросовісних організацій).

В ЄС також створена *спеціальна Європейська рада з питань захисту даних (EDPB)* як незалежний європейський орган, метою якого є забезпечення послідовного застосування GDPR та сприяння співпраці між органами влади ЄС щодо захисту даних. До складу Ради входять представники 27 держав ЄС та 3 країн ЄЕЗ, що входять до складу Європейської асоціації вільної торгівлі (ЄАВТ).

Також Рада є учасником *Глобальної асамблеї конфіденційності* [25] - найважливішого світового форуму для обміну знаннями, досвідом та ідеями в галузі захисту персональних даних та конфіденційності. Вперше асамблея була проведена у 1979 році як Міжнародна конференція уповноважених із захисту даних та конфіденційності. Понад чотири десятиліття вона функціонує як майданчик для зустрічей лідерів у галузі захисту персональних даних. Це досягається спільними зусиллями організацій з 6 континентів - загалом ста десяти акредитованих членів та шістнадцяти спостерігачів з усього світу. Уповноважений Верховної Ради України з прав людини був акредитований для участі у Асамблеї у Амстердамі, 26 жовтня 2015 року Постановою про акредитацію під час 37-го скликання [26].

У квітні 2021 року Рада оприлюднила свій Річний Звіт за 2020 р. [27] з проведеними заходами, використаними ресурсами, новими учасниками та планом подальших дій, а вже 30 червня 2020 року Рада анонсувала свою *Стратегію «Формування безпечнішого цифрового майбутнього»* на 2020-2024 рр. [28] для громадськості. Стратегія була прийнята на тлі пандемії COVID-19, яка підняла важливість цифрової економіки, а також необхідність ефективної гарантії щодо захисту даних та конфіденційності у кіберпросторі. Метою стратегії є формування більш безпечної, справедливої та стійкішої цифрової Європи, особливо для найбільш вразливих груп суспільства. У дусі співпраці та єдності Рада продовжуватиме роботу з органами влади та експертами в різних сферах політики щодо вирішення нових цифрових питань та викликів.

У 2019 році Європейська комісія вперше опублікувала "*Етичні настанови щодо надійного штучного інтелекту"*, які визначають етичні принципи та пов'язані з ними цінності, яких слід дотримуватися при розробці, впровадженні та використанні систем штучного інтелекту. Відповідно до цих настанов, штучний інтелект повинен бути: законний - з дотриманням усіх чинних законів та норм; етичний - з дотриманням етичних принципів та цінностей; надійний з технічної точки зору та враховуючи соціальне середовище. Після пілотного процесу, в якому взяли участь понад 350 зацікавлених сторін, 17 липня 2020 року *Експертна група високого рівня зі штучного інтелекту (AI HLEG)* представила свій остаточний *Чек-лист для оцінки надійності штучного інтелекту* [29]. Він включає *7 ключових вимог до програмних продуктів*: людська свобода волі та нагляд; технічна надійність та безпека; конфіденційність та управління даними; прозорість; різноманітність, недискримінація та справедливість; екологічний та соціальний добробут; підзвітність.

Але окрім державних нормативних актів *активна робота щодо забезпечення цифрової етики повинна запроваджуватись власне бізнесом.*

Як зазначають фахівці консалтингової компанії *Deloitte* [30], організаціям потрібно продумати цифрову культуру ретельно, включаючи принципи експериментування, розумного ризику, постійного навчання та співпраці. Компанії повинні розуміти, як передавати цю культуру не лише своїм працівникам, а

й своїм підрядникам, постачальникам та іншим учасникам господарської діяльності, навіть програмним ботам, що діють від імені організації. Для підприємств *цифрова етика повинна стати невід'ємною частиною ділових операцій.*

Цифрова етика покликана забезпечити відповідальні дії на благо всіх, в тому числі самих компаній. Компанії, які застосовують цифрову етику у своїх бізнес-моделях, створюють довіру до своїх продуктів і послуг, і чим більш послідовним чином цифрова етика буде застосовуватися в компанії, тим надійнішою буде ця компанія для своїх клієнтів, ділових партнерів і зацікавлених сторін.

