

Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії

*Стендер Світлана Василівна¹, Фротер Оксана Сергіївна²,
Снітко Юлія Миколаївна³*

Опубліковано	Секція	УДК
15.12.2023	Економіка	338.22:004

DOI: <http://dx.doi.org/10.5281/zenodo.10389831>

Ліцензовано за умовами Creative Commons BY 4.0 International license

Анотація. Актуальність дослідження зумовлена стрімким поширенням і впровадженням цифрових технологій у всі сектори економіки, тому важливим є аспект забезпечення кіберзахисту систем і даних від несанкціонованого доступу завдяки новітнім технологіям та правовому регулюванню. Виходячи з існуючих класифікацій складових економічної безпеки, значну роль відіграє інформаційна безпека. Виявляється, що майже всі класифікації так чи інакше розглядають інформаційну безпеку як спосіб соціально-економічних систем надавати та захищати інформацію. Метою статті є дослідження та обґрунтування необхідності регулювання питання захисту економіки від кіберзагроз в умовах сьогодення України. Методологічно дослідження здійснено з використанням аналітичного та прогностичного, феноменологічних та історичних методів, системно-структурного підходу, аналізу та синтезу з урахуванням поставленої мети, визначених завдань. З'ясовано проблемні процеси, які безпосередньо позначаються на економічній безпеці держави, окремих регіонів та підприємств. Кіберпростір розглянуто як середовище для потенційної злочинної діяльності. Визначено характеристики економічної безпеки такі, як стійкість до внутрішніх і зовнішніх загроз, економічна незалежність, самовідтворення і розвиток, національні інтереси, які можуть бути просунуті і захищені в кіберпросторі. У трикутнику «органи державної влади – приватний сектор – громадянське суспільство» запропоновано створити ефективну систему державного регулювання кібербезпеки та умови для онлайн-обміну інформацією, оптимізувати кадрове забезпечення сектору кібербезпеки, розробити систему економічних індикаторів функціонування кіберпростору. У висновках висвітлено перспективи досліджень щодо створення ефективної організаційно-технічної моделі національної системи кібербезпеки,

¹ кандидат економічних наук, доцент, кафедра обліку, оподаткування та технологій електронного бізнесу, Навчально-науковий інститут бізнесу і фінансів, Заклад вищої освіти "Подільський державний університет", м. Камянець-Подільський, вул. Шевченка, 13, <https://orcid.org/0000-0002-6234-1877>

² кандидат економічних наук, доцент кафедри економіки, факультет економіки і підприємництва, Уманський національний університет садівництва, м. Умань, вул. Інституцька, 1, <https://orcid.org/0000-0002-6770-9618>

³ старший викладач, кафедра правознавства та фінансів, Полтавський інститут економіки і права Відкритого міжнародного університету розвитку людини "Україна", м. Полтава, вул. Монастирська, 6, <https://orcid.org/0009-0002-7115-3867>

стимулювання інноваційної діяльності, спрямованої на оптимізацію національного законодавства.

Ключові слова: захист економіки, несакціонований доступ, проблеми кібербезпеки, інноваційні рішення, оптимізація законодавства.

Digital integration and cyber protection of the economy of Ukraine: legal aspects and innovative strategies

Annotation. The relevance of the research is driven by the rapid proliferation and implementation of digital technologies across all sectors of the economy. Therefore, it is crucial to ensure cybersecurity for systems and data against unauthorized access using advanced technologies and legal regulations. Information security plays a significant role in the classifications of economic security components, highlighting its importance in enabling socio-economic systems to provide and protect information. The article aims to explore and justify the need for regulating the protection of the economy from cyber threats in the contemporary context of Ukraine. The research methodology employs analytical and predictive, phenomenological and historical methods, a systemic-structural approach, and analysis and synthesis in alignment with the defined goals and tasks. Problematic processes directly impacting the economic security of the country, specific regions, and enterprises have been identified. Cyberspace is considered an environment for potential criminal activity. Characteristics of economic security, such as resilience to internal and external threats, economic independence, self-reproduction and development, and the advancement and protection of national interests, have been defined within the cyberspace context. The article suggests creating an effective system of state regulation of cybersecurity and conditions for online information exchange in the triangle of "state authorities – private sector – civil society." It also proposes optimizing the staffing of the cybersecurity sector, and developing a system of economic indicators for cyberspace functioning. In the conclusions, the perspectives of research are highlighted, focusing on the creation of an effective organizational-technical model for the national cybersecurity system, stimulating innovative activities aimed at optimizing national legislation.

