Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні

Development of Digital Economy in the Context of Information Security in Ukraine

Любомир Сопільник [1], Руслан Скриньковський [1], Мирослав Ковалів [2], Роман Заяць [3], Олександр Малашко [1], Сергій Єсімов [2], Микола Микитюк [4]

Lyubomyr Sopilnyk, Ruslan Skrynkovskyy, Myroslav Kovaliv, Roman Zayats, Oleksandr Malashko, Serhii Yesimov, Mykola Mykytiuk

[1] *Lviv University of Business and Law*
99 Kulparkivska Street, Lviv, 79021, Ukraine

[2] *Lviv State University of Internal Affairs*
26 Horodotska Street, Lviv, 79007, Ukraine

[3] *Lviv Scientific Research Forensic Center of the Ministry of Internal Affairs of Ukraine*
24 Koniushynna, Lviv, 79040, Ukraine

[4] *Institute of Department of State Guard of Ukraine Taras Shevchenko National University of Kyiv*
8 Petra Bolbochana Street, Kyiv, 01014, Ukraine

DOI: 10.22178/pos.58-7

JEL Classification: K40

Received 20.04.2020
Accepted 26.05.2020
Published online 31.05.2020

Corresponding Author:
Myroslav Kovaliv
mkovaliv1@ukr.net

Анотація. У статті розглядається розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. Описується правовий режим забезпечення інформаційної безпеки у контексті нормативних документів стратегічного планування, подальші напрями розвитку та формування нового регуляторного середовища забезпечення інформаційної безпеки та кібербезпеки, що слугує чинником розвитку цифрової економіки. Проаналізовано ситуацію зі станом забезпечення інформаційної безпеки та кібербезпеки в Україні, вплив європейської інтеграції на процес розвитку цифрової економіки. Обґрунтовано доцільність встановлення удосконаленого нормативно-правого регулювання у контексті реалізації основних напрямів Європейського Союзу та НАТО щодо забезпечення інформаційної безпеки.

Ключові слова: цифрова економіка; інформаційні правопорушення; інформаційна безпека; кібербезпека; Європейський Союз; НАТО.

Abstract. The article studies the development of the digital economy in the context of providing information security in Ukraine. The legal regime of information security in the context of normative documents of strategic planning, further directions of development and formation of a new regulatory environment for information security and cybersecurity, which serves as a factor in the development of digital economy, are described. The situation with the state of information security and cybersecurity in Ukraine, the impact of European integration on the process of digital economy development are analyzed. The expediency of establishing improved legal regulation in the context of the implementation of the main directions of the European Union and NATO on information security is substantiated.

Keywords: digital economy; information offenses; informational security; cybersecurity; the European Union; NATO.

ВСТУП

У зв'язку з розвитком інформаційного суспільства, цифрової трансформації та технологій перед державою та правом стоять завдання, що стосуються пошуку можливостей правового регулювання таких явищ (цифрових технологій), як роботизація та кіберсистеми, штучний інтелект, великі дані, Інтернет речей, Інтернет-банкінг, телемедицина, інформаційно-освітні платформи, блокчейн, безпілотні та мобільні технології тощо (рис. 1).