В 2019 році фахівці *PwC* [16] провели опитування 300 компаній різних сфер економіки *Германії з приводу відповідальної цифровізації бізнесу, яке допомогло з'ясувати стан справ, основні проблеми та перспективи в цій сфері.*

Дослідження, зокрема показало, що тільки 33% опитаних компаній оцінюють власний стан цифрової трансформації як позитивний, і найбільш вирішеним питанням вважають забезпечення захисту та безпеки даних (82% опитаних). *Тобто компанії в більшій мірі акцентують увагу і зусилля не на етичних чи організаційних, а на технічних проблемах цифрової етики*. При цьому *найбільш важливими проблемами впровадження цифрової етики компанії вважають* відсутність відповідних кадрів, які можуть кваліфіковано розробляти стратегії цифрових перетворень (56% опитаних), недостатню обізнаність компаній щодо важливості цифрової етики (51% опитаних), недостатній рівень навиків співробітників щодо використання цифрової інформації (44 % опитаних).

За думкою учасників дослідження, *цифрова етика вже дуже впливає на компанії,* зокрема, на обробку конфіденційної інформації, такої як дані співробітників або клієнтів (85 %), системи IT- безпеки (78 %) і цифрову корпоративну культуру (62 %). *Етичні питання також відіграють важливу роль в бізнесі*, зокрема, у забезпеченні прозорості для співробітників, клієнтів і зацікавлених сторін, а також в прийнятті стратегічних рішень (по 59 %). Відповідно 59% корпорацій займаються питаннями забезпечення цифрової етики всередині корпорацій на рівні вищого керівництва. *Однак, тільки в кожної п'ятої компанії є спеціальний фахівець з етичних питань.*

*Які заходи, пов'язані з цифровою відповідальністю, вже реалізують компанії?* Перш за все, це рекомендації щодо захисту даних та їх обробки (78 %), а також рекомендації щодо забезпечення прозорості щодо цифрових тем (57 %). Для компаній також важливо, щоб рішення, засновані на алгоритмах в області штучного інтелекту, могли коригувати люди (44 %) і що існують обов'язкові правила для внутрішнього і зовнішнього онлайн-спілкування (43 %).

Але, *сформульовані стандарти цифрової етики та цифрової відповідальності,* які можуть служити орієнтирами для корпоративних рішень, менш поширені: до сих пір з ними працювала тільки чверть компаній (24 % опитаних).

І останнє важливе питання дослідження: *«Які зацікавлені сторони впливають на внутрішні правила компанії по цифровій етиці?».* Компанії зазначили, що найважливішу роль грає законодавець (73 %), на другому і третьому місці - клієнти і співробітники (68 і 60 %, відповідно). Інші зацікавлені сторони, такі як конкуренти, інвестори або профспілки, грають другорядну роль.

PwC рекомендує *п'ять напрямків відповідальної цифровізації для компаній* [17]:

*1.* Компанії повинні *взяти відповідальність на себе*, а не чекати зовнішніх регуляторів. Для цього, зокрема, необхідно *створити кодекс цифрової етики.*

*2.* Слід *використовувати існуючі*

*структури* - цінностям цифрової етики необхідно відвести постійне місце в існуючих системах управління, таких як *управління ризиками, комплаєнс і заходи з управління персоналом*.

3. Необхідно *підвищувати кваліфікацію в галузі цифрової етики* - тільки ті співробітники, які добре обізнані про цифрову етику, володіють навичками чутливості і вирішення питань, необхідних для вирішення безлічі різних проблем цифрової етики.

4. Необхідно *забезпечити етику у всіх бізнес-процесах* - цифрова комплексна перевірка повинна проходити через весь ланцюжок поставок. Теплова карта цифрової етики та кодекс поведінки можуть проілюструвати ризики та дозволити компанії прозоро повідомляти свої корпоративні вимоги постачальникам та зацікавленим сторонам.

5. *Розробка продукту повинна орієнтуватися на цінність* - необхідно використовувати етичні принципи проектування для запобігання ризиків на самих ранніх етапах розробки продукту, а не реагувати на ризики в міру їх виникнення.

*Вважаємо, що рекомендації експертів PwC будуть корисними для українського бізнесу.*

*Однак, система цифрової етики бізнесу, створена в державі і компаніях, це - лише необхідна умова етики цифрових відносин. Максимально необхідна умова - правильний моральний вибір кожної особистості, яка приймає рішення в сфері використання нових технологій і результатів їх застосування (в т.ч. особистих даних), в економіці і бізнесі. Як зазначає Дейв Ярдлі, тиск конкуренції може змусити людей приймати рішення з руйнівними наслідками. Тому, реальна цифрова етика економічних відносин «означатиме наявність навичок і моральної мужності, щоб кинути виклик існуючим нормам і діяти етично»* [15].