Keywords: protection of the economy, unauthorized access, cyber security issues, innovative solutions, optimization of legislation.

Вступ

Стрімкий розвиток процесу диджиталізації є джерелом не лише нових можливостей, але й ризиків та загроз для інформаційної безпеки національної економіки.

Поряд з традиційними загрозами, такими як промислове шпигунство, навмисне або ненавмисне розголошення працівниками конфіденційної інформації та комерційної таємниці, недобросовісна поведінка конкурентів, включаючи завдання шкоди діловій репутації, втручання третіх осіб в інформаційні системи і мережі та порушення цілісності баз даних, інформаційних ресурсів і технологій в економіці, з'являється багато нових загроз, методи ідентифікації та протидії яким ще не до кінця розроблені. До них відносяться кібератаки, витік персональних даних, вплив шпигунських програм і вірусів, фішинг і загрози, пов'язані з оновленням комп'ютерного програмного забезпечення. Кіберзагрози постійно зростають, тож важливо здійснювати моніторинг кібербезпеки України, виокремлювати основні виклики у побудові національної системи кіберзахисту та визначати шляхи їх подолання.

У сучасному світі питання економічної безпеки набуває особливого значення, оскільки впливає на геополітичне майбутнє країни, стан її національної економіки,

соціально-економічний добробут громадян та формування національної ідентичності. Адже в постіндустріальному суспільстві інформаційні технології охоплюють усі види людської діяльності, в тому числі й економічну. Чим швидше розвиваються інформаційні технології у світі, тим актуальнішим стає питання захисту інформаційно-комунікаційних систем. Однак окрім позитивного впливу, інформаційні технології також створюють можливості для певних видів злочинів та зловживань. Жертвами кіберзлочинності стають не лише окремі особи, а й компанії, галузі та навіть цілі держави. Тому жодна країна не може говорити про свою економічну безпеку, якщо вона не захищена в кіберпросторі.

Серед різних видів безпеки економічна безпека є найважливішою, оскільки вона безпосередньо пов'язана зі стабільним розвитком національної економіки та її різних секторів. Економічна безпека є основою для проведення структурних реформ, посилення конкурентоспроможності національної економіки на світовому ринку та підвищення функціональної ефективності на галузевому рівні. Економічна безпека у сфері державного регулювання економіки та державного управління економікою передбачає здатність національної економіки розширювати своє відтворення для задоволення потреб народу і держави на певному рівні, протистояти дестабілізуючому впливу факторів, що загрожують сталому і збалансованому розвитку країни, та забезпечувати надійність функціонування національної економіки у світовій економічній системі. Це складна і багатфакторна категорія, що характеризує компетентність.

Науковим дослідженням питання цифрової інтеграції та кіберзахисту економіки України, включаючи правові аспекти та інноваційні стратегії, займалась велика кількість дослідників. Зокрема, С. Онищенко та А. Глушко аналізують важливі підходи у вирішенні проблеми кібербезпеки у сучасній цифровій інтеграції України [1].

Про методи та інструменти захисту від кіберзагроз зазначають Г. Михальченко та інші. До них відносять криптографічні методи захисту економічних даних та навіть штучний інтелект, який є рушійним механізмом для боротьби з кіберзагрозами [2]. До прикладу, А. Семченко, Д. Малковський та Т. Станіславський наголошують, що важливою складовою кібербезпеки є відновлення роботи системи, яка постраждала внаслідок атак [3].

Прямий зв'язок між кібербезпекою і безпечним економічним функціонуванням держави вивчає С. Горбаченко [4]. На думку В. Бикова, О. Романовського та Ю. Романовської, Україні варто спрямувати свої сили на створення ефективного координуючого навчального центру з кібербезпеки [5]. О. Бакалінська та О. Бакалинський надають важливу інформацію щодо вдосконалення правової основи кіберзахисту в умовах сучасності [6].

Л. Мельник та інші виявляють особливості співпраці України з іншими державами для розвитку економіки, у яких суттєву роль відіграє цифровий аспект [7].

Важливим аспектом у розвитку та існуванні держави є розгляд сучасних трендів економічних загроз та напрями їх удосконалення завдяки державному управлінню у сфері економічної безпеки, зазначають О. Панченко та В. Гнатенко [8].

З огляду на значущість кібербезпеки важливим є питання цифрового маркетингу, який допомагає підвищувати конкурентоздатність підприємств, їхніх товарів та послуг, активно використовуючи маркетингові інструменти в цифровому просторі, вказує Р. Ігнатенко [9]. К. Краус, Н. Краус та О. Штепа акцентують увагу на інноваційних підходах до напрацювання і розвитку видів захисту від кіберзагроз з метою безпеки економічних даних України в умовах воєнного стану [10]. Ю. Кіндзерський формулює думку про взаємозв'язок розвитку цифрових технологій із кібербезпекою [11].