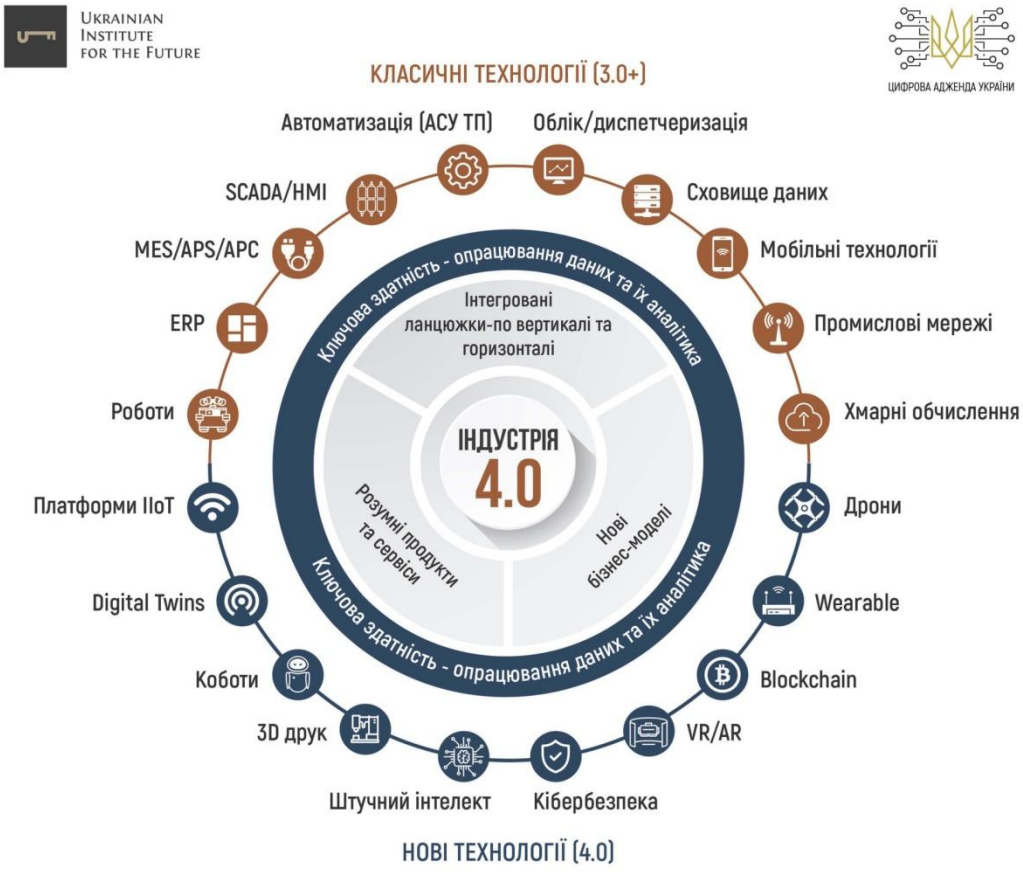

Рисунок 1 – Ключові технології цифрових трансформацій (за матеріалами [1])

З огляду на логіку міждисциплінарного підходу до регулювання правових відносин, пов'язаних з юридичною відповідальністю за правопорушення у сфері забезпечення інформаційної безпеки, тут важливими є інституційні підходи до розвитку понятійного апарату. В даний час у інформаційній сфері в міжгалузевому економіко-правовому просторі використовується досить широкий понятійно-категоріальний апарат, що вимагає певної уніфікації, зокрема, це стосується регулювання цифрової економіки та процесів цифровізації (цифрової трансформації).

Дослідження правової площини розвитку цифрової економіки, особливо в контексті забезпечення інформаційної безпеки, потребує постійного аналізу науковців і правників внаслідок суттєвого розширення нормативно-правової бази щодо впровадження цифрової економіки та ефективного використання цифрових технологій у всіх сферах життя.

Різні підходи до забезпечення інформаційної безпеки та впровадження системи кібербезпеки обґрунтовуються в роботах українських дослідників: О. Баранова, О. Голобуцького, М. Демкова, Д. Дубова, С. Дубової, О. Ємельяненка, П. Клімушина, І. Клименка, І. Коліушка, В. Брижка, А. Новицького, Н. Коритнікової, І. Куспляка, К. Линьова, Ю. Машкарова, А. Серенока, О. Орлова, В. Пархоменка, Г. Почепцова, О. Радченка, О. Шевчука та ін. [2] Дослідження правової площини розвитку цифрової економіки, особливо в контексті забезпечення інформаційної безпеки, потребує постійного аналізу науковців і правників внаслідок суттєвого розширення нормативно-правової бази щодо впровадження цифро-

вої економіки та ефективного використання цифрових технологій у всіх сферах життя.

Метою статті є дослідження цифрової економіки як фактора розвитку інституту юридичної відповідальності за правопорушення у сфері забезпечення інформаційної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Пріоритетним завданням в умовах інформаційного суспільства є розвиток цифрової економіки, повноцінна реалізація якої можлива при наявності гарантій безперебійної роботи інформаційної інфраструктури. У тексті Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. зазначено, що формування цифрової економіки та забезпечення національних інтересів у галузі цифрової економіки є стратегічним пріоритетом України в умовах європейської інтеграції [3].