Доповнюючи Дейва Ярдлі, зауважимо, що *ускладнення правильного морального вибору в сучасному світі взагалі пов'язане із зростанням «вантажу відповідальності»: (*зростанням вимог до управлінців та професіоналів щодо їх компетентності у багатьох галузях (технології, економіка, право, ін.), вимог до швидкості прийняття рішень та їх зваженості щодо соціальних, екологічних наслідків), а також із *«цілепокладанням капіталізму»* (див. наступний висновок). *А для України, тисячолітня культура якої завжди сприяла формуванню високоморальної особистості, зараз, нажаль, для особи, яка приймає рішення, виникає додаткова велика морально-психологічна напруга діяти морально в умовах коли, суспільство, закони, виховання, ЗМІ не заохочують до цього, до того ж поведінка лідерів та бізнесу не є взірцем моральної відповідальності.*

*Тому, на нашу думку, етика бізнесу, і як навчальна дисципліна, і як практика діяльності, в умовах цифровізації реально повинна бути компасом прийняття правильних рішень. Їй необхідно стати фундаментом для професійних рішень, способом мислення і поведінки, спрямованих на збереження і розвиток людської особистості. Це - найважливіше завдання сучасного виховання і освіти. І це - наш четвертий висновок.*

*П'яте - дотримання цифрової етики бізнесу, на жаль, буде все більш складним і обмеженим в результаті вбудованого в модель капіталізму цілепокладання, орієнтованого на прибуток, а також посилення конкуренції в умовах системної кризи капіталізму і переходу до посткапіталізму.* Зупинимося на цьому пункті більш детально.

Вбудовані в систему проблеми, що роблять цифрову етику обмеженою, а на якомусь етапі навіть неможливою, можна побачити *на прикладі умов для економічної ефективності ШІ, які наводять аналітики PwC* [18-20].

В даний час найбільший виграш від ШІ досягається за рахунок підвищення продуктивності, оскільки підприємства

використовують ШІ для автоматизації процесів і допомоги співробітникам у прийнятті більш ефективних рішень. Але, як показало глобальне дослідження штучного інтелекту, проведене PwC в 2017 році, *більша частина економічного впливу ШІ надалі буде забезпечуватись за рахунок споживання через більш якісні, персоналізовані і засновані на даних продукти і послуги. За прогнозом 45% загальної економічної вигоди до 2030 року буде забезпечено саме за рахунок удосконалення продукції, яка стимулює споживчий попит.*

Причому в цих тенденціях простежується, як мінімум, *чотири глобальні ризики*. Перший пов'язаний зі скороченням робочих місць в результаті нового витка автоматизації. Другий - з непередбаченими, цілком можливо, катастрофічними результатами непродуманого використання рішень ШІ. Третій - з проблемою управління поведінкою споживача, що само по собі неетично, якими б благими намірами це не пояснювалося. Четвертий ризик також пов'язаний зі споживанням, а саме з його різким скороченням (внаслідок зростання безробіття) і диференціацією (кастомізацією) самих споживачів. *Ці ризики є і економічними, і етичними проблемами, що в принципі не мають свого позитивного рішення в межах капіталістичної моделі економіки.*

Шостий висновок, в т. ч. пов'язаний з попереднім. Погодимося з Грі Хассельбалч, *в сучасному світі ніхто не зможе знайти ідеального рішення етичних дилем, з якими ми стикаємося* [12]. Етика завжди була покликана визначати «правильне» і «неправильне» з урахуванням загальних культурних цінностей і соціальних угод, але, на нашу думку, сьогодні цього «спільного» стає все менше. Більш того, нова і, активно впроваджувана, *філософія трансгуманізму* виправдовує все те, що було під забороною в традиційних для європейської культури, християнській філософії та філософії гуманізму. Також необхідно враховувати проблеми недостатньої технічної, цифрової компетентності багатьох користувачів нових технологій і звідси - непередбаченість наслідків використання цих технологій.

Одна із найактуальніших проблем, що гостро виявилась під час карантинних обмежень, це розвиток так званого *Інтернету поведінки (IoB)*.

Gartner, описуючи основні стратегічні технологічні тенденції на 2021 рік у якості першої тенденції називає саме розвиток Інтернету поведінки (IoB), тобто *використання даних для зміни поведінки* [31].

Як показує *приклад моніторингу протоколу COVID-19, IoB використовує дані для зміни поведінки.* З ростом технологій, які збирають «цифрову пил» у повсякденному житті - *дані, які охоплюють цифровий і фізичний світи - цю інформацію можна використовувати для впливу на поведінку через петлі зворотного зв'язку.* IoB може збирати, комбінувати і обробляти дані з багатьох джерел, включаючи: дані комерційних клієнтів; дані про громадян, оброблювані державним сектором і державними установами; соціальні медіа; суспільне надбання розпізнавання осіб; і відстеження місця розташування.