Процеси цифровізації безпосередньо пов'язані з євроінтеграційними перетвореннями, на шлях яких стала Україна, підсумовують С. Башлай та І. Яремко [12]. Сучасні перспективи розвитку та удосконалення сфери кібербезпеки в Україні дослідила В. Тогобицька [13]. Переваги цифрової інтеграції в Україні та її основні принципи на глобальному та національному рівнях розглянули І. Іртищева, О. Сенкевич [14].

Відповідно, *метою даної статті* є дослідження та обґрунтування необхідності регулювання питання захисту економіки від кіберзагроз в умовах цифрової інтеграції України.

Матеріали та методи. Дослідження здійснено з використанням загальнонаукових та спеціальних методів, обраних з урахуванням поставленої мети, визначених завдань, предмета та об'єкта дослідження. Водночас на основі детального аналізу методів економічних досліджень в Україні виявлено необхідність доктринальної гармонізації методів дослідження кібербезпеки.

Зокрема, феноменологічні методи використовувалися для дослідження феномену кіберзахисту економіки, його унікальних особливостей в Україні та причин зростання, формування і збереження високого рівня поширеності та небезпеки. Історичний метод використовувався для аналізу та систематизації першопричин кіберзагроз в Україні. Цей метод також допоміг пояснити труднощі щодо протидії кіберзагрозам в Україні, зокрема через зберігання важливих даних у інформаційному просторі в сучасному світі.

Застосовуючи поєднання аналітичного та прогностичного методів, автор визначив сфери державної діяльності, які потребують реформування з метою організації ефективної та комплексної системи кіберзахисту економічних даних в Україні. Водночас, зважаючи на українські реалії, акцент зроблено на «зовнішніх» перешкодах у суспільних відносинах, які поглиблюють проблему. З цією метою автор використовує порівняльно-правовий підхід для опису досвіду та сучасного стану здійснення моніторингу кібербезпеки України.

Системно-структурний підхід дозволив розглянути кіберзагрозу як системне явище, проаналізувати закономірності її появи, вплив на економіку, природу її структурних елементів та взаємозв'язки і залежності між чинниками, що її породжують. Ця методологія, до якої були долучені методи аналізу, абстрагування та узагальнення, також дозволила визначити місце і значення органів державної влади в даній проблематиці. Узагальнення та абстрагування дали змогу скласти опис характеру загроз у сучасній цифровій інтеграції України.

Аналіз і синтез дали можливість здійснити дослідження форм і проявів кіберзагроз як загального явища. Індукція та дедукція дозволили проаналізувати кібербезпеку через характеристику цифрової інтеграції і, навпаки, проаналізувати окремі інтеграційні процеси в економіці через загальну характеристику кібербезпеки. Також використовувалися методи аналогії (для дослідження етіології та феноменології певних економічних явищ); формулювання та перевірки гіпотез (для формулювання та перевірки гіпотез щодо основних причин виникнення та поширення кіберзагроз, домінуючих причин протиправної діяльності щодо порушення кібербезпеки держави); інші наукові методи, що взаємодіють між собою з метою забезпечення об'єктивності, повноти та всебічності дослідження.

Результати

Цифрові технології значно знизили витрати на пошук, обмін та зберігання інформації. Істотно розширився інформаційний сектор для людей та бізнесу. Змінилася також роль інформації як ресурсу в системах управління економікою. Власне, ці фактори сприяли появі термінів «цифрова економіка», «цифрова інтеграція» та «кібербезпека» [15].

У кожній країні існують певні галузі та сектори національної економіки, які є основою економічної безпеки, водночас прагнення реалізувати свій потенціал у сфері ІТ є одним із головних світових трендів. Тому розглядається тотальна цифровізація економічних процесів з одночасною передачею великих обсягів інформації у кіберсистеми і відповідно все більшого значення набувають питання кібербезпеки економіки держави.

Останніми роками є зрушення в категорії «кібербезпека», поступово переходячи від мікрорівня до макрорівня. Однак проблема полягає не лише в захисті інформації на окремому пристрої чи в локальній мережі. Мова йде про необхідність створення єдиної системи кібербезпеки на національному рівні як зрілої складової національної та економічної безпеки. При цьому напрям загроз поступово змінюється: від локальних і відомчих загроз до національних і наднаціональних. Основними цілями кібератак є діяльність урядів, правоохоронних органів, збройних сил, засобів масової інформації, міських систем життєзабезпечення, транспортних і комунікаційних мереж, атомної та хімічної промисловості, національних енергетичних і фінансових систем тощо [2]. Фактично, сам кіберпростір вважається середовищем для потенційної злочинної поведінки в таких формах, як несанкціонований доступ до конфіденційної інформації, збої в роботі програмного забезпечення тощо.

