ЕКОНОМІЧНА БЕЗПЕКА
ECONOMIC SECURITY

УДК 351/354
doi: https://doi.org/10.15330/apred.1.21.436-450

Квасній Л.Г.[1], Сисин Г.І.[2], Кебус В.М.,[3] Якубовська О.Б.[4]

РОЛЬ ДЕРЖАВНИХ ІНІЦІАТИВ У ЗМІЦНЕННІ КІБЕРБЕЗПЕКИ ЯК СТИМУЛУ РОЗВИТКУ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ В УКРАЇНІ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

[1]Дрогобицький державний педагогічний університет імені Івана Франка,
кафедра математики та економіки,
вул. Івана Франка, 24, м. Дрогобич,
82100, Україна,
тел.: (096) 742-37-21,
e-mail: lg_k@ukr.net
ORCID: https://orcid.org/0000-0001--5248-544X

[2]Прикарпатський інститут імені Михайла Грушевського ПрАТ «ВНЗ «МАУП»,
кафедра менеджменту організацій, економіки та підприємництва
вул. Івасюка, 21, м. Трускавець,
82200,Україна,
тел.: (097) 523-07-39,
e-mail: gala_sysyn@ukr.net,
ORCID: https://orcid.org/0000-0003-4957-1536

[3] ПрАТ «ВНЗ «МАУП»,
вул. Фрометівська, 21, м. Київ,
82100, Україна,
тел.: (050)0700429,
e-mail: kebus.vitalik@gmail.com
ORCID: https://orcid.org/0009-0003-4659-3243

[4] Дрогобицький державний педагогічний університет імені Івана Франка,
кафедра математики та економіки,
вул. Івана Франка, 24, м. Дрогобич,
82100, Україна,
тел.: (097) 523 9583 ,
e-mail: koledg_o@ukr.net
ORCID: https://orcid.org/0009-0007-4680-8370

Анотація. Стаття спрямована на дослідження ролі державних ініціатив у зміцненні кібербезпеки як стимулу розвитку малого та середнього бізнесу в Україні. Мета статті – є дослідження ролі державних ініціатив у зміцненні кібербезпеки як чинника стимулювання розвитку малого та середнього бізнесу в Україні в умовах євроінтеграційних процесів, а також обґрунтування напрямів удосконалення національної політики у сфері кіберзахисту для підвищення конкурентоспроможності МСП на європейському ринку. В статті обґрунтовано основні виклики та можливості забезпечення кібербезпеки малого і середнього бізнесу (МСБ) України в контексті євроінтеграції, проаналізовано відповідність національного законодавства

європейським стандартам у сфері захисту даних, а також запропоновано шляхи підвищення рівня цифрової безпеки підприємств відповідно до вимог ЄС.

Для дослідження ролі державних ініціатив у зміцненні кібербезпеки як стимулу розвитку малого та середнього бізнесу (МСБ) нами використовувались такі методи: аналіз документів та контент-аналіз; порівняльний аналіз; кейс-стаді. У статті проаналізовано основні кіберзагрози, з якими стикаються підприємства цього сектору, а також виклики, пов'язані з цифровою трансформацією та адаптацією до європейських стандартів кіберзахисту; наведено аналіз впливу державних ініціатив на кібербезпеку МСБ в Україні. Окреслено напрями вдосконалення системи безпеки МСБ. Обґрунтовано перспективи можливої інтеграції українських підприємств у європейський кіберпростір та напрями міжнародної співпраці у сфері захисту інформації.

Наукова новизна дослідження полягає в обґрунтуванні ролі державних ініціатив у сфері кібербезпеки як чинника стимулювання розвитку малого та середнього бізнесу України в контексті євроінтеграційних процесів. Запропоновано авторське бачення системи заходів державної підтримки малого та середнього бізнесу у сфері кіберзахисту як важливого елементу підвищення конкурентоспроможності українських підприємств на європейському ринку.

Стаття має практичну цінність для підприємців, державних органів та фахівців у сфері кібербезпеки, сприяючи підвищенню захисту бізнесу та його конкурентоспроможності в умовах євроінтеграції.

Ключові слова: кібербезпека, державні програми та ініціативи у сфері кібербезпеки, малий та середній бізнес, цифрова трансформація, євроінтеграція, кіберзагрози, інформаційна безпека.

Kvasniy L.G.[1], Sysyn G.I.[2], Kebus V.M.,[3] Yakubovska O.B.[4]

THE ROLE OF STATE INITIATIVES IN STRENGTHENING CYBERSECURITY AS AN STIMULATOR FOR THE DEVELOPMENT OF SMALL AND MEDIUM BUSINESSES IN UKRAINE IN THE CONDITIONS OF EUROPEAN INTEGRATION

[1] Drohobych Ivan Franko State Pedagogical University,
Department of Mathematics and Economics,
Ivan Franko St., 24, Drohobych,
82200, Ukraine,
tel.: (096) 742-37-21,
e-mail: lg_k@ukr.net
ORCID: https://orcid.org/0000-0003-1699-054X

[2]Precarpathian Institute named of Mykhailo Hrushevsky of Interregional Academy of Personnel Management,
department of management of organizations,
economy and entrepreneurship,
St. V. Ivasyuka, 21, Truskavets,
82200, Ukraine,
tel.: (097) 523-07-39,
e-mail: gala_sysyn@ukr.net,
ORCID: https://orcid.org/0000-0003-4957-1536

[3]Interregional Academy of Personnel Management,
Frometivska St., 21, Kyiv,
03930, Ukraine,
tel.: (050)0700429,
e-mail: kebus.vitalik@gmail.com
ORCID: https://orcid.org/0009-0003-4659-3243