*На нашу думку, застосування IoB в більшості випадків звичайного життя не є етично виправданим, але саме ця технологія широко використовується великими корпораціями.*

І, нарешті, останній висновок. Цифрова етика стала місцем зустрічі інтересів різних суб'єктів економічної діяльності - держави, наддержавних структур управління, великих компаній (насамперед, високотехнологічних), політиків і простих споживачів, тому *є загроза лобіювання кожної з сильних сторін своєї, «вигідної цифрової етики».* У цих умовах складно, але *необхідно створювати цифрову етику економіки*

*(бізнесу), орієнтовану на інтереси і дотримання гідності людської особистості, збереження традиційних цінностей, та на традиції гуманізму.*

*На жаль, процес цифровізації, є однією з головних технічних умов переходу до посткапіталізму – системи, де моралі, з точки зору її класичного розуміння в парадигмі гуманізму, з позиції традиційних цінностей, не буде місця. Вже зараз в рамках трансгуманізму існує нова "етика" (постетика, антиетика) життя і бізнесу (економіки), в якій місце людини займе постлюдина.*

*В рамках домінуючої лінійної парадигми розвитку суспільства та економіки цей процес зупинити неможливо. Його можна тільки призупинити. І головний інструмент опору негативним змінам та мінімізації ризиків, це -забезпечення інституційної та індивідуальної етики бізнесу та економіки в умовах цифровізації на засадах традиційних цінностей.*

Що стосується інституційного рівня, ми вже відзначали певний досвід європейських країн.

В Україні законодавчими актами, які гарантують право людини на захист даних є [32, 33]: Конституція України (стаття 32); Загальна Декларація прав людини (стаття 12); Міжнародний Пакт про громадянські і політичні права (стаття 17); Конвенція про захист прав людини і основоположних свобод (стаття 8); Конвенція Ради Європи про захист осіб у зв'язку автоматичною обробкою персональних даних; Закон України «Про захист персональних даних»; Витяг з Кодексу України про адміністративні правопорушення (стаття 188-39 «Порушення законодавства у сфері захисту персональних даних», стаття 188-40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»); Витяг з Кримінального кодексу України (стаття 182 «Порушення недоторканності приватного життя»); Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 № 1/02-14.

Звісно, що цей перелік не є вичерпним. *Щодо законодавчої бази з питань цифрової етики ведення бізнесу, то вона в Україні відсутня.*

У вересні 2019 року за фінансової підтримки Агентства США з міжнародного розвитку (USAID) через програму Counterpart International *українською Громадською організацією «Лабораторія цифрової безпеки»* [34], в рамках проекту «Програма захисту цифрових прав в Україні» було підготовлено та опубліковано низку рекомендацій щодо посиленого захисту прав людини в Інтернеті. У коло рекомендацій, з якими ми згодні, входять такі:

1. Розробити та впровадити систему моніторингу та оцінки цифрового захисту прав людини;
2. Розпочати діалог з експертами та правозахисниками стосовно законодавчих та інші ініціатив, спрямованих на регулювання суспільних відносин у Інтернеті через запуск робочої групи або проведення робочих операцій та зустрічей з метою запобігання порушенням прав людини, скласти чітку та збалансовану концепцію регулювання відносин щодо розповсюдження інформації в Інтернеті;
3. Розробити і включити до освітніх програм державних службовців питання щодо забезпечення захисту прав людини в Інтернеті;
4. Включати тренінги, пов'язані з інформаційними технологіями та забезпеченням захисту прав людини в Інтернеті до програми отримання кваліфікації судді;
5. Розробити та забезпечити інтеграцію до шкільних програм обов'язкові складові компетенції Інтернету та ЗМІ, забезпечити включення відповідних компонентів у програми навчання та підвищення кваліфікації вчителів.

Починати з виховання та освіти - це, на нашу думку, найбільш тривалий, але й найбільш дієвий шлях, який необхідно обрати. Саме він сприяє формуванню, підтримці та реалізації формуванню етики економічних відносин на особистісному рівні. І в цьому напрямі вже існують певні здобутки.