Кібератаки також можуть мати негативний вплив на економіку країни в цілому, оскільки в кіберпросторі відбувається багато взаємопов'язаних процесів. Крім того, атаки на критично важливу інфраструктуру, будь то банківська чи енергетична, завжди мають прямий негативний вплив на бізнес-процеси.

Сучасні кризові тенденції, в яких розвивається українська економіка під тиском внутрішніх і зовнішніх деструктивних чинників, посилені викликами глобалізації, загрозами світовій економіці та зовнішньою агресією, зумовлюють необхідність модернізації існуючої системи економічної безпеки. Ефективність нової моделі національної економічної безпеки залежить від того, наскільки вона зможе адекватно вирішувати завдання захисту від модифікованих традиційних і нових специфічних загроз. Результативність вирішення цих завдань полягає у правильній та своєчасній ідентифікації таких загроз [7].

Класифікація поточних загроз національній економічній безпеці держави з урахуванням традиційних, відомих, нових, специфічних загроз може бути використана для визначення причинно-наслідкових зв'язків, послідовності виникнення та джерел, а також їх оцінки при плануванні та реалізації серії заходів. Вони полягають у забезпеченні національної економічної безпеки, створюючи тим самим новітню ефективну модель національної економічної безпеки. Тому важливо визначити головні чинники, які активно впливають на формування економічної безпеки будь-якої держави (табл. 1).

Таблиця 1

Основні характеристики економічної безпеки

Назва характеристик	Сутність	Інструменти захисту в кіберпросторі
Економічна незалежність	Здатність суб'єктів, відповідальних за економічну безпеку, приймати та впроваджувати власні стратегічні економічні та політичні рішення для розвитку.	Захист від кібервтручання в економічну діяльність національних суб'єктів господарювання.

Національні інтереси	Здатність національної економіки захищати економічні інтереси країни.	Створення ефективного режиму, щоб регулювати кібербезпеку саме на державному рівні.
Стійкість протидії зовнішнім та внутрішнім загрозам	Надійність та міцність зв'язків між усіма елементами економічної системи, стабільність економічного розвитку країни та її здатність стримувати і нейтралізувати дестабілізуючі фактори.	Розробка системної моделі кіберпростору та виявлення факторів, що впливають на його функціонування.
Саморозвиток та самовідтворення	Створення необхідних умов для проведення ефективної економічної політики, розширення власного виробництва та забезпечення конкурентоспроможності національної економіки на міжнародній арені.	Впровадження спеціальних методів і технологій для забезпечення стійкості кіберзахисту до загроз.

Джерело: складено на основі даних [4].

На національному рівні поняття «інформаційна безпека» означає захищеність інформації від несанкціонованих дій (випадкових або навмисних), що призводять до її зміни, розкриття або знищення.

В Україні поняття «інформаційна безпека» вперше було визначено в Законі України № 537-V від 9 січня 2007 року «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», який визначає інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства і держави та запобігання шкоді, завданій через: використання неповної, несвоєчасної та недостовірної інформації; негативні наслідки використання інформаційних технологій; несанкціоновані поширення; використання або порушення цілісності, конфіденційності та доступності інформації [16].

Відповідно до Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» питання інформаційної безпеки мають вирішуватися у таких напрямках:

- забезпечення повноцінного функціонування національної інформаційної інфраструктури та захисту її критично важливих елементів;
- підвищення рівня координації діяльності державних органів з виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання та усунення таких загроз, здійснення міжнародного співробітництва з цих питань;
- удосконалення нормативно-правової бази з питань інформаційної безпеки, зокрема щодо захисту інформаційних ресурсів, боротьби з комп'ютерною злочинністю, захисту персональних даних та забезпечення правопорядку в інформаційній сфері;
- розгортання та розвиток національної системи засекреченого зв'язку як сучасної захищеної транспортної інфраструктури, здатної інтегрувати територіально розподілені інформаційні системи, що обробляють інформацію з обмеженим доступом [16].

До прийняття Закону України «Про основні засади забезпечення кібербезпеки України» правовою основою кібербезпеки в Україні були Конституція України, Закони

України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», Конвенція Ради Європи про кіберзлочинність, окремі міжнародні договори, ратифіковані Верховною Радою України, Доктрина інформаційної безпеки України та інші нормативно-правові акти [9].