Поряд з тим, у Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. також підкреслено, що інформаційна безпека необхідна для реалізації державної політики розвитку суспільних відносин у сфері цифрової економіки. Водночас тут доцільно зазначити, що Закон України «Про національну безпеку України» вказує на пріоритетність забезпечення інформаційної безпеки, вироблення заходів щодо вдосконалення системи забезпечення інформаційної безпеки держави [4].

За результатами дослідження з'ясовано, що сьогодні в Україні значна увага приділяється питанням забезпечення інформаційної безпеки об'єктів енергопостачання, ядерних і транспортних об'єктів, в той же час новітні галузі економіки потребують додаткової уваги.

У Законі України «Про основні засади забезпечення кібербезпеки України» зазначено, що об'єктами кібербезпеки є: конституційні права, свободи людини та громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу, що є об'єктами цифрової економіки [5].

Соціологічні дослідження показують, що в Україні дві третини керівників компаній вважають, що кількість злочинів в цифровому середовищі за останні три роки зросла, що вимагає вдосконалення системи інформаційної безпеки у всіх секторах економіки.

Водночас, як зазначає М. Гуцалюк [6], небезпечним в експертному середовищі вважається динамічний розвиток Інтернету речей (*Internet of Things*, далі – IP). З'явилися DDoS-атаки, що походять від певних (конкретних) бот-мереж компрометованих пристроїв IP. Протягом 2020 р. прогнозується зростання кількості таких кібератак орієнтовно на 25 %. Прогнозується також поширення IP [6].

Незважаючи на те, що Закон України «Про основні засади забезпечення кібербезпеки України» визначив основні напрями правового регулювання у зазначеній сфері, Стратегія кібербезпеки України залишається документом стратегічного планування в даній галузі [7].

Беручи до уваги наведене вище, доцільно також зазначити, що для Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. важливою складовою частиною є реалізація заходів, направлених на забезпечення кібербезпеки. Практично всі заходи, які передбачені Планом заходів на 2018 р. з реалізації Стратегії кібербезпеки України (їх понад 30), пов'язані з розвитком системи правового забезпечення інформаційної безпеки, оскільки потрібні системні зміни, спрямованих на формування правових умов для розвитку цифрової економіки [8].

З огляду на це вважаємо, що не втратили актуальності цільові установки та ключові показники реалізації Стратегії кібербезпеки України в контексті досягнення таких завдань, як:

– забезпечення єдності, стійкості та безпеки інформаційно-телекомунікаційної інфраструктури України на всіх рівнях інформаційного простору; забезпечення організаційного та правового захисту особи, бізнесу та державних інтересів при взаємодії в умовах цифрової економіки;

– створення умов для лідируючих позицій України в галузі експорту послуг і технологій

інформаційної безпеки; формування стратегічних пріоритетів та врахування національних інтересів в міжнародних документах з питань інформаційної безпеки.

До числа основних принципів інформаційної безпеки в умовах цифрової економіки відносяться необхідність заміщення технологій, розроблених у Російській Федерації, незалежно від сфери застосування в економіці, забезпечення цілісності, аутентифікації та конфіденційності, доступності інформації, що передається, процесів обробки, використання національних технологій, розроблених за стандартами Європейського Союзу або які застосовуються в Європейському Союзі (далі – ЄС) та НАТО, а також відповідного програмного забезпечення і технічних засобів з використанням криптографічних стандартів і методів шифрування НАТО.

Формування нових суспільних відносин, пов'язаних з розвитком цифрової економіки, вимагає наукового осмислення питань і організаційно-правового забезпечення інформаційної безпеки з позиції інформаційного права, вдосконалення механізмів юридичної відповідальності та правового регулювання, рішення ряду правових і організаційних питань з метою розвитку цифрової економіки, передбаченою в стратегічних документах.

Як зазначає С. Щеглюк, однією з головних складових цифрової економіки є суттєве зміщення в Інтернет операцій продажу товарів, надання послуг господарюючими суб'єктами, державою [9].

Розширення застосування нових форм отримання товарів і послуг споживачами спричинить збільшення обсягу безготівкових розрахунків і як наслідок – зростання ризиків, пов'язаних з такими розрахунками. Проведення державою політики розвитку цифрової економіки вимагає створення надійної системи безпеки, яка гарантує захищеність безготівкових коштів населення.