Слід відзначити роботу представника кафедри філософії НТУ «Київський політехнічний інститут імені Ігоря Сікорського», професора Девтерова І., який і в своїх наукових публікаціях [35, 36], і в навчальних матеріалах висвітлює етичні проблеми у кіберпросторі. Так, вже сьогодні на базі НТУ КПІ розпочато викладання навчальної дисципліни «Інтернетика» [37], яка є науково та методологічно обґрунтованою системою оволодіння особистістю специфіки самореалізації у соціокультурному і професійному інтернет-середовищі – кіберсоціумі, що полягає у засвоєнні знань, умінь та навичок кіберадаптації, кіберсоціалізації, ефективної професійної (науково-інформаційної, фінансово-економічної, соціально-політичної, освітянської, правової, культурно-етичної) діяльності у кіберсоціальних структурах. Зокрема, однією з навчальних тем дисципліни є «Особисте управління споживанням інформації. Маніпулятивні технології і інформаційна безпека особистості», «Цифрова етика» та багато інших. Це той досвід, який, на нашу думку, необхідно транслювати на всю систему освіти. І роботу в цьому напрямі потрібно поглиблювати.

Але в цілому українська наукова, освітянська і бізнес спільнота ще тільки починає системно вивчати та впроваджувати в практику етику економічних відносин та бізнесу в умовах цифровізації. Тому матеріал цієї статті, сподіваємось, може дати певний поштовх до роздумів, праці та системних дій в цьому напрямі.

**Висновки.** Технології нового покоління засновані на цифрових, відкривають людству нові перспективи, але й водночас, створюють величезні проблеми і загрози. Зокрема, існує можливість використовувати такі технології і масиви персональних даних в егоїстичних, руйнівних цілях для отримання прибутку або влади і управління поведінкою людей.

Ще однією загрозою і проблемою є значний пробіл в оцінці допустимості розвитку нових технологій з точки зору моралі і права. В якості однієї з відповідей на ці загрози і проблеми в європейському науковому просторі було сформовано окремий напрям, присвячений цифровій етиці бізнесу. Але він ще не знайшов свого належного відображення в українському освітньо-науковому просторі.

В цій статті автори дають визначення сутності цифрової етики бізнесу, основних етичних дилем, проводять системний аналіз проблем та напрямів забезпечення цифрової етики бізнесу на платформі парадигми духовно-моральної та соціокультурної детермінації соціально-економічного розвитку. Також автори розглядають європейський досвід забезпечення цифрової етики економічних відносин, європейську та вітчизняну законодавчу базу у сфері захисту персональних даних. Автори висвітлюють результати досліджень світових компаній у контексті глобальної кризи довіри до збирачів персональних даних, а також у напрямі забезпечення цифрової відповідальності бізнесу.

На закінчення хотілось би зазначити, що цифрова етика стала місцем зустрічі інтересів різних економічних суб'єктів - держави, наднаціонального уряду, великих компаній (особливо високотехнологічних), політиків і звичайних споживачів, тому існує загроза лобіювання кожної з сильних сторін її "корисної цифровий етики". У цих умовах складно, але необхідно створити цифрову етику економіки (бізнесу), орієнтовану на збереження традиційних цінностей і традицій гуманізму.

На нашу думку для *України*, *важливо не тільки розробити низку відповідних правових актів, але, перед усім, значно посилити етичну складову в освітньому просторі відповідно до соціокультурного принципу, і займатись системною підготовкою фахівців в галузі етики економічних відносин та ведення бізнесу в умовах цифровізації та цифрової трансформації компаній, в межах передвищої, вищої освіти, системи підвищення кваліфікації кадрів.*