[4] Drohobych Ivan Franko State Pedagogical University,
Department of Mathematics and Economics,
Ivan Franko St., 24, Drohobych,
82200, Ukraine,
tel.: (097) 523 9583 ,
e-mail: koledg_o@ukr.net
ORCID: https://orcid.org/0009-0007-4680-8370

Abstract. The article is aimed at exploring the role of state initiatives in strengthening cybersecurity as an incentive for the development of small and medium -sized businesses in Ukraine. The purpose of the article is to study the role of state initiatives in strengthening cybersecurity as a factor in stimulating the development of small and medium -sized businesses in Ukraine in the conditions of European integration processes, as well as justifying the directions of improvement of national policy in the field of cyber defense for improving the competitiveness of SMEs in the European market. The article substantiates the basic challenges and opportunities for providing cybersecurity of small and medium -sized businesses (IAS) of Ukraine in the context of European integration, the compliance of national legislation with European standards in the field of data protection, and the ways of raising digital security of enterprises in accordance with EU requirements are analyzed.

To study the role of state initiatives in strengthening cybersecurity as an incentive for the development of small and medium-sized businesses (IAS), we used the following methods: document analysis and cybersecurity content analysis; comparative analysis; Case stady. The article analyzes the main cyber threats facing the enterprises of this sector, as well as challenges related to digital transformation and adaptation to European cyber defense standards; The analysis of the impact of state initiatives on CISBOs of IAS in Ukraine is given.A comparative analysis of Ukrainian initiatives in the field of cybersecurity and practices of EU countries is presented. The directions of improvement of the ICB safety system are outlined. The prospects of possible integration of Ukrainian enterprises into the European cyberspair and areas of international cooperation in the field of information protection are substantiated.

The scientific novelty of the study is to substantiate the role of state initiatives in the field of cybersecurity as a factor in stimulating the development of small and medium -sized business of Ukraine in the context of European integration processes. The author's vision of the system of state support for small and medium -sized businesses in the field of cyber defense is proposed as an important element of increasing the competitiveness of Ukrainian enterprises in the European market.

The article is of practical value for entrepreneurs, public authorities and cybersecurity experts, helping to increase business protection and its competitiveness in European integration. The article has practical tips for small and medium-sized businesses to implement effective cybersecurity measures, which will increase their resistance to cyber threats and ensure the continuity of business processes.

Keywords: cybersecurity, state programs and initiatives in the field of cybersecurity, small and medium-sized businesses, digital transformation, European integration, cyber threats, information security.

Вступ. У сучасному світі кібербезпека стала важливим чинником стабільного розвитку бізнесу, особливо в умовах цифрової трансформації та зростання кіберзагроз. Для малого і середнього бізнесу (МСБ), який є основою економіки України, захист даних та інформаційних систем набуває ще більшої актуальності, у зв’язку із збільшенням кількості кібератак та викликів, спричинених війною.

Євроінтеграційний курс України передбачає поступове впровадження європейських стандартів у сферу кібербезпеки та захисту персональних даних. Зважаючи на швидке зростання кіберзагрози та посилення вимог, організаціям необхідно приділити увагу кібербезпеці без зволікань. Впровадження стандарту ISO 27001 не тільки забезпечить відповідність оновленим регуляторним нормам, а й стане основою для ефективного управління безпекою, сприяючи зниженню ризиків і зміцненню довіри клієнтів та партнерів. Таким чином, адаптація українського

законодавства до норм Загального регламенту про захист даних (GDPR) [1] та Директиви NIS2 [2] є кроком на шляху до посилення цифрової безпеки українського бізнесу та його конкурентоспроможності на європейському ринку. Кравчук В., досліджуючи проблеми кіберзахисту малого і середнього бізнесу, зауважує, що «багато власників компаній малого і середнього бізнесу не розуміють потреби у витратах на захист компанії від кіберзагроз. Однак така ситуація триває доти, доки власник не зіткнеться з кібератакою, яка може призвести до блокування процесів і сервісів підприємства, фінансових втрат, а в гіршому випадку до повної зупинки чи втрати бізнесу» [3]. Кузьменко О., Маклюк О., Чернишова О. наголошують, що «Український бізнес перебував під загрозою кібератак від початку незалежності країни, а з початком повномасштабного вторгнення кібератаки набули значних масштабів» [4]. Білявська Ю., Шестак Я. обґрунтовують кібербезпеку та кібергігієну в новій ері цифрових технологій [5].

Вишнівський В., Пампуха А. характеризують цифрову трансформацію кібербезпеки [6]. Віннікова І., Марчук наголошують, що «щодня тисячі малих підприємств в усьому світі піддаються кібер-атакам. Крадії намагаються вкрасти інформацію та гроші, або втрутитися в бізнес» [7, с. 110]. В дослідженнях Тимошенко О., Гаврилюк О. акцентовано увагу на кібербезпеці та штучному інтелекті у контексті забезпечення безпеки підприємництва у військовий час [8].

Однак, при впровадженні європейських стандартів, малий і середній бізнес в Україні часто стикається з низкою проблем у сфері кібербезпеки. До них належать обмежені фінансові ресурси для впровадження сучасних систем захисту, недостатня обізнаність підприємців з кіберризиками, поява комплексних механізмів державної підтримки, а також загрози, пов’язані з активізацією військових кібератак з боку російських хакерських угруповань. Нами проведено комплексний аналіз впливу державної політики на кібербезпеку МСБ в контексті інтеграції України до європейського цифрового простору та досліджено взаємозв’язок між державними ініціативами у сфері кібербезпеки та конкурентоспроможності МСБ, що сприятиме підвищенню ефективності таких ініціатив як стимулу для розвитку бізнесу в контексті євроінтеграції.