З огляду на те, що інформаційна безпека та кібербезпека є одним з пріоритетних напрямів розвитку цифрової економіки, на порядку денному стоїть вирішення низки завдань внутрішнього та зовнішнього характеру.

Важливими з них, з метою забезпечення інформаційної безпеки є створення середовища в частині встановлення критеріїв походження програмного забезпечення, регламентація і організація обміну інформацією.

З метою протидії комп'ютерній злочинності (що актуально для фінансової сфери) важливим є введення в експлуатацію спеціалізованої системи, яка призначена для оперативної взаємодії уповноважених суб'єктів протидії інформаційним правопорушенням і конфліктам з використанням інформаційно-комунікаційних технологій та інших технічних засобів.

Відповідно до зазначених документів доцільним є не лише створення та використання спеціалізованого ресурсу ЄС, необхідного для забезпечення взаємодії з органами, уповноваженими у сфері протидії протиправним діям, але й важливим є створення в рамках ЄС обліку правопорушень в інформаційній сфері, що доцільно внести у проект Стратегії інтеграції України до Єдиного цифрового ринку Європейського Союзу [10]. Зазначену пропозицію можливо не потрібно реалізовувати, але відсутня інформація щодо зазначеного обліку.

Автор Н. Ткачук [11] дотримується думки, що здійснення цивільного контролю у сфері кібербезпеки ускладнює відсутність відповідної публічної інформації з боку компетентних державних органів, в першу чергу – Державної служби спеціального зв'язку і захисту інформації України як державного органу, на який покладено завдання із узагальнення інформації про хід виконання планових заходів із реалізації Стратегії кібербезпеки України, а також Національного координаційного центру кібербезпеки. Сприяти вирішенню цього питання могло б оприлюднення на офіційних веб-ресурсах цих органів узагальнених матеріалів щодо стану та конкретних результатів діяльності суб'єктів національної системи кібербезпеки із виконання планів реалізації Стратегії кібербезпеки України з урахуванням вимог Закону України «Про державну таємницю» [11].

Розвиток цифрової економіки пов'язаний з формуванням інформаційного простору ЄС, а це неможливо без застосування таких методів, як аналіз і синтез в різних галузях права. Сьогодні актуальними є питання гармонізації правового регулювання суспільних відносин, що виникають у зв'язку з розвитком цифрової економіки.

Разом з тим, не вирішеними залишаються питання забезпечення суверенітету в інформаційному просторі, необхідність створення регіонального простору для економічно-безпечної взаємодії бізнесу від викликів і загроз в інформаційній сфері.

Відповідно до постанови Кабінету Міністрів України від 18 вересня 2019 р.»"Питання Міністерства цифрової трансформації» закріплені повноваження Міністерства цифрової трансформації України. Центральний орган виконавчої влади бере участь у формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності [12].

У даному випадку маються на увазі відомості про комп'ютерні інциденти та загрози безпеці інформації між операторами великих масивів даних і Національним координаційним центром кібербезпеки, розробка концепції цифрового суверенітету, де ключовими є питання про відповідальність за правопорушення в інформаційній сфері та реалізації механізмів залучення до відповідальності.

У Міністерстві цифрової трансформації України створено підрозділ, в обов'язки якого входять моніторинг радіочастотної служби відомства, що управляє мережами в критичних ситуаціях. Підрозділ повинен володіти інформацією про всю інфраструктуру зв'язку. Визначає порядок управління мережею, встановлює вимоги до обладнання Кабінет Міністрів України. Вжиті заходи повинні вирішити питання про конфіденційність передачі електронних повідомлень між користувачами. З метою забезпечення інформаційний безпеки оператор зв'язку, який надає послуги з надання доступу до Інтернету, зобов'язаний забезпечити установку в мережі зв'язку технічних засобів протидії загрозам.

Подані технічні засоби надаватимуться операторам зв'язку на безоплатній основі, що виключить додаткове навантаження на них. На власників ліній зв'язку, які перетинають державний кордон, пропонується покласти обов'язок щодо подання до уповноваженого органу інформації про використання ліній зв'язку та про здійснення функції маршрутизації повідомлень засобами зв'язку. Передбачається створення центру моніторингу та управління мережею зв'язку загального користування, завданням якого буде забезпечення доступності послуг зв'язку на території країни у кризових ситуаціях, координація зусиль операторів мобільного зв'язку при необхідності. Централізоване управління повинно здійснюватися тільки в разі, коли загроза реалізована.