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Дніпровської політехніки.* 2020. № 3 (71). С. 18-26.
2. Шраменко О. В., Савчук І. Н. Інфраструктурна безпека в епоху цифрової економіки. *Причорноморські економічні студії.* 2020. Випуск 58-1. С. 84-89.
3. Пантєлєєва Н. М., Романовська Н. М., Романовська М. С. Кіберзагрози в умовах цифрової економіки. *Фінансовий простір*. 2019. № 1. С. 130-144.
4. Войтович О. Виявлення негативних впливів у соціальних інтернет-сервісах. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. №2. С. 93-105.
5. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* 2018. №1. С. 75-86.
6. Ткаченко О. Конфіденційність даних користувачів у сучасних месенджерах. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* 2019. Том 2. №2. С. 184-192.
7. Карпенко Ю. В. Етичні принципи застосування штучного інтелекту в публічному управлінні. *Вісник НАДУ. Серія «Державне управління».* 2019. № 4(95). С. 93-97.
8. Хрущ С. Методи виявлення інформаційно-психологічних впливів в соціальних мережах. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* 2019. Том 2. №1. С. 60-74.
9. Hasselbalch G. Data ethics is a game of interests. URL: https://dataethics.eu/data-ethics-is-a-game-of-interests/ (дата звернення: 15.07.2021).
10. Hasselbalch G. Ethics for the Digital Age. URL: https://dataethics.eu/a-new-ethics-for-the-digital-age (дата звернення: 15.07.2021).
11. Hasselbalch G., Tranberg P. Data Ethics — The New Competitive Advantage. URL: https://dataethics.eu/wp-content/uploads/DataEthics-UK-original.pdf (дата звернення: 15.07.2021).
12. Hasselbalch G. A human centric approach to AI: The EU Ethics Guidelines for AI. URL: https://dataethics.eu/a-human-centric-approach-to-ai-the-eu-ethics-guidelines-for-ai (дата звернення: 15.07.2021).
13. Henshall A. What is Digital Ethics?: 10 Key Issues Which Will Shape Our Future. URL: https://www.process.st/digital-ethics/ (дата звернення: 15.07.2021).
14. Meulen R. Kick-Start the Conversation on Digital Ethics. URL: https://www.gartner.com/smarterwithgartner/kick-start-the-conversation-on-digital-ethics-2 (дата звернення: 15.07.2021).
15. Yardley D. The top five ethical | moral principles for digital transformation. URL: https://www.consultancy.uk/news/16602/the-top-five-ethical-moral-principles-for-digital-transformation (дата звернення: 15.07.2021).
16. Hanauer D. Digitale Ethik Chancen, Orientierung und Haltung für verantwortungsbewusste Unternehmen in der digitalen Welt. URL: https://www.pwc.de/de/managementberatung/risk/digitale-ethik.html (дата звернення: 15.07.2021).
17. Hanauer D. Digital Ethics. Opportunities, orientation and attitude for responsible companies in the digital world. URL: https://www.pwc.de/de/managementberatung/ris

k/digitale-ethik.html (дата звернення: 15.07.2021).

18. PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution What's the real value of AI for your business and how can you capitalise? URL: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html (дата звернення: 15.07.2021).

19. Sizing the prize What's the real value of AI for your business and how can you capitalise? URL: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf (дата звернення: 15.07.2021).

20. 2019 AI Predictions. Six AI priorities you can't afford to ignore URL: https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions-2019.html (дата звернення: 15.07.2021).

21. Global crisis in trust over personal data. URL: https://winmr.com/global-crisis-in-trust-over-personal-data/ (дата звернення: 15.07.2021).

22. Компанієць В.В. Моральніоснови економіки та підприємницької діяльності : підручник. Харків : УкрДУЗТ, 2018. – 454 с. URL: http://lib.kart.edu.ua/handle/123456789/385 (дата звернення: 15.07.2021).

23. Посібник з європейського права у сфері захисту персональних даних. — К.: К.І.С., 2015. – 216 с.

24. General Data Protection Regulation. URL: https://gdpr-info.eu/ (дата звернення: 15.07.2021).

25. Global Privacy Assembly. URL: https://globalprivacyassembly.org/ (дата звернення: 15.07.2021).

26. 37th International Conference of Data Protection and Privacy Commissioners. Accreditation resolution. URL: https://globalprivacyassembly.org/wp-content/uploads/2015/02/Accreditation-resolution-2015.pdf (дата звернення: 15.07.2021).

27. Annual Report 2020. Europian Data Protection Supervisor. The EU's independent data protection authority. URL: https://edps.europa.eu/system/files/2021-04/2021-04-19-annual-report-2020_EN.pdf (дата звернення: 15.07.2021).

28. Shaping a safer digital future. The EDPS Strategy 2020-2024. URL: https://edps.europa.eu/edps-strategy-2020-2024/ (дата звернення: 15.07.2021).

29. The High-Level Expert Group on AI. The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment. URL: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (дата звернення: 15.07.2021).

30. Deloitte. Future of risk in the digital era Transformative change. Disruptive risk. URL: https://www2.deloitte.com/us/en/pages/advisory/articles/digital-ethics.html (дата звернення: 15.07.2021).

31. Panetta K. Gartner Top Strategic Technology Trends for 2021 URL: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/ (дата звернення: 15.07.2021).

32. ТОП-10 питань у сфері захисту персональних даних. URL: https://www.prostir.ua/?library=top-10-pytan-u-sferi-zahystu-personalnyh-danyh (дата звернення: 15.07.2021).

33. Україна 2030Е — країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (дата звернення: 15.07.2021).