Постановка завдання. Кіберзлочинність – все більший виклик для бізнесу у всіх країнах. Україна в топі ризикованих країн [9].

Мета статті – дослідження ролі державних ініціатив у зміцненні кібербезпеки як чинника стимулювання розвитку малого та середнього бізнесу в Україні в умовах євроінтеграційних процесів, а також обґрунтування напрямів удосконалення національної політики у сфері кіберзахисту для підвищення конкурентоспроможності МСП на європейському ринку.

Для дослідження ролі державних ініціатив у зміцненні кібербезпеки як стимулювання розвитку малого та середнього бізнесу (МСБ) в Україні в умовах євроінтеграції нами використовувались такі методи: аналіз документів та контент-аналіз у сфері кібербезпеки; порівняльний аналіз при порівнянні українських державних ініціатив у сфері кібербезпеки з практиками країн ЄС; опитування та інтерв'ю при зборі даних від представників МСБ щодо їх досвіду, потреби та оцінки впливу державних ініціатив на їх кібербезпеку; кейс-стаді при розгляді конкретних прикладів МСБ, які успішно адаптовані до вимог кібербезпеки завдяки державній підтримці.

Результати. Україна є однією з країн, що зазнають найбільшу кількість кібератак у світі. Згідно зі звітом Європейського сховища кіберзлочинів (EuRepoC), опублікованим у березні 2024 року, Україна дає п’яте місце за кілька політично вмотивованих кібератків, з часткою 2,6% від загальної кількості. Лідерами цього

рейтингу є Китай (майже 12%), Росія (11,6%), Іран (5,3%) та Північна Корея (4,7%) [10].

Інтеграція до Європейського союзу (ЕС) вимагає подальшої гармонізації законодавства у різних сферах, включно з кібербезпекою. Це передбачає адаптацію національних стандартів захисту інформації до вимог Директиви NIS2 та Регламенту GDPR, що регулюють безпеку цифрової інфраструктури та обробку персональних даних. «Щодня людство виробляє 2,5 ексабайта інформації, при цьому обсяг бізнес-даних подвоюється кожні 14 місяців. «Розумні» пристрої та нові послуги можуть бути причиною непередбачених наслідків та загроз» [7, с. 110]. Малий та середній бізнес (МСБ) в Україні змушений пристосовуватися до цих змін, забезпечуючи відповідність новим правилам, що стає викликом через обмежені ресурси та недостатній рівень обізнаності про сучасні кіберзагрози.

Малий та середній бізнес (МСБ) в Україні стикається з новими викликами у сфері захисту даних, спричиненими цифровізацією, поширенням роботи в онлайн-середовищі та посиленням кіберзагроз. Державні ініціативи у сфері кібербезпеки поступово підвищують обізнаність малого та середнього бізнесу про сучасні кіберзагрози та необхідні захисні заходи. Впровадження освітніх програм, рекомендацій та грантової підтримки стимулює МСБ до використання базових засобів кіберзахисту і адаптації до європейських стандартів. Однак обмежені фінансові ресурси та недостатній рівень впровадження державних інструментів поки що залишають підприємства цього сектора вразливими до складних кібератак.

Таблиця 1

Основні виклики та можливості для МСБ України у сфері кібербезпеки в контексті євроінтеграції та впровадження норм GDPR та NIS2 в національне законодавство

Table 1

Key challenges and opportunities for Ukrainian SMEs in the field of cybersecurity in the context of European integration and the implementation of GDPR and NIS2 norms into national legislation

Категорія	Виклики	Можливості
Законодавче регулювання	1. Необхідність адаптації бізнесу до вимог GDPR та NIS2. 2. Високі штрафи за порушення норм захисту даних. 3. Недостатня кількість спеціалістів із правового супроводу кібербезпеки.	1. Гармонізація українського законодавства з європейськими нормами, що сприяє виходу на міжнародні ринки. 2. Підвищення рівня захисту персональних даних, що зміцнює довіру клієнтів.
Фінансові аспекти	1. Високі витрати на впровадження стандартів кібербезпеки. 2. Обмежені фінансові ресурси для впровадження сучасних технологій захисту.	1. Доступ до грантів і програма підтримки від ЄС та міжнародних організацій. 2. Зменшення негативних фінансових втрат від кібератаків у довгостроковій перспективі.
Технологічна спроможність	1. Відсутність єдиних стандартів кіберзахисту серед українського МСБ. 2. Високий рівень кіберзагрози та атак на бізнес.	1. Доступ до передових європейських технологій у сфері кібербезпеки. 2. Можливість залучення європейських інвесторів і партнерів відповідно до стандартів.

Категорія	Виклики	Можливості
	3. Низька обізнаність щодо сучасних методів захисту даних.	
Кадрове забезпечення	1. Дефіцит кваліфікованих фахівців у сфері кібербезпеки. 2. Висока вартість навчання персоналу.	1. Розвиток державних і міжнародних програм підготовки фахівців. 2. Зростання послуг з аутсорсингової кібербезпеки.
Довіра та конкурентоспроможність	1. Низький рівень довіри клієнтів до захисту своїх персональних даних. 2. Відсутність сертифікації відповідності європейським стандартам у багатьох компаніях.	1.Підвищення конкурентоспроможності українських компаній на ринку ЄС. 2. Формування іміджу надійного бізнес-партнера.

**Джерело: сформовано авторами на основі [4 – 9]*

В табл. 1 представлено основні виклики та можливості, з якими стикається малий та середній бізнес України у сфері кібербезпеки в контексті євроінтеграції.