Заходи реагування передбачають необхідність координації дій операторів зв'язку, власників інфраструктури та Інтернет-компаній щодо запобігання загрозам і ліквідації наслідків. Це дозволить сформувати детальну схему мереж зв'язку в Україні, визначити стійку, безперебійну роботу та подальший розвиток з урахуванням реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. та плану заходів щодо її реалізації.

У даний час такі ключові поняття цифрової економіки, як «електронна взаємодія» і «інформаційна інфраструктура електронної взаємодії», не розкриваються в Законі України «Про інформацію». На офіційному веб-сайті Міністерства цифрової трансформації України у розділі «Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ)» у наданому переліку нормативних документів немає визначення зазначених термінів [13].

Можна стверджувати, що відсутнє легальне (правове) визначення термінів «електронна взаємодія» і «інформаційна інфраструктура електронної взаємодії» на законодавчому та підзаконному рівні, хоча розуміння вказаних термінів впливає на встановлення механізмів взаємодії органів державної влади на основі інформаційних технологій та на базові вимоги до використання єдиної системи міжвідомчої електронної взаємодії.

З урахуванням вищезазначеного, доцільно погодитися з твердженням М. Рощук [14] про необхідність вдосконалення нормативної бази, систематизації інформаційного законодавства та закріплення основних правових положень, що стосуються всіх інформаційних процесів у базовому Законі України «Про захист інформації в інформаційно-телекомунікаційних системах», оскільки за

умови комплексного підходу до вдосконалення законодавства у галузі інформаційного права цифрова економіка буде розвиватися [14, 15]. Для цього очевидна необхідність розвитку інституту юридичної відповідальності.

Значущою проблемою теоретичного та прикладного характеру є питання про притягнення до кримінальної відповідальності юридичних осіб.

У даний час в кримінальному законодавстві відсутній інститут відповідальності юридичних осіб за інформаційні злочини. Стаття 96-3 Кримінального кодексу України не містить у переліку інформаційних злочинів, крім статті 376-1 «Незаконне втручання в роботу автоматизованої системи документообігу суду». Це викликає певну дискусію, хоча потреба у вирішенні питань про відповідальність юридичних осіб в умовах транскордонного обміну інформацією сучасного світу очевидна.

Дане питання має особливе значення з огляду на виконання Україною міжнародних зобов'язань з метою реалізації вимог різних міжнародних конвенцій (про протидію корупції, тероризму, екстремізму, цілого ряду проектів Організації економічної співпраці та розвитку – ОЕСР) та реалізації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [16].

Аналіз міжнародного досвіду показує, що механізм кримінальної відповідальності юридичних осіб застосовується у сфері протидії інформаційним правопорушенням, вимагає подальших міжгалузевих досліджень, але в першу чергу в науці кримінального права. Питання протидії інформаційним правопорушенням слід розглядати на національному та міжнародному рівнях.

В умовах транскордонного інформаційного обміну без міжнародних правових механізмів неможливо залучення винної особи до відповідальності, забезпечення інформаційної безпеки, формування глобального або регіонального інформаційного простору. Це вимагає нових теоретико-правових підходів, спрямованих на вироблення міжгалузевих механізмів для розвитку нових інститутів, класифікації нових суб'єктів відносин, принципів, внесення змін у нормативно-правові акти, в тому з числі, у галузеві акти, оскільки інститут відповідальності за інформаційні правопорушення має міжгалузевий характер.

План заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. передбачав ряд заходів, спрямованих на формування політики щодо розвитку цифрової економіки в рамках інтеграції до Європейського Союзу та гармонізацію підходів до нормативно-правового регулювання щодо Цифрового порядку денного для Європи (*Digital agenda for Europe*).

Вектор інформаційної безпеки у контексті Плану заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. включає напрям, що забезпечує колективну інформаційну безпеку, передбачає реалізацію необхідних елементів інфраструктури єдиного інформаційного простору і електронного підпису, що забезпечує транскордонну інформаційну взаємодію в ЄС у межах цифрової економіки. План заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. зазнав змін в цій частині.