Україна активно займається питаннями кібербезпеки з 2016 року, з прийняттям Стратегії кібербезпеки України [17], затвердженої Указом Президента України № 96 від 27 січня 2016 року. Відповідно до цієї Стратегії було ухвалено Закон України від 5 жовтня 2017 року

№ 2163-VIII «Про основні засади забезпечення кібербезпеки України» [18]. Закон встановлює правові та організаційні основи забезпечення захисту важливих інтересів людини і громадянина, суспільства та держави у кіберпросторі, захисту національних інтересів України, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, принципи забезпечення кібербезпеки України, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації діяльності із забезпечення кібербезпеки. Забезпечення кібербезпеки в Україні ґрунтується на таких принципах:

- верховенство права, законність, повага до прав людини та основоположних свобод, належна правова процедура забезпечення національних інтересів України, відкритість, доступність, стабільність та безпека кіберпростору, розвиток мережі Інтернет та відповідальна поведінка в кіберпросторі;
- взаємодія державного та приватного секторів у сфері кібербезпеки та кіберзахисту;
- широка співпраця з громадянським суспільством, зокрема обмін інформацією про інциденти кібербезпеки;
- реалізація спільних науково-дослідних проєктів;
- підготовка та підвищення кваліфікації кадрів;
- пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам;
- реалізація невід'ємного права держави на самооборону за міжнародним правом у разі актів агресії в кіберпросторі;
- пріоритетність превентивних заходів;
- невідворотність покарання за кіберзлочини;
- пріоритетний розвиток та підтримка вітчизняного науково-технічного та виробничого потенціалу;
- забезпечення демократичного цивільного контролю над воєнними та правоохоронними органами, утвореними відповідно до законодавства України, які здійснюють діяльність у сфері кібербезпеки [16].

Національна система кібербезпеки – це комплексна система, в якій взаємопов'язані Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи та Національний банк України, діяльність яких спрямована на забезпечення кібербезпеки та пов'язані з нею політичні, науково-технічні, інформаційні, освітні, організаційні, правові, оперативно-розшукові та каральні заходи.

Кіберзахист в розумінні ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» – це організаційні, правові, інженерно-технічні, криптографічні та технологічні заходи захисту інформації, спрямовані на попередження кіберінцидентів, виявлення та запобігання кібератакам, ліквідацію їхніх наслідків та відновлення стабільності і надійності функціонування комунікаційних і технічних систем [18].

Аналіз цього індикатора показує, що правова база є важливою для забезпечення кібербезпеки. Правовий контекст оцінюється на основі кількості правових інституцій та організацій, відповідальних за кібербезпеку. Остання не може бути забезпечена без належних технічних навичок для виявлення та реагування на кібератаки (рис. 1).



Рис. 1. Система національної безпеки в кіберекономічному просторі

Джерело: [8]

Ключовими елементами ефективно функціонуючої системи кібербезпеки є модель управління, що відповідає рівню проблеми, яку необхідно вирішити; наглядний орган, що складається з відповідних експертів. Все це складає основу інституційних елементів кібербезпеки на національному рівні.

Можливості підвищення потенціалу та рівня кібербезпеки оцінюються за кількістю науково-дослідних та дослідно-конструкторських проєктів у цій сфері, наявністю освітніх та навчальних програм, акредитованих експертів та органів державної влади. Посилення співпраці на національному та міжнародному рівнях є передумовою ефективності боротьби з кіберзлочинністю, що засвідчує кількість партнерств з обміну інформацією.

Рівень цифрового розвитку (DDL) розраховується за допомогою Індексу розвитку ІКТ (IDI) та Індексу мережевої готовності (NRI). Індекс розвитку ІКТ (IDI) – показник рівня розвитку інфраструктури інформаційних технологій. Моніторинг стану розвитку ІТ в кожній країні та її позиції на світовому ІТ-ринку здійснюється за допомогою трьох субіндексів: індекс доступу, використання та навичок. Індекс мережевої готовності (NRI) складається з чотирьох субіндексів, які оцінюють: середовище для розвитку ІКТ; готовність суспільства до використання ІКТ; фактичне використання урядами, бізнесом та населенням; наслідки використання ІКТ для економіки та суспільства. Перші три субіндекси є драйверами зростання та передумовами для четвертого субіндексу (вплив ІКТ на економіку) [4].