Науковці зауважують, що «Організації малого та середнього бізнесу стають усе більш залежними від інформаційних систем, що робить їх уразливими для кіберризиків: витоку даних внаслідок кібератак і комп'ютерних вірусів, втрати даних через людський фактор або збої у роботі носіїв інформації» [7, С. 110].

Крім того, малий та середній бізнес часто не має доступу до власних ІТ-відділів, що призводить до залежності від сторонніх підрядників, які не завжди забезпечують належний рівень безпеки. Відсутність систематичного навчання персоналу збільшує ризики соціальної інженерії та фішингових атак, які залишаються одними з найбільших загроз для бізнесу.

Таблиця 2

Державні ініціативи України, що впливають на кібербезпеку та цифровізацію малого і середнього бізнесу (МСБ)

Table 2

Ukraine's state initiatives that affect the cybersecurity and digitalization of small and medium -sized businesses (IAS)

Державна ініціатива	Суть та вплив на МСБ
Національна стратегія кібербезпеки України (2021)	Визначає захист підприємницького середовища як пріоритет. Вимагає підвищення стійкості бізнесу до кіберзагроз.
Закон України "Про основні засади забезпечення кібербезпеки" (2017)	Створює правову базу для захисту бізнесу, вводить поняття критичної інфраструктури, до якої можуть належати й великі МСБ.
Програма "Дія.Бізнес"	Державна платформа підтримки підприємців, включає освітні курси з цифрової безпеки, консультації щодо захисту бізнесу онлайн.
Нацпроект "Дія" та е-сервіси для бізнесу	Запуск електронної реєстрації ФОП та ТОВ, отримання ліцензій онлайн – все це супроводжується стандартами кіберзахисту.

Державна ініціатива	Суть та вплив на МСБ
CERT-UA (урядова команда реагування на кіберінциденти)	Розсилає рекомендації та попередження про кібератаки, у т.ч. для бізнесу. Надає інструкції для МСБ щодо базового захисту.
Програма EU4Digital (спільно з ЄС)	Сприяє цифровій трансформації МСБ у регіонах України, передбачає навчання підприємців цифровій безпеці та захисту даних.
Національний банк України (НБУ) – вимоги до фінансових сервісів	Запроваджує стандарти кіберзахисту для платіжних систем, фінтеху, якими користується малий бізнес.
Мінцифри – концепція "Безпечна цифровізація бізнесу" (ініціатива 2023 р.)	Розробка рекомендацій та грантових програм для МСБ на впровадження систем кібербезпеки (наприклад, для інтернет-магазинів).

**Джерело: сформовано авторами на основі [4 – 11]*

Останніми роками хакерські атаки стають більш складними та цілеспрямованими, а кіберзлочинці використовують сучасні технології, такі як штучний інтелект, автоматизовані боти та фішингові кампанії, щоб отримати несанкціонований доступ до даних компаній. Особливої уваги потребують атаки на критичну інфраструктуру, злам корпоративних мереж, витоки конфіденційної інформації та шкідливе програмне забезпечення (наприклад, програми-вимагачі). Для МСБ такі загрози можуть мати руйнівні наслідки, оскільки вони часто не мають достатніх ресурсів для швидкого відновлення після інцидентів.

Швидкий розвиток інформаційних технологій призводить до появи нових ризиків і загроз у кіберпросторі. Хмарні сервіси, блокчейн, Інтернет речей (IoT) – усі ці технології, хочуть і значно підвищують ефективність роботи, водночас відкривають додаткові вразливі місця для кібератак як у професійному, так і в особистому середовищі.

Практика показує, що кіберзлочинність виникає в різноманітних формах, включаючи шахрайство з персональними даними, викрадання інформації, атаки із застосуванням програм-вимагачів, фішингові кампанії, а також цілеспрямовані атаки на критичну інфраструктуру. Зростаюча стійкість та масштабність таких загроз постійно вимагає вдосконалення заходів кібербезпеки, підвищення обізнаності користувачів і розробки надійних механізмів захисту.

У 2020 році під впливом COVID-19 бізнес зіштовхнувся з фінансовими проблемами та бюджетними обмеженнями, надаючи перевагу основним оперативним процесам, а не інвестиціям у кібербезпеку. Ресурси були перерозподілені на підтримку віддаленої роботи, що призвело до скорочення витрат на рішення з кібербезпеки. Крім того, збільшена кількість хакерських атак та загроз через швидкий перехід до дистанційного формату роботи загострила час, вимагаючи перегляду підходів до захисту інформаційних систем. «Підприємництво складає невід'ємну частину життєдіяльності будь-якої країни. Його стабільний стан та безпека функціонування детермінують успішність соціально-економічного, технологічного, інноваційного та інформаційного розвитку суспільства. Умови воєнного часу вносять ряд особливостей у здійснення підприємницької діяльності»[8].

