

ЧЕРЕП Олександр Григорович

д-р екон. наук, професор,
Запорізький національний університет
ORCID ID: 0000-0002-3098-0105

ДАШКО Ірина Миколаївна

д-р екон. наук, професор,
Запорізький національний університет

БЕХТЕР Лілія Анатоліївна

канд. екон. наук, доцент,
Запорізький національний університет
Україна

ПРОБЛЕМИ ТА ОСНОВНІ НАПРЯМКИ ФОРМУВАННЯ СИСТЕМИ ЗАХИСТУ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ УКРАЇНИ

Сьогодні цифрова трансформація стала масовим явищем, а відповідні проєкти – життєво важливими для успіху не тільки окремих підприємств, але також регіонів і країн. При цьому трансформація тісно пов'язана з тенденцією сервізації соціально-економічних систем і багато в чому реалізується на її основі. Причому цей взаємозв'язок і механізм її здійснення залишаються недостатньо вивченими, що обумовлює потребу в розвитку інструментарію його виявлення, оцінки та управління ним¹.

Аналіз зарубіжної практики, а також теоретичних досліджень показує, що цифрова трансформація соціально-економічних систем здійснюється на основі цифрових платформ, що інтегрують господарські, соціальні та технологічні процеси, які формують цифрові сервісні екосистеми. У зв'язку з цим, у контексті цифрової економіки та менеджменту виникає новий інститут чи нова категорія бізнес-структур у сфері послуг - сервісні інтегратори, роль яких у прогресивному цифровому розвитку істотно зростає.

Тому велика роль відводиться формуванню механізмів їх функціонування, способів управління мережевої сервісної взаємодії з іншими економічними суб'єктами, що на практиці стримують розвиток підприємств - сервісних інтеграторів. Важливе значення має також формування системи захисту цифровізації економіки України, що дозволяє нейтралізувати існуючі загрози національній безпеці України у кіберпросторі.

1 Voronkova V., Nikitenko V., Oleksenko R., Cherep O., Andriukaitiene R., Briki I. Digital paradigm of economy and management in the conditions of global human transformation. *Technology Transfer: Innovative Solutions in Social Sciences and Humanities*, 2021. 4, 37–40. doi: <http://doi.org/10.21303/2613-5647.2021.001769>

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» саме «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі забезпечує кібербезпеку»².

До основних напрямів формування правової основи забезпечення кібербезпеки України слід віднести:

- нормативне закріплення понятійного апарата у сфері кібернетичної безпеки;

- створення, за участю зацікавлених відомств, базового документу (тезаурусу, ДСТУ) із визначенням основних понять у сфері кібербезпеки та забезпечення імплементації необхідних термінів до чинного законодавства України, а саме шляхом внесення змін і доповнень до законів України «Про інформацію»³, «Про захист інформації в інформаційно-телекомунікаційних системах»⁴, «Про основи національної безпеки України»⁵, «Про телекомунікації»⁶ тощо;

- розроблення Стратегії кібернетичної безпеки України та подання її на затвердження Президентів України;

- розроблення та подання на розгляд Верховної Ради України проекту Закону України «Про основи кібернетичної безпеки України»⁷, в якому, зокрема:

- а) визначити понятійний апарат, перелік основних загроз кібернетичній безпеці України;

- б) передбачити створення правової основи та матеріально-технічної бази системи кібернетичної безпеки України;

- в) визначити критерії віднесення об'єктів національного сегменту кіберпростору всіх форм власності до критичної інфраструктури, порядок формування переліку таких об'єктів;

2 Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII

3 Закон України «Про інформацію» Режим доступу: <http://www.otei.odessa.ua/wp-content/uploads/2017/10/ua055uk.pdf>. Відомості Верховної Ради України від 01.12.1992 - 1992 р., № 48. Голос України від 13.11.1992

4 Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 1089-IX від 16.12.2020. Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

5 Закон України «Про національну безпеку України» Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

6 Закон України «Про телекомунікації» № 1089-IX від 16.12.2020. Режим доступу: <https://zakon.rada.gov.ua/laws/show/1280-15#Text>

7 Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII

г) визначити компетенцію державних структур у сфері кібербезпеки та їх форми взаємодії між собою і приватним сектором. – внесення, з метою приведення національного законодавства у відповідність до положень Конвенції Ради Європи про кіберзлочинність, відповідних змін і доповнень до законів України «Про Національну поліцію»⁸, «Про Службу безпеки України»⁹, «Про оперативно-розшукову діяльність»¹⁰, «Про організаційно-правові основи боротьби з організованою злочинністю»¹¹ та ін;

д) за прикладом США, перевести більшу частину розрахунків у безготівкову форму. Це значно зменшить рівень тіньової економіки в країні, оскільки стане легше відслідковувати службам кібербезпеки сумнівні операції переказу коштів¹²;

є) поєднуючи останні досягнення НТП з нововведеннями в співробітництві з працівниками на виробництвах, ефективною інновацією було б створення спеціальної ІТ-платформи, сутність якої полягала б у вільному вираженні думок та пропозицій працівників щодо поліпшення процесу виготовлення продукції. Таке впровадження в змозі дати гарні зрушення у сферах сільського господарства та харчової промисловості, бо в цьому випадку, трудові ресурси згаданих виробництв одночасно є споживачами, які мають своє бачення продукту, який споживають¹³.