Основою взаємодії повинен стати національний сегмент України, інтегрований в інформаційні системи ЄС. Питання формування єдиного інформаційного простору цифрової економіки України багато в чому дискусійне з технологічної точки зору, має ряд теоретичних, практичних і організаційних задач національного та міжнародного рівня, що вимагає розроблення стратегічного планування розвитку цифрової економіки у контексті Цілей сталого розвитку України на період до 2030 р. [17].

Таке завдання є вкрай актуальним для розвитку економіки, товарообігу, митної та банківської взаємодії, формування єдиного цифрового середовища взаємодії у межах інформаційного простору Європейського Союзу. Доцільно зауважити, що План заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. у певній мірі мав спільні заходи організаційного порядку, що й заходи з реалізації інформаційної безпеки. Наприклад, Протокол спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури та під час попередження, виявлення, припинення кібератак

та кіберінцидентів, а також при усуненні їхніх наслідків (проект) [18].

При реалізації програми розвитку цифрової економіки слід доцільно також передбачити необхідність створення інформаційної системи попередження та виявлення комп'ютерних атак, шляхом підписання міжнародних угод та створення механізму взаємодії суб'єктів єдиного інформаційного простору. Водночас варто зауважити, що зазначений підхід розглядався у нормативних документах щодо інформаційної безпеки, але у даний час відсутня відкрита інформація з даного питання.

Прикладом може служити те, що у межах НАТО досягнута домовленість про зміцнення взаємодії компетентних органів держав-членів НАТО у сфері протидії тероризму, сепаратизму, екстремізму, в тому числі з питань посилення антитерористичної захищеності критично важливих об'єктів і місць масового перебування людей, моніторингу загроз терористичного характеру в глобальному інформаційному просторі та забезпечення кібербезпеки.

Реалізація Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. свідчить про необхідність розвитку міжнародного співробітництва в галузі забезпечення міжнародної інформаційної безпеки в самих різних форматах. Є необхідність розвитку міжнародного співробітництва взаємодії уповноважених органів країн-учасників в рамках ЄС і НАТО для аналізу кіберзагроз, забезпечення безпеки не тільки на Інтернет просторі, а й інформаційної інфраструктури, зокрема в фінансово-кредитній, енергетичній, транспортній, управлінській сферах тощо.

Розглянуті фактори, на думку А. Войціховського [19], позначені у Стратегічній концепції оборони та безпеки членів Організації Північноатлантичного договору свідчать про те, що питання протидії та забезпечення інформаційної безпеки набувають особливого звучання для України [19]. У цих умовах є гостра необхідність правових захисних заходів для забезпечення довгострокової та стійкої роботи інформаційної інфраструктури в Україні, для підвищення надійності роботи Інтернет сервісів – електронної пошти, Інтернет-банкінгу тощо та захисту від зовнішніх і внутрішніх загроз. Це певною мірою знаходить відображення у необхідності розвитку юридичної відповідальності за інформаційні правопорушення.

Цифрова економіка України передбачає розвиток значної кількості серверів, держава повинна забезпечити повноцінний доступ до цих серверів, гарантувати громадянам, що з їх даними (відомостями) нічого не трапиться, не відбудеться ніякої втрати, враховуючи, що такі прецеденти вже мали місце у країнах близького зарубіжжя.

ВИСНОВКИ

Здійснений аналіз питань (аспектів) розвитку цифрової економіки в контексті забезпечення інформаційної безпеки в Україні не претендує на абсолютну повноту вивчення усіх питань, які виникають на практиці, проте виконане дослідження дає можливість стверджувати, що:

1. Співпраця держав-членів Європейського Союзу та НАТО в умовах глобального транскордонного інформаційного суспільства та розвитку цифрової економіки повинна здійснюватися при тісній взаємодії щодо підвищення рівня міжнародної інформаційної безпеки.

2. При реалізації заходів розвитку цифрової економіки необхідно передбачити заходи формування безпечного інформаційного простору та забезпечення інформаційної безпеки на основі єдиної політики інформаційної безпеки та кібербезпеки держав-учасників Європейського Союзу та Північноатлантичного Альянсу (НАТО).