Таблиця 3

Особливості, інструменти, цілі, пріоритети державної політики у сфері захисту кіберпростору

Table 3

Features, tools, goals, public policy priorities in the field of cyberspace protection

Категорія	Характеристика з прикладами для України
Особливості	- Комплексність – політика охоплює законодавство, технічні стандарти, освіту, міжнародну співпрацю - Адаптивність – регулярне оновлення стратегії кібербезпеки (остання редакція 2021 р.) - Міжвідомча взаємодія – участь СБУ, Держспецзв'язку, Нацполіції, НБУ та Мінцифри - Міжнародна координація – інтеграція у структури НАТО, ЄС (процес імплементації Директиви NIS2) - Захист критичної інфраструктури – насамперед енергетика, фінансовий сектор, зв'язок, транспорт
Інструменти	- Нормативно-правова база – Закон України "Про основні засади забезпечення кібербезпеки України" (2017), Стратегія кібербезпеки (2021), імплементація європейських норм - Державні програми і проєкти – нацпроєкт "Дія", розвиток електронних послуг з урахуванням безпеки - CERT-UA – урядовий центр реагування на комп'ютерні інциденти - Контроль і моніторинг – аудит захисту інформації в органах влади та критичній інфраструктурі - Освітні програми – ініціатива "Кібербезпека: захисти себе в інтернеті" для підприємців - Державно-приватне партнерство – співпраця з бізнесом через платформи кібербезпеки при Мінцифрі
Цілі	- Забезпечення національної безпеки в умовах гібридної війни - Захист прав громадян при використанні цифрових сервісів ("Дія", е-ідентифікація) - Захист критичної інфраструктури від кібератак (особливо в енергетиці та фінансах) - Підвищення довіри до електронного урядування та цифрових послуг - Стимулювання МСП до цифровізації шляхом підтримки кіберстійкості
Пріоритети	- Гармонізація з правом ЄС – імплементація Директиви NIS2 до 2027 р., адаптація стандартів ENISA - Захист критичної інфраструктури – введення категоризації об'єктів критичної інформаційної інфраструктури (КІІ) - Розвиток реагування на інциденти – підсилення спроможностей CERT-UA та регіональних підрозділів - Підтримка МСП – субсидії на кіберзахист, освітні програми, консалтинг для малого бізнесу (приклад – програма EU4Digital) - Міжнародне співробітництво — участь у програмах НАТО CCDCOE, співпраця з ЄС у рамках Східного партнерства

**Джерело: сформовано авторами на основі [4 – 5]*

У багатьох компаніях, зокрема малих та середніх підприємствах, недостатньо коштів для модернізації інфраструктури безпеки, що зробило їх вразливими до нових видів атаки. Науковці наголошують, що «особливу стурбованість потенційні кібератаки викликають у підприємств сфери торгівлі й комунікаційних технологій, а також малого та середнього бізнесу» [8, с.7]. У період 2020-2021 рр. також зросла важливість управління ризиками та інтеграції кібербезпеки в стратегічне планування бізнесу, після чого безпека стала критичним елементом для забезпечення безперервності бізнесу в умовах пандемії.

Важливим чинником залишається низький рівень кіберграмотності серед працівників, що підвищує ризик успішного проведення атак соціальної інженерії. Водночас зростаючий обсяг регулювання, зокрема впровадження норм GDPR та NIS2, вимагає від підприємств дотримання нових стандартів безпеки, що, хоч і потребує додаткових ресурсів, водночас відкриває можливості для підвищення довіри клієнтів та партнерів.

Помірне зростання ринку у 2022 році було зумовлено релокаціями компаній МСБ та закриттями офісів, що призвели до зменшення внутрішнього попиту на кібербезпеку та сповільнення росту інвестицій. Перехід на гібридні моделі роботи та масове використання віддалених платформ зменшили потребу в традиційних рішеннях для захисту офісної інфраструктури, що негативно вплинуло на ринок фізичних кіберзахисних технологій. Однак збільшення кількості віддалених співробітників і нові загрози, пов'язані з хмарними технологіями, підштовхнули компанії до інвестицій у нові інструменти кібербезпеки, зокрема для захисту кінцевих пристроїв та безпечного доступу до даних. Попри загальне зниження попиту, зростання інтересу до рішень для захисту хмарних середовищ і управління ризиками в кіберпросторі стало основним драйвером розвитку ринку в 2022 році. Також важливим чинником було зростання регулювань і нормативних вимог, що змусило бізнеси переглянути свої стратегії кібербезпеки та сприяло розвитку ринку послуг і рішень для забезпечення відповідності стандартам.

З метою підвищення конкурентоспроможності малого та середнього бізнесу України на європейському ринку доцільно сформувати інтегровану систему державної підтримки МСБ у сфері кібербезпеки, яка повинна включати такі ключові елементи:

1. Фінансова підтримка заходів кіберзахисту:

- запровадження державних грантів та субсидій для МСБ на придбання ліцензованого програмного забезпечення, систем захисту інформації та проведення аудитів кібербезпеки;
- податкові пільги для підприємств, які інвестують у впровадження систем кіберзахисту відповідно до європейських стандартів.

2. Освітньо-консультаційна підтримка:

- створення на базі платформи "Дія.Бізнес" єдиної освітньої програми з кібербезпеки для підприємців з акцентом на вимоги ринку ЄС;
- організація національної мережі центрів консультування МСБ з питань кібербезпеки та цифровізації.

3. Нормативно-правова стимуляція:

-гармонізація українського законодавства з Директивою NIS2 та іншими актами ЄС, що регулюють кіберзахист бізнесу;

- запровадження добровільної сертифікації МСБ за стандартами кібербезпеки ЄС як інструменту підвищення довіри з боку європейських партнерів.

4. Інфраструктурна підтримка:

- розвиток спільних для МСБ центрів кіберзахисту на регіональному рівні (Public Security Operation Centers – SOC), які надаватимуть послуги моніторингу та реагування на інциденти;

- інтеграція МСБ до національної системи раннього попередження про кіберзагрози (CERT-UA) з доступом до актуальних рекомендацій та інструментів захисту.

5. Міжнародне співробітництво та інтеграція:

- розширення участі українських МСБ у програмах ЄС (наприклад, Digital Europe Programme) з отриманням доступу до новітніх технологій кіберзахисту;

- проведення спільних тренінгів і навчальних заходів за участю європейських експертів з кібербезпеки.