Цифровий розвиток є пріоритетним напрямом і предметом для розробки відповідних стратегічних документів в нашій державі та країнах ЄС. У 2018 році було схвалено Концепцію цифрового економічного та соціального розвитку України на 2018–2020 роки, у 2021 році набув чинності Закон України «Про стимулювання розвитку цифрової економіки в Україні» [19], а в Економічній стратегії України до 2030 року

визначено порядок денний українського цифрового економічного розвитку. Європейський Союз прийняв стратегічний документ «Цифровий компас 2030» [20], в якому викладено бачення та шлях до орієнтованого на людину, сталого та більш процвітаючого цифрового майбутнього. Документ ЄС має чотири ключові компоненти:

- кваліфіковане населення та висококваліфіковані цифрові фахівці;
- безпечна, ефективна та стійка цифрова інфраструктура;
- цифрова трансформація бізнесу;
- оцифрування державних послуг [20].

Участь у програмі «Цифрова Європа» є важливим інструментом цифровізації української економіки в контексті інтеграційного процесу [21]. «Цифрова Європа» запущена в 2021 році (після тривалого періоду COVID-19) з метою прискорення економічного відновлення Європи та цифрової трансформації. Програма спрямована на розвиток передових цифрових навичок, впровадження цифрових навичок у бізнес-діяльність, розвиток цифрової інфраструктури та надання цифрових послуг громадянам і органам влади Європейського Союзу (ЄС) та інших країн-учасниць програми.

Завдання «Цифрової Європи» сприяє досягненню двох стратегічних цілей ЄС: «зеленого переходу» та цифрової трансформації, а також передбачає підвищення стійкості та стратегічної автономії. Програма «Цифрова Європа» є одним із найсильніших джерел фінансування, яке отримала Україна [21].

Варто зазначити, що у вересні 2022 року Україна та ЄС підписали угоду про участь України в програмі ЄС «Цифрова Європа» (2021–2027). Програма сприяє цифровізації європейських країн у кількох напрямках. Щоб взяти участь у програмі, держави повинні зробити пожертву. Однак ЄС відмовився платити Україні за 2022 рік і запропонував 95% знижку на податкові внески на 2023–2027 роки [12].

Фінансування проєктів у рамках програми Digital Europe в основному відбувається в п'яти сферах, що є важливими для економіки держави: високопродуктивне обчислення; штучний інтелект, дані та хмарні сервіси; передові цифрові технології; забезпечення широкого використання цифрових технологій у бізнесі та суспільстві; кібербезпека (застосовується лише до ЄС держав-членів) [21].

Як і в попередній стратегії, кібербезпека залишається одним із пріоритетів системи національної безпеки України. Важливо звертати особливу увагу на загрози з боку агресивних сусідів, і враховувати, що автоматизація захисту мережі є ефективним інструментом для зниження ризику та потенційної шкоди, спричиненої можливими вторгненнями в мережеві системи.

Враховуючи взаємозалежність, яка існує між питаннями забезпечення економічної безпеки та кіберзахисту, важливо інтегрувати численні напрями, пов'язані з кіберпростором у синтез економічних та управлінських досліджень.

Насамперед, створити ефективну національну систему нагляду за мережевою безпекою. З точки зору управління, конкретні системи повинні базуватися на розробці відповідних планів заходів і подальшому контролю за їх виконанням. Затверджена Стратегія кібербезпеки України передбачає, що заходи, спрямовані на її забезпечення, мають здійснюватися планово [17]. Кабінету Міністрів України за участю Служби безпеки України, Служби зовнішньої розвідки України та Національного інституту стратегічних досліджень потрібно розробити щорічний план заходів щодо реалізації конструктивних положень Закону про кібербезпеку.

Необхідно забезпечити умови для онлайн-обміну інформацією в трикутнику «національна влада – приватний (переважно бізнес) сектор – громадянське суспільство» для запобігання реальним і потенційним загрозам критичній інформаційній інфраструктурі та оперативного інформування національних органів влади для прийняття ефективних управлінських рішень у межах своїх можливостей [4].

Кадровий аспект є міжнародним у контексті проблем у сфері забезпечення кваліфікованими фахівцями з кіберзахисту. З одного боку, можна сказати, що зовнішній ринок праці має великі перспективи для кваліфікованих вітчизняних фахівців, але з іншого – імміграційний процес може нести додаткові ризики для кібербезпеки нашої країни.

Важливо розробити систему економічних показників можливостей кіберпростору та їхньої ефективності проти потенційних загроз. На даний час важко оцінити ефективність заходів кібербезпеки та потенційні втрати від кіберзагроз. Як наслідок, деякі керівники підприємств неохоче інвестують у заходи з кібербезпеки через відсутність прямих економічних вигод. Те ж саме стосується і оцінки ефективності інноваційних проєктів, пов'язаних з кібербезпекою.