34. Digital Rights Agenda for Ukraine / Vita Volodovska, Maksym Dvorovyi. — Kyiv: NGO Digital Security Lab Ukraine, 2019. — 56 p.

*35.* Девтеров И. В. О киберсоциальной антропологии и искусственном интеллекте. *Ідеї академіка ВМ Глушкова і сучасні проблеми штучного інтелекту: матеріали VIII Всеукраїнської науково-практичної конференції «Глушковські читання».* Київ. 29 листопада 2019 р. Київ: Ліра-К. 2019. С. 66–69.

36. Девтеров І. Етичні проблеми кіберпростору. *Вища освіта України*. 2011.

№ 2. С. 27-32.

37. Інтернетика. Методичні рекомендації до вивчення дисципліни, проведення практичних занять та самостійної роботи студентів усіх напрямів підготовки ОКР «Бакалавр» денної форми навчання. Уклад.: Девтеров І.В., Міняйло В.С., Столяренко Д.А.. К.: НТУУ «КПІ», 2015. – 28 с.

## REFERENCES

1. Kindzers`ky`j Yu. V. (2020) Kiberbezpeka ta stanovlennya cy`frovoyi ekonomiky`: problemy` vzayemozv'yazku [Cybersecurity and the formation of the digital economy: problems of interconnection]. *Ekonomichny`j visny`k Dniprovs`koyi politexniky`.* Vol. 3. No.71. pp. 18-26.

2. Shramenko O. V., Savchuk I. N. (2020) Infrastrukturna bezpeka v epoxu cy`frovoyi ekonomiky` [Infrastructure security in the digital economy]. *Pry`chornomors`ki ekonomichni studiyi.* Vol. 58-1. pp. 84-89.

3. Pantyelyeyeva N. M., Romanovs`ka N. M., Romanovs`ka M. S. (2019) Kiberzagrozy` v umovax cy`frovoyi ekonomiky` [Cyber threats in the digital economy]. *Finansovy`j prostir.* No.1. pp. 130-144.

4. Vojtovy`ch O. (2018) Vy`yavlennya negaty`vny`x vply`viv u social`ny`x internet-servisax [Detection of negative influences in social Internet services]. *Cy`frova platforma: informacijni texnologiyi v sociokul`turnij sferi.* No. 2. pp. 93-105.

5. Tkachenko O. (2018) Kiberprostir i kiberbezpeka: problemy`, perspekty`vy`, texnologiyi [Cyberspace and cybersecurity: problems, prospects, technologies]. *Cy`frova platforma: informacijni texnologiyi v sociokul`turnij sferi.* No. 1. pp. 75-86.

6. Tkachenko O. (2019) Konfidencijnist` dany`x kory`stuvachiv u suchasny`x mesendzherax [Confidentiality of user data in modern messengers]. *Cy`frova platforma: informacijni texnologiyi v sociokul`turnij sferi*. 2019. Vol. 2. No.2. pp. 184-192.

7. Karpenko Yu. V. (2019) Ety`chni pry`ncy`py` zastosuvannya shtuchnogo intelektu v publichnomu upravlinni [Ethical principles of application of artificial intelligence in public administration]. *Visny`k NADU. Seriya «Derzhavne upravlinnya».* Vol. 4. No.95. pp. 93-97.

8. Xrushh S. (2019) Metody` vy`yavlennya informacijno-psy`xologichny`x vply`viv v social`ny`x merezhax [Methods of identifying information and psychological influences in social networks]. *Cy`frova platforma: informacijni texnologiyi v sociokul`turnij sferi.* Vol. 2. No.1. pp. 60-74.

9. Hasselbalch G. (2018) Data ethicsis a game of interests. Available at: https://dataethics.eu/data-ethics-is-a-game-of-interests/

10. Hasselbalch G. (2016) Ethics for the Digital Age. Available at: https://dataethics.eu/a-new-ethics-for-the-digital-age

11. Hasselbalch G., Tranberg P. (2016) Data Ethics — The New Competitive Advantage. Available at: https://dataethics.eu/wp-content/uploads/DataEthics-UK-original.pdf

12. Hasselbalch G. (2019) A human centric approach to AI: The EU Ethics Guidelines for AI. Available at: https://dataethics.eu/a-human-centric-approach-to-ai-the-eu-ethics-guidelines-for-ai

13. Henshall A. (2018) What is Digital Ethics?: 10 Key Issues Which Will Shape Our Future. Available at: https://www.process.st/digital-ethics/

14. Meulen R. (2017) Kick-Start the Conversation on Digital Ethics. Available at: https://www.gartner.com/smarterwithgartner/kick-start-the-conversation-on-digital-ethics-2