Застосування такої системи заходів дозволить українським малим і середнім підприємствам не лише мінімізувати кіберризики, а й підвищити свою привабливість для європейських партнерів, які все більше орієнтуються на відповідність високим стандартам кібербезпеки. Це сприятиме інтеграції українського бізнесу в єдиний цифровий ринок ЄС і розширенню його експортного потенціалу.

Разом з тим, вразливість МСБ залишається підвищеною через обмежені фінансові та кадрові ресурси для повноцінного захисту. Саме тому державні ініціативи відіграють ключову роль як стимулюючий і компенсуючий фактор для підвищення кіберстійкості малого бізнесу.

Політика кібербезпеки МСБ визначається такими документами:

- Міжнародні документи (Директива NIS2 ЄС, стандарти ISO/IEC 27001);

- Національні стратегії та закони (Стратегія кібербезпеки України, Закон України «Про основні засади забезпечення кібербезпеки»);

- Документи регуляторів (постанови НБУ, рекомендації Держспецзв'язку);

- Політики великих компаній (кіберстратегії корпорацій, що визначають ринкові стандарти).

Проблемою є й імплементація GDPR, оскільки для багатьох підприємств, особливо у сфері МСБ, це означає необхідність значних змін у підходах до збору, обробки та зберігання персональних даних. Вимоги Регламенту передбачають суворий контроль над обробкою інформації, обов’язкове отримання згоди від суб’єктів даних, право клієнтів на видалення своїх даних, а також необхідність повідомляти про витоки інформації в стислі терміни.

Однією з головних проблем для українського бізнесу є відсутність достатньої правової та технічної експертизи щодо відповідності GDPR. Багато компаній не мають внутрішніх фахівців із захисту даних (Data Protection Officer – DPO), що ускладнює належне застосування регламенту та створює ризики правопорушення. Крім того, виконання вимог потребує додаткових фінансових витрат на оновлення IT-інфраструктури, проведення аудитів безпеки та адаптацію політик конфіденційності.

Отже, Україна поступово наближається до стандартів ЄС, але поки що існують розриви, особливо в частині охоплення МСБ та фінансової підтримки їх кіберзахисту. В ЄС вже діє обов'язкова відповідальність середнього бізнесу за відповідність стандартам кібербезпеки, з конкретними фінансовими та адміністративними стимулами для підприємств. Українські ініціативи наразі зосереджені на освітніх та консультативних заходах, тоді як у країнах ЄС більше застосовуються системні фінансові інструменти та стандартизовані практики сертифікації.

Таблиця 4

Порівняльний аналіз українських ініціатив у сфері кібербезпеки та практик країн ЄС

Table 4

Comparative analysis of Ukrainian cybersecurity and practices of EU cybersecurity and practices

Критерій	Україна	Країни ЄС
Законодавча база	Закон України «Про основні засади забезпечення кібербезпеки» (2017), Стратегія кібербезпеки (2021)	Директива NIS (2016), оновлена Директива NIS2 (2022)
Охоплення МСБ	МСБ поки що опосередковано охоплюється нормами, акцент — на критичній інфраструктурі	Директива NIS2 вже прямо поширюється на середні підприємства в окремих секторах
Інституційна структура	Головні органи — Держспецзв'язку, CERT-UA, НКЦК при РНБО	В кожній країні діє національний компетентний орган і CSIRT з обов'язками координації
Підтримка МСБ у кіберзахисті	Переважно інформаційна (платформа "Дія.Бізнес", рекомендації CERT-UA); окремі гранти Мінцифри	В ЄС діють програми фінансування кіберзахисту МСБ (наприклад, Digital Europe Programme) та податкові стимули
Системи раннього попередження	CERT-UA надає попередження та рекомендації бізнесу	У ЄС розвиненіші системи обміну інформацією через мережі CSIRTs Network та European Cyber Shield
Імплементація стандартів	В процесі гармонізації із європейськими стандартами ISO/IEC та NIS2	Широко застосовуються обов'язкові стандарти та сертифікації (ENISA, ISO, ETSI)
Освітні програми з кібербезпеки	Починають впроваджуватись, але поки що точково	У країнах ЄС діють національні програми підвищення кіберкваліфікації МСБ, часто з державною підтримкою

**Джерело: сформовано авторами на основі [11 – 13]*

Практика показує, що в залежності від розміру, компанії можуть витрачати від 10 до 50% свого річного бюджету на кібербезпеку. Науковці зауважують, що «кіберпростір стає середовищем, де існує велика кількість суб'єктів, метою діяльності яких є заволодіння особистими даними споживачів, даними бізнес-суб'єктів платіжними системами, коштами чи особистими даними інтернеткористувачів» [12]. Через ризик пошкодження сервісів і систем під час російського вторгнення компанії почали переносити свою ІТ-інфраструктуру в хмарні сервіси. Після початку агресії з боку росії Національний банк України дозволив фінансовим установам переміщати

дані та системи за межі країни, що сприяло збільшенню попиту на хмарні технології [13]. Статистика показує, що 592 млрд доларів США становлять витрати на публічні хмарні сервіси у світі у 2023 році [13].