Важливим напрямом правового забезпечення системи кібернетичної безпеки України є також поглиблення міжнародного співробітництва у цій сфері. З огляду на те, що жодна держава неспроможна самотійно забезпечити ефективний захист об'єктів національної інфраструктури у кіберпросторі, такі системи розробляються кожною з провідних держав світу

8 Закон України «Про Національну поліцію». (Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379). Режим доступу: <https://zakon.rada.gov.ua/laws/show/580-19#Text>

9 Закон України «Про службу безпеки України». (Відомості Верховної Ради України (ВВР), 1992, № 27, ст.382). Режим доступу: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>

10 Закон України «Про оперативно-розшукову діяльність». (Відомості Верховної Ради України (ВВР), 1992, № 22, ст.303). Режим доступу: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

11 Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» Режим доступу: https://kodeksy.com.ua/pro_organizatsijnopravovi_osnovi_borot_bi_z_organizovanoyu_zlochinnistyu/download.htm

12 Череп О.Г., Сопіна А.Є. Розподіл доходів між українцями як основа сталого розвитку суспільства. Modern trends in science and practice./ «Актуальні тенденції розвитку науки і практики. Випуск 1». Compiled by V. Shpak; Chairman of the Editorial Board S.Tabachnikov. Volume 1. Sherman OAKS. California. GS Publishing service. 2021. P. 44- 51. ISBN 978-1-7364133-4-0 та ідентифікатор цифрового об'єкта DOI: 10.51587/9781-7364-13302-2021-005. Режим доступу: <https://www.eo.kiev.ua/ua/content/148/>

13 Череп А.В., Лищенко О.Г., Руднік О.Р. Необхідність адаптації вітчизняних виробництв до нових потреб населення на засадах інноваційного розвитку. Modern trends in science and practice./ «Актуальні тенденції розвитку науки і практики. Випуск 1». Compiled by V. Shpak; Chairman of the Editorial Board S.Tabachnikov. Volume 1. Sherman OAKS. California. GS Publishing service. 2021. P. 39- 44. ISBN 978-1-7364133-4-0 та ідентифікатор цифрового об'єкта DOI: 10.51587/9781-7364-13302-2021-005. Режим доступу: <https://www.eo.kiev.ua/ua/content/148/>

з урахуванням принципів міжнародного співробітництва та перспективами їх інтеграції у глобальну систему кібербезпеки.

Завданнями Урядової команди реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (CERT-UA) є:

- 1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;
- 2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;
- 3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;
- 4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;
- 5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;
- 6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;
- 7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;
- 8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;
- 9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії загрозам в кіберпросторі.

До таких проблем в першу чергу відносяться: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів.

Відповідно до вищезазначеного, пропонуємо наступні рекомендації:

1. Виразний тренд посилення кіберскладової у системах державної безпеки провідних країн світу обумовлює необхідність якнайшвидшого впорядкування політики Української держави у сфері кібербезпеки. Ключовим в цьому процесі має стати визначення цілей та методів їх досягнення (в першу чергу коротко- та середньострокових).

На сьогоднішній день принаймні декілька відомств розпочали роботу над такими документами як загальнодержавного (Апарат РНБО України) так і відомчого (Міністерство оборони України) значення і такі ініціативи потребують державної підтримки.

2. Вбачається доцільним провести попередній огляд кібербезпекової сфери держави (наприклад в рамках створення відповідної «Білої книги»¹⁴), що дозволив би більш чітко визначити сучасний стан нормативного забезпечення сфери кібербезпеки та основних проблем, що мають бути вирішені вже найближчим часом. Створення такого документу можливе і з залученням відповідних організацій громадянського суспільства.

3. Вже найближчим часом мають бути здійснені практичні кроки задля вирішення термінологічних проблеми в сфері кібербезпеки. Першочерговим завданням є створення за участю зацікавлених відомств базового документу із визначеннями основних понять в кібербезпековій сфері – «кіберпростір», «кібербезпека», «кібератака», «кібернапад», «кіберзахист», «кібертероризм», «кіберзлочин». Координаційною структурою в даному процесі міг би виступити Національний інститут стратегічних досліджень.