Суттєву роль відіграють інтелектуальні методи кібербезпеки (ситуаційний аналіз, інтелектуальні методи виявлення вторгнень в системи, інтелектуальна ідентифікація користувачів під час кібератак) та психологічні і поведінкові підходи (заохочення персоналу, популяризація кібербезпеки) з одночасним використанням їх для максимального впровадження інновацій у сфері криптографічного захисту [11].

Якщо зараз не використовувати сучасні засоби захисту даних, у майбутньому будуть необхідні ще більш значні витрати фінансових ресурсів порівняно з уже вкладеними інвестиціями в сучасний та ефективний захист баз даних. На рисунку 2 подані шляхи посилення кібербезпеки, яких важливо дотримуватися.



Рис. 2. Шляхи посилення кібербезпеки господарської діяльності національних бізнес-одиниць

Джерело: складено на основі даних [10].

Національні правові норми у сфері кібербезпеки потребують удосконалення, оскільки їх формулювання допускають неоднозначне тлумачення або містять свідомі законодавчі прогалини та не забезпечують принцип правової визначеності, що унеможливлює виконання завдань і функцій кібербезпеки та кіберзахисту; створює підґрунтя для конфліктів компетенції відповідних повноважних органів, порушуючи принцип розумної достатності правового регулювання [11].

Усе законодавство повинно бути спрямоване на створення та забезпечення функціонування кібервійськ, а також має бути розроблене таким чином, щоб бути взаємосумісним з аналогічними структурами країн-членів НАТО.

Україні слід використовувати досвід та практики ЄС і НАТО для створення широкої національної системи сертифікації з кібербезпеки, розробки планів реагування на великі інциденти та кризи (від національних планів реагування на надзвичайні (кризові) ситуації в кіберпросторі до планів реагування на загрози щодо конкретних об'єктів критичної інформаційної інфраструктури), розвитку та поглиблення державно-приватного партнерства та інтенсифікувати наукові дослідження у цій сфері. Військова агресія росії проти України призвела до формування нових відносин у сфері кіберзахисту та кібербезпеки. Всі вони мають бути систематизовані та уніфіковані, а законодавчі заходи з цих питань мають бути відповідним чином змінені та доповнені. Також залишаються не імplementованими низка директив ЄС з питань кібербезпеки та міжнародні стандарти у цій сфері.

Висновки

Таким чином, враховуючи наукові розробки та нормативно-правову базу кібербезпеки в економіці України, важливо формувати якісно нові форми відносин у кіберпросторі і відповідно розвивати систему з позитивними якостями. Слід зазначити, що виклик кібербезпеки стає сучасним і невід'ємним елементом, пов'язаним з політичною діяльністю в інформаційному просторі, зниженням ризику кібератак, запобіганням їхнім негативним наслідкам та поступовим вдосконаленням механізмів взаємодії. Державна політика має бути спрямована на подальше вдосконалення механізмів захисту.

Отримані дані свідчать про те, що національна економіка поступово переходить у цифровий простір у контексті європейської інтеграції. Незважаючи на воєнний стан, розвиток цифрової трансформації та цифрової економіки України триває та оновлюється. Докладаються зусилля для інституційної підтримки цього розвитку та створення умов для управлінських інновацій. Особливу роль у цьому процесі відіграє участь України в програмі «Цифрова Європа», яка має на меті прискорити економічне відновлення та цифрову трансформацію в країнах-учасниках. Та все ж на рівні національної економіки важливо стимулювати інноваційну діяльність, спрямовану на побудову ефективних організаційно-технічних моделей національної системи кібербезпеки.

Подальші дослідження мають бути спрямовані на розробку математичної моделі, яка дозволить комплексно оцінити стан цифрової трансформації та кіберзахисту економіки у світі та в Україні.