REFERENCES

1. Fishchuk, V., Matiushko, V., Cherniev, Ye., Yurchak, O., Lavryk, Ya., & Amelin, A. (2020). *Ukraina 2030E – kraina z rozvynutoiu tsyfrovoiu ekonomikoiu* [Ukraine 2030E is a country with a developed digital economy]. Retrieved April 8, 2020, from https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.htmlhttps://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (in Ukrainian)

[Фіщук, В., Матюшко, В., Чернєв, Є., Юрчак, О., Лаврик, Я., & Амелін, А. (2020). *Україна 2030Е – країна з розвинутою цифровою економікою*. Актуально на 08.04.2020. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html].

2. Skrynkovskyy, R., Pawlowski, G., Harasym, P., & Koropetskyi, O. (2017). Cybernetic Security and Business Intelligence in the System of Diagnostics of Economic Security of the Enterprise. *Path of Science, 3*(10), 5001–5009. doi: 10.22178/pos.27-6

3. Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii [On approval of the Concept of development of the digital economy and society of Ukraine for 2018-2020 and approval of the action plan for its implementation](Ukraine), 17.01.2018, No 67-r. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/67-2018-r (in Ukrainian)
[Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації (Україна), 17.01.2018, № 67-р. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/67-2018-р].

4. Pro natsionalnu bezpeku Ukrainy [On the national security of Ukraine] (Ukraine), 21.06.2018, No 2469-VIII. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/2469-19(in Ukrainian)
[Про національну безпеку України (Україна), 21.06.2018, № 2469-VIII. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/2469-19].

5. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of cybersecurity in Ukraine] (Ukraine), 05.10.2017, No 2163-VIII. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian)
[Про основні засади забезпечення кібербезпеки України (Україна), 05.10.2017, № 2163-VIII. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/2163-19].

6. Hutsaliuk, M. (2019). Suchasni tendentsii orhanizovanoi kiberzlochynnosti [Current trends in organized cybercrime]. *Informatsiia i pravo, 1*, 118–128 (in Ukrainian)
[Гуцалюк, М. (2019). Сучасні тенденції організованої кіберзлочинності. *Інформація і право, 1*, 118–128].

7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine"] (Ukraine), 15.03.2016, No 96/2016. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/96/2016 (in Ukrainian)
[Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (Україна), 15.03.2016, № 96/2016. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/96/2016].

8. Pro zatverdzhennia planu zakhodiv na 2018 rik z realizatsii Stratehii kiberbezpeky Ukrainy [On approval of the action plan for 2018 for the implementation of the Cyber Security Strategy of Ukraine] (Ukraine), 11.07.2018, No 481-r. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/481-2018-p (in Ukrainian)
[Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України (Україна), 11.07.2018, № 481-р. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/481-2018-р].

9. Shchehliuk, S. (2019). *Morfolohiia tsyfrovoi ekonomiky: osoblyvosti rozvytku ta rehuliuvannia tsyfrovykh tekhnolohichnykh platform* [Morphology of digital economy: features of development and regulation of digital technological platforms]. Lviv: Instytut rehionalnykh doslidzhen im. M. I. Dolishnoho NAN Ukrainy (in Ukrainian)
[Щеглюк, С. (2019). *Морфологія цифрової економіки: особливості розвитку та регулювання цифрових технологічних платформ*. Львів: Інститут регіональних досліджень ім. М. І. Долішнього НАН України].

10. Derzhavne ahentstvo z pytan elektronnoho uriaduvannia v Ukraini. (2018, December 20). U Kyievi obhovoryly intehratsiiu Ukrainy do Yedynoho tsyfrovoho rynku Yevropeiskoho Soiuzu [Ukraine's integration into the European Union's Digital Single Market was discussed in Kyiv].Retrieved April 8, 2020, from https://www.kmu.gov.ua/news/u-kiyevi-obgovorili-integraciyu-ukrayini-do-yedinogo-cifrovogo-rinku-yevropejskogo-soyuzu (in Ukrainian)
[Державне агентство з питань електронного урядування в Україні. (2018, Грудень 20). *У Києві обговорили інтеграцію України до Єдиного цифрового ринку Європейського Союзу*. URL: https://www.kmu.gov.ua/news/u-kiyevi-obgovorili-integraciyu-ukrayini-do-yedinogo-cifrovogo-rinku-yevropejskogo-soyuzu].