4. Актуальною залишається проблема імплементації необхідної термінології до законодавства України, що на сьогоднішній день ускладнено особливостями юридичного характеру. Вбачається доцільним закласти ключові терміни кібербезпекової сфери (а разом і сфери інформаційної безпеки в цілому) у нову редакцію Закону України «Про інформацію»¹⁵. Щодо дію-

14 Біла книга 2021: інформаційний бюлетень. Київ: Служба зовнішньої розвідки України. 2021.- 74 с. Режим доступу: <https://szru.gov.ua/download/white-book/WB-2021.pdf>

15 Закон України «Про інформацію» Режим доступу: <http://www.otei.odessa.ua/wp-content/uploads/2017/10/ua055uk.pdf>. Відомості Верховної Ради України від 01.12.1992 - 1992 р., № 48. Голос України від 13.11.1992

чих нормативно-правових документів, які визначають функціонування сектору безпеки (зокрема – його завдання), то в них доречним було б внести певні зміни, що відображали б посилення актуальності кібербезпекової проблематики. Зокрема до Закону України «Про основи національної безпеки України»¹⁶ (ст.7, замість змісту пункту «в інформаційній сфері»): «зростання рівня мілітаризації кіберпростору, активізація використання новітніх ІКТ для досягнення військово-політичних та кримінальних цілей державними та недержавними суб'єктами».

5. Доцільним є врахування проблематики кібербезпеки та зростання її важливості у середньо- та довгостроковій перспективі для українських реалій під час проведення Оборонного огляду та підготовки «Стратегічного оборонного бюлетеню на період до 2025 року»¹⁷.

6. З метою вирішення проблем координації інституцій задіяних в системі забезпечення кібербезпеки України, все ще актуальним залишається створення відповідних структур. Такою попередньо може стати Робоча підгрупа Спільної робочої групи Україна- НАТО високого рівня з питань кібернетичного захисту. Однак в середньостроковій перспективі більш доцільним вбачається створення окремого «Міжвідомчого координаційного центру із кібербезпеки», який на постійній основі забезпечував би не лише координацію діяльності силових відомств, однак і концептуальні розробки щодо оптимізації (як законодавчих, так і на рівні узгодження порядку дій в надзвичайних ситуаціях) дій українських спецслужб в сфері захисту національного кіберпростору. До її роботи мають бути залучені представники всіх відомств, що згідно діючого законодавства задіяні в сфері захисту національного кіберпростору, а також представники наукових (аналітичних) структур.

7. Незважаючи на вочевидь малоперспективну з точки зору реальних результатів міжнародну діяльність під егідою ООН із вироблення єдиних підходів до міжнародної інформаційної безпеки та демілітаризації кіберпростору, Україна має стати активним учасником даних процесів.

З одного боку це буде сприяти поліпшенню іміджу держави (як продовження політики роззброєння та зменшення військових потенціалів), а з

16 Закон України «Про основи національної безпеки України». (Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351). Режим доступу: <https://zakon.rada.gov.ua/laws/show/964-15#Text>

17 Про Стратегію національної безпеки України: за станом на 12.02.2007 р. / Указ Президента України від 12.02.2007 р., № 105/2007. [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>; Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: за станом на 09.01.2007р. / Закон, затверджений ВР України 09.01.2007 № 537-V. [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/537-16>.

іншого – впливати на формування остаточних документів з даної проблеми, що можуть бути вироблені спеціальними робочими групами. Таким чином, вбачається доцільним Міністерству зовнішніх справ України активізувати роботу у форматі комісій, експертних груп, інших дорадчих та координуючих органів ООН, що в даний час задіяні у формуванні політики ООН в сфері міжнародної інформаційної безпеки та глобальної кібербезпеки.

Нині питання забезпечення кібербезпеки є вкрай важливими для України. У сьогоdnшній ситуації наша держава є об'єктом кіберагресії з боку Кремля. З огляду на ведення російської гібридної війни, де кіберпростір є ареною ведення військових дій, Україні необхідно розбудовувати не тільки оборонні спроможності у кіберпросторі, а й наступальні.

У протистоянні існуючим викликам і загрозам кібербезпеці заважають дві основні проблеми. Перша - це відсутність загальної термінології. Такі поняття, як кіберпростір, кібербезпека, кібервійна, кібератака, кібертероризм широко використовуються у науці, проте, дотепер ще не існує чітко визначеного їх змісту. Це у свою чергу, ускладнює наукове осмислення та подальше практичне подолання тих проблем і викликів, які постають у кіберпросторі.

Другою проблемою є те, що за період незалежності і безпосередньо до 2014 року була відсутня якісна нормативно правова база у сфері кібербезпеки. Однак відзначимо, що за останні роки вона значно удосконалилася.

Загалом, не зважаючи на певну розпорошеність, законодавство у сфері кібербезпеки України в останні роки було переглянуто і трансформовано відповідно до нових викликів та загроз. Це дає підстави вважати, що законодавча база у поєднанні із реструктуризацією системи національної безпеки дозволять створити потужний механізм стримування зовнішньої кіберагресії.

Разом з тим зауважимо, що побудова законодавства у такій важливій сфері, як кібербезпека, відбувається за принципом надолуження згаяного. Натомість, потрібно навчитися стратегічно планувати, прогнозувати.

Відзначимо, у сучасних умовах громадські об'єднання, як невід'ємний елемент громадянського суспільства, є повноцінним учасником процесу забезпечення інформаційної безпеки України. Взаємодія між громадським сектором та державними інститутами є важливим аспектом безпекової політики, однак, потребує додаткового вивчення та дослідження.