Список використаних джерел

1. Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. № 1 (84). С. 13–20. DOI: [https://doi.org/10.26906/EiR.2022.1\(84\).2540](https://doi.org/10.26906/EiR.2022.1(84).2540) (дата звернення: 17.11.2023).
2. Михальченко Г. Г., Снітко Ю. М., Іваненко В. О. Кібербезпека в економіці: захист від кіберзагроз у диджиталізованому світі. *Наукові записки Львівського університету*

- бізнесу та права. 2023. № 38. С. 377–383. DOI: <http://dx.doi.org/10.5281/zenodo.10012434> (дата звернення: 17.11.2023).
3. Семенченко А. І., Мялковський Д. В., Станіславський Т. В. Науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. *Інвестиції: практика та досвід*. 2018. № 18. С. 87–94. URL: <http://www.investplan.com.ua/?op=1&z=6303&i=16> (дата звернення: 17.11.2023).
 4. Горбаченко С. Кібербезпека як складова економічної безпеки України. *Galician economist journal*. 2020. № 5 (66). С. 180–186. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2020.0 (дата звернення: 17.11.2023).
 5. Биков В. Ю., Романовський О. О., Романовська Ю. Ю. Навчання кібербезпеки і кіберзахисту фахівців з управління фінансами, економікою і бізнесом. *ІТЗН*. 2020. № 80 (6). С. 386–413. DOI: <https://doi.org/10.33407/itlt.v80i6.4101> (дата звернення: 17.11.2023).
 6. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки України. *Підприємництво, господарство і право*. 2019. № 9. С. 100–108. DOI: <https://doi.org/10.32849/2663-5313/2019.9.17> (дата звернення: 17.11.2023).
 7. Цифровий вектор інтеграції України в ЄС: воєнні виклики сьогодення / Л. Г. Мельник та ін. *Наукові праці Міжрегіональної академії управління персоналом. Економічні науки*. 2023. № 3 (70). С. 18–26. DOI: <https://doi.org/10.32689/2523-4536/70-3> (дата звернення: 17.11.2023).
 8. Панченко О. А., Гнатенко В. С. Економічна кібербезпека в державній системі національної безпеки. *Публічне урядування*. 2021. № 2 (27). С. 22–31. DOI: [https://doi.org/10.32689/2617-2224-2021-2\(27\)-3](https://doi.org/10.32689/2617-2224-2021-2(27)-3) (дата звернення: 17.11.2023).
 9. Ігнатенко Р. В. Розвиток цифрового маркетингу у світі та в Україні. *Бізнес Інформ*. 2022. № 1. С. 450–455. <https://doi.org/10.32983/2222-4459-2022-1-450-455> (дата звернення: 17.11.2023).
 10. Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26–37. DOI: <https://doi.org/10.31649/ins.2022.3.26.37> (дата звернення: 17.11.2023).
 11. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник*. 2020. № 3. С. 18–26. DOI: <https://doi.org/10.33271/ebdut/71.018> (дата звернення: 17.11.2023).
 12. Башлай С., Яремко І. Цифровізація економіки України в умовах євроінтеграційних процесів. *Економіка та суспільство*. 2023. № 48. DOI: <https://doi.org/10.32782/2524-0072/2023-48-48> (дата звернення: 17.11.2023).
 13. Тогобицька В. Д. Цифрова економіка: виклики і перспективи для розвитку України. *Вісник національного університету цивільного захисту України*. 2019. № 1 (10). С. 444–451. URL: <http://repositc.nuczu.edu.ua/handle/123456789/16145> (дата звернення: 17.11.2023).
 14. Іртищева, І. О., Сенкевич О. Ф. Цифрова трансформація регіонів України: об'єктивна необхідність, принципи цифрового розвитку та особливості регулювання. *Регіональна економіка*. 2020. № 1. С. 14–21. DOI: <https://doi.org/10.36818/1562-0905-2020-1-2> (дата звернення: 17.11.2023).
 15. Цифрова економіка в Україні: виклики сьогодення та завдання управління / І. О. Іртищева та ін. *Ефективна економіка*. 2020. № 7. URL: <http://www.economy.nayka.com.ua/?op=1&z=8074> (дата звернення: 17.11.2023).
 16. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text> (дата звернення: 17.11.2023).

17. Про стратегію кібербезпеки України: Рішення Ради нац. безпеки і оборони України від 27.01.2016. URL: <https://zakon.rada.gov.ua/laws/show/n0003525-16#Text> (дата звернення: 17.11.2023).
18. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. № 2163-VIII : станом на 17 серпня 2022 р. <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 17.11.2023).
19. Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15.07.2021 № 1667-IX : станом на 1 січ. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text> (дата звернення: 17.11.2023).
20. Україна 2030Е – країна з розвинутою цифровою економікою. Економічна стратегія України 2030. URL: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoju.html> (дата звернення: 17.11.2023).
21. Федорак В. Як взяти участь у Програмі «Цифрова Європа»: приклади проєктів, відкриті конкурси, підготовка проєктної заявки. *Децентралізація*. URL: <https://decentralization.gov.ua/news/16008> (дата звернення: 17.11.2023).