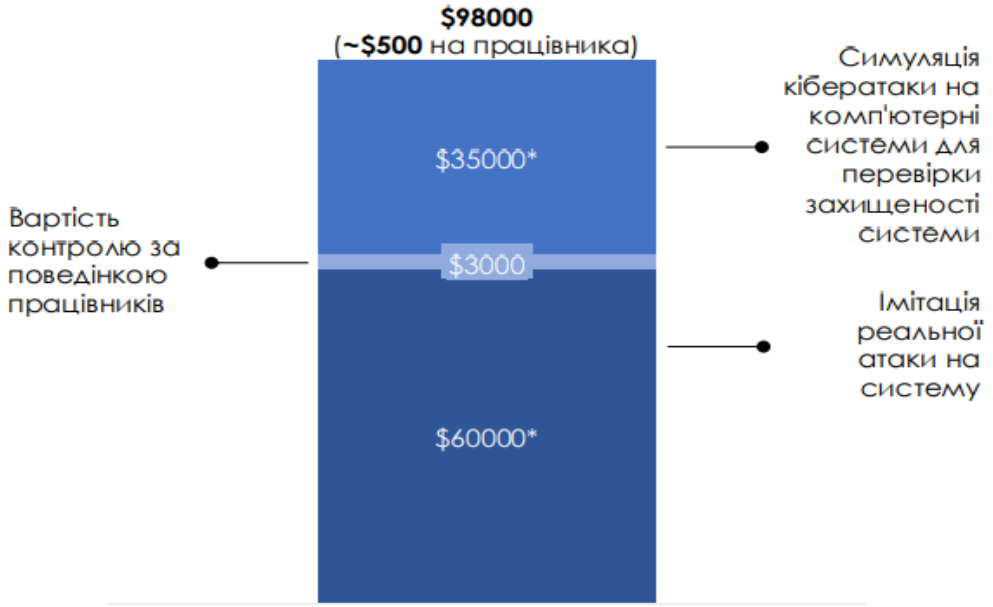

Рис. 1. Витрати на кіберзахист компанії в Україні в 2023 (На прикладі компанії розміром в 200 працівників)

Fig.1. Cost of the company's cyber defense in Ukraine in 2023 (for an example of a company in size in 200 employees)

«Молоді українські стартапи в галузі кібербезпеки мають значний потенціал для зростання, зокрема завдяки фокусу на малому та середньому бізнесі (МСБ). Вони отримують фінансування через гранти від Brave1, USAID та USF, з сумами від $12 000 до $194 000. Попри обмежену інвестиційну активність, успішні стартапи, як Osavul, Mantis Analytics та SOC Prime, демонструють позитивні результати»[14]

Імплементація GDPR має і позитивні аспекти. Дотримання стандартів захисту персональних даних підвищує рівень довіри клієнтів, спрощує вихід на ринки ЄС і сприяє створенню культури кібербезпеки в компаніях. Крім того, адаптація до європейських норм дозволяє бізнесу запровадити сучасні методи управління даними, зменшуючи ризики витоків та кібератак.

Системні інтегратори – це сервісні компанії з кібербезпеки повного циклу, які спеціалізуються на впровадженні різних технологій безпеки в єдине рішення. Вони надають комплексні послуги для забезпечення повного захисту бізнесу від кіберзагроз. 60% з найбільших вітчизняних системних інтеграторів надають послуги з кібербезпеки [15]. Проте на практиці послуги системних інтеграторів часто занадто дорогі для малих та середніх підприємств, що робить їх доступними переважно для великих компаній зі значними бюджетами.

«На українському ринку кібербезпеки значно домінують міжнародні компанії, які надають передові рішення та послуги. Дані гравці пропонують комплексні інструменти кібербезпеки, які все ширше впроваджуються бізнесом та державними організаціями по всій країні. Вітчизняним розробникам необхідно шукати конкурентну перевагу над світовими компаніями» [15, с. 26]. Дослідження показують, що в середньому країни витрачають на кібербезпеку від 0,05% до 0,2% ВВП. Наприклад, США витрачають понад 10 млрд дол. на рік лише на федеральний рівень кіберзахисту. В країнах ЄС витрати на кібербезпеку складають 0,1-0,15% ВВП. В Україні у 2024 році на

кібербезпеку виділили близько 2,3 млрд грн (приблизно 0,1% ВВП України). Ці кошти розподіляються між Держспецзв'язком, кіберполіцією, СБУ та Міноборони (на військову кібербезпеку) [16].

Індустрія кібербезпеки в Україні потребує стимулювання. «Нова ера кібербезпеки потребує цілком нових підходів до управління підприємством та його ресурсами, зокрема інформаційними. Успіх таких змін значною мірою залежить від того, наскільки гнучко організовані бізнес-процеси на підприємстві, а також як імплементуються нові моделі та методи роботи» [4].

Міжнародні програми допомоги, які є основним джерелом фінансування споживання продуктів та послуг у сфері кібербезпеки, часто віддають перевагу вибору компаній зі свого національного ринку, ігноруючи пропозиції на українському ринку. Подальша реалізація такої політики на великих масштабах може призвести до деградації українського ринку.

Державі доцільно впровадити програми та заходи, які сприятимуть розвитку конкурентоспроможності національної індустрії, зокрема через можливу локалізацію досліджень та розробок (R&D) у сфері кібербезпеки, що, серед іншого, забезпечить отримання унікальної інформації в умовах кіберагресії проти України. Взаємозв’язок між державними ініціативами у сфері кібербезпеки та конкурентоспроможності малого та середнього бізнесу (МСБ) є суттєвим і багатогранним. Ефективна державна політика в цій сфері може суттєво вплинути на розвиток та стійкість МСБ.

Практика показує, що державні ініціативи, спрямовані на покращення кібербезпеки, створюють середовище довіри для бізнесу та споживачів. Захищеність від кіберзагрози забезпечує стабільність роботи та збереження конфіденційної інформації, що є важливим для репутації компаній.