15. Yardley D. (2018) The top five ethical | moral principles for digital transformation. Available at: https://www.consultancy.uk/news/16602/the-top-five-ethical-moral-principles-for-digital-transformation

16. Hanauer D. (2019) Digitale Ethik Chancen, Orientierung und Haltung für verantwortungsbewusste Unternehmen in der

digitalen Welt. Available at: https://www.pwc.de/de/managementberatung/risk/digitale-ethik.html

17. Hanauer D. (2019) Digital Ethics. Opportunities, orientation and attitude for responsible companies in the digital world. Available at: https://www.pwc.de/de/managementberatung/risk/digitale-ethik.html

18. PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution What's the real value of AI for your business and how can you capitalise? Available at: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

19. Sizing the prize What's the real value of AI for your business and how can you capitalise? Available at: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

20. 2019 Predictions. Six AI priorities you can't afford to ignore . Available at: https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions-2019.html

21. Global crisis in trust over personal data. Available at: https://winmr.com/global-crisis-in-trust-over-personal-data/

22. Kompaniyecz` V.V. (2018) Moral`ni osnovy` ekonomiky` ta pidpry`yemny`cz`koyi diyal`nosti [Moral foundations of economics and entrepreneurship]. – Kharkiv: UkrDUZT. 454 p. Available at: http://lib.kart.edu.ua/handle/123456789/385 (in Ukrainian)

23. Posibny`k z yevropejs`kogo prava u sferi zaxy`stu personal`ny`x dany`x [Guide to European law in the field of personal data protection] (2015) - Kyiv: K.I.S. 216 p. (in Ukrainian)

24. General Data Protection Regulation. Available at: https://gdpr-info.eu/

25. Global Privacy Assembly. Available at: https://globalprivacyassembly.org/

26. 37th International Conference of Data Protection and Privacy Commissioners. Accreditation resolution. Available at: https://globalprivacyassembly.org/wp-content/uploads/2015/02/Accreditation-resolution-2015.pdf

27. Annual Report 2020. Europian Data Protection Supervisor. The EU's independent data protection authority. Available at: https://edps.europa.eu/system/files/2021-04/2021-04-19-annual-report-2020_EN.pdf

28. Shaping a safer digital future. The EDPS Strategy 2020-2024. Available at: https://edps.europa.eu/edps-strategy-2020-2024/

29. The High-Level Expert Group on AI. The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

30. Deloitte. Future of risk in the digital era Transformative change. Disruptive risk. Available at: https://www2.deloitte.com/us/en/pages/advisory/articles/digital-ethics.html

31. Panetta K. (2020) Gartner Top Strategic Technology Trends for 2021 Available at: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/

32. TOP-10 py`tan` u sferi zaxy`stu personal`ny`x dany`x [TOP-10 issues in the field of personal data protection]. Available at: https://www.prostir.ua/?library=top-10-pytan-u-sferi-zahystu-personalnyh-danyh (in Ukrainian)

33. Ukrayina 2030E — krayina z rozvy`nutoyu cy`frovoyu ekonomikoyu [Ukraine 2030E is a country with a developed digital economy]. Available at: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html

34. Volodovska V., Dvorovyi M. (2019) Digital Rights Agenda for Ukraine. - Kyiv: NGO Digital Security Lab Ukraine. 56 p.

*35.* Devterov Y`. V. (2019) O ky`bersocy`al`noj antropology`y` y` y`skusstvennom y`ntellekte [About cybersocial anthropology and artificial intelligence]. *Ideyi akademika VM Glushkova i suchasni problemy` shtuchnogo intelektu: materialy` VIII Vseukrayins`koyi naukovo-prakty`chnoyi konferenciyi «Glushkovs`ki chy`tannya». Kyiv.*

*November 29, 2019*. Kyiv: Lira-K. pp. 66–69.

36. Devterov I. (2011) Ety`chni problemy` kiberprostoru [Ethical problems of cyberspace]. *Vy`shha osvita Ukrayiny*. No.2. pp. 27-32.

37. Devterov I.V., Minyajlo V.S., Stolyarenko D.A. (2015) Internety`ka [Internetics]. Metody`chni rekomendaciyi do vy`vchennya dy`scy`pliny`, provedennya prakty`chny`x zanyat` ta samostijnoyi roboty` studentiv usix napryamiv pidgotovky` OKR «Bakalavr» dennoyi formy` navchannya. Kyiv: NTUU «KPI». 28 p.