11. Tkachuk, N. (2019). Stan ta problemni pytannia realizatsii Stratehii kiberbezpeky Ukrainy [Status and problematic issues of implementation of the Cyber Security Strategy of Ukraine]. *Informatsiia i pravo, 1*, 129–134 (in Ukrainian)
[Ткачук, Н. (2019). Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право, 1*, 129–134].

12. Pytannia Ministerstva tsyfrovoi transformatsii [Issues of the Ministry of Digital Transformation] (Ukraine), 18.09.2019, No 856. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/856-2019-п (in Ukrainian)
[Питання Міністерства цифрової трансформації (Україна), 18.09.2019, № 856. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п].

13. Derzhavnyi tsentr informatsiinykh resursiv Ukrainy. (2020). Systema elektronnoi vzaiemodii orhaniv vykonavchoi vlady [System of electronic interaction of executive bodies].Retrieved April 8, 2020, from http://dir.gov.ua/sistema-elektronnoyi-vzayemodiyi-organ (in Ukrainian)
[Державний центр інформаційних ресурсів України. (2020). *Система електронної взаємодії органів виконавчої влади*. Актуально на 08.04.2020. URL: http://dir.gov.ua/sistema-elektronnoyi-vzayemodiyi-organ].

14. Roshchuk, M. (2018). Development of electronic government in Ukraine: legal aspects of providing information security. *Ukrainian Scientific Journal of Information Security, 24*(1). doi: 10.18372/2225-5036.24.12309

15. Pro zakhyst informatsii u informatsiino-telekomunikatsiinykh systemakh [On information protection in information and telecommunication systems] (Ukraine), 05.07.1994, No 80/94-VR. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/80/94-вр (in Ukrainian)
[Про захист інформації у інформаційно-телекомунікаційних системах (Україна), 05.07.1994, № 80/94-ВР. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр].

16. Pro ratyfikatsiiu Uhody pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony [On the ratification of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part] (Ukraine), 16.09.2014, No 1678-VII. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/1678-18 (in Ukrainian)
[Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (Україна), 16.09.2014, № 1678-VII. Актуально на 08.04.2020. URL: https://zakon.rada.gov.ua/laws/show/1678-18].

17. Pro tsili staloho rozvytku Ukrainy na period do 2030 roku [On the goals of sustainable development of Ukraine for the period up to 2030] (Ukraine), 30.09.2019., No 722/2019. Retrieved April 8, 2020, from https://zakon.rada.gov.ua/laws/show/722/2019 (in Ukrainian)
[Про цілі сталого розвитку України на період до 2030 року (Україна), 30.09.2019, № 722/2019. Актуально на 08.04.2020. URL. https://zakon.rada.gov.ua/laws/show/722/2019].

18. Derzhavna sluzhba spetsialnoho zv'iazku ta zakhystu informatsii Ukrainy. (2019). *Protokol spilnykh dii osnovnykh sub'iektiv zabezpechennia kiberbezpeky, sub'iektiv kiberzakhystu ta vlasnykiv (rozporiadnykiv) ob'iektiv krytychnoi informatsiinoi infrastruktury ta pid chas poperedzhennia, vyiavlennia, prypynennia kiberatak ta kiberintsydentiv, a takozh pry usunenni yikhnikh naslidkiv* [Protocol of joint actions of the main subjects of cyber security, cyber security subjects and owners (managers) of critical information infrastructure objects and during the prevention, detection, cessation of cyber attacks and cyber incidents, as well as in the elimination of their consequences].Retrieved April 8, 2020, from http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=308016&cat_id=38837&ctime=1559743156921 (in Ukrainian)
[Державна служба спеціального зв'язку та захисту інформації України. (2019). *Протокол спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури та під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків*. Актуально на 08.04.2020. URL. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=308016&cat_id=38837&ctime=1559743156921].

19. Voitsikhovskyi, A. V. (2018). Kiberbezpeka yak napriam yevroatlantychnoi intehratsii Ukrainy [Cybersecurity as a direction of Ukraine's Euro-Atlantic integration]. In *Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii* (pp. 42–48). Kharkiv: Pravo (in Ukrainian)
[Войціховський, А. В. (2018). Кібербезпека як напрям євроатлантичної інтеграції України. В *Право і безпека у контексті європейської та євроатлантичної інтеграції* (с. 42–48). Харків: Право].