Інвестування держави в інфраструктуру кібербезпеки та розробку нормативно-правових актів сприятимуть зменшенню ризиків кібератак. Це, у свою чергу, зменшує кількість фінансових втрат для МСБ, пов’язаних з інцидентами кібербезпеки, що підвищує їх конкурентоспроможність.

Державні програми, які підтримують цифровізацію та впровадження новітніх технологій, стимулюють МСБ до інноваційного розвитку. Це дозволяє бізнесу адаптуватися до сучасних викликів та ефективніше конкурувати на ринку. Також, стратегія розвитку МСБ в Україні включає інноваційність та цифровізацію як ключові напрямки, що сприяють відновленню бізнесу та його адаптації до нових умов.

Відповідність міжнародним стандартам кібербезпеки, досягнута державними ініціативами, відкриває для МСБ можливості виходу на міжнародні ринки. Це розширює їх потенціал і забезпечує конкурентоспроможність на глобальному рівні.

Таким чином, державні ініціативи у сфері кібербезпеки є фактором виробництва, що впливає на конкурентоспроможність МСБ, забезпечуючи їм стабільність, можливості для розвитку та інтеграції у світову економіку.

На нашу думку, державі важливо не лише декларативно визнавати, але й активно впроваджувати принцип розвитку державно-приватного партнерства як один із пріоритетів політики в сфері кібербезпеки. Підприємствам доцільно об'єднувати свої зусилля через організацію конференцій, комітетів та клубів для системного просування інтересів та взаємодії усіх стейкхолдерів кібербезпеки в Україні.

Попри ці виклики, євроінтеграція сприятиме доступу МСБ до грантових програм, впровадження ініціатив ЄС з підвищення рівня кіберзахисту, а також впровадження аутсорсингових рішень з кібербезпеки. Використання хмарних сервісів із вбудованими засобами захисту, автоматизація процесів кібербезпеки та співпраця з

національними центрами реагування на кіберінциденти сприятиме підвищенню стійкості малого та середнього бізнесу до кібератак.

Висновки. Захист даних в МСБ – неодмінна умова євроінтеграції. Євроінтеграційний процес забезпечує поступ впровадження національних і галузевих практик безпеки, норм відповідності для цифрових продуктів і послуг, що призведе до попиту на більш широке впровадження організаційно-технічних заходів безпеки. Враховуючи стандарти ЄС у сфері кібербезпеки, як NIS2, компанії будуть змушені посилити захист своїх інформаційних систем, дотримуючись європейських вимог щодо безпеки мережевих та інформаційних систем. Це зумовити потребу в оновленні інфраструктури та технологій, зокрема для захисту персональних даних, що також відповідає вимогам GDPR, і забезпечення безпеки на всіх етапах життєвого циклу цифрових продуктів.

Важливим чинником стане інтеграція кібербезпеки в корпоративну культуру та операційну діяльність підприємств, після впровадження заходів безпеки не буде лише вимогою, але й конкурентною перевагою на ринку ЄС. Очікується також підвищення попиту на послуги з консалтингу у сфері кібербезпеки та навчання персоналу, після чого бізнесу будуть потрібні спеціалісти, які швидко інтегрують цю практику відповідно до європейських стандартів і забезпечують відповідність вимогам безпеки.

Стаття має практичну цінність для підприємців, державних органів та фахівців у сфері кібербезпеки, сприяючи підвищенню захисту бізнесу та його конкурентоспроможності в умовах євроінтеграції.

В статті сформовано практичні поради для малого та середнього бізнесу щодо впровадження ефективних заходів кібербезпеки, що сприятимуть підвищенню їх стійкості до кіберзагроз та забезпеченню безперервності бізнес-процесів. Співпраця з державними та міжнародними ініціативами з кібербезпеки також може стати важливим кроком для зниження ризиків і зміцнення захисту бізнесу..

Перспективи подальших досліджень полягатимуть у формуванні проактивного підходу, аналізі інвестицій у безпеку та швидкого реагування, що сприятиме зниженню ризиків й забезпеченню стабільності і конкурентоспроможності бізнесу.

1. Загальний регламент про захист даних (GDPR). Офіційний переклад українською мовою. URL: kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення: 02.02.2025)
2. Директива кібербезпеки NIS2. URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua (дата звернення: 02.02.2025)
3. Кравчук В. Проблеми кіберзахисту малого і середнього бізнесу. URL: https://elartu.tntu.edu.ua/bitstream/lib/44408/2/IMSTT_2023_Kravchuk_V-Cybersecurity_issues_for_64-65.pdf (дата звернення: 02.02.2025)
4. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. №44. URL: https://doi.org/10.32782/2524-0072/2022-44-21
5. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59.
6. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпеки: науково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій Навчально-наукового інститут захисту інформації. Київ, 2022. С. 31–33
7. Віннікова І. І., Марчук С.В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу і управління ними. *Східна Європа: Економіка, Бізнес та управління*. 2018. Випуск 5(16). С. 110-115
8. Тимошенко О.І., Гаврилюк О. В. Кібербезпека та штучний інтелект у контексті забезпечення безпеки підприємництва у військовий час. Актуальні питання забезпечення кібербезпеки та захисту інформації: Матеріали IX Міжнарод. наук.-практ. конф., Київ, 30 березня 2023 р. / Редкол.: О. І. Тимошенко та ін. К.: Вид-во Європейського університету, 2023.
9. Квасній Л. Г., Квасній З. В., Грицко О. М. Управління ефективністю стратегії цифрового бізнесу. *Публічне урядування*. 2022. №2 (30). С. 40-46. URL: https://doi.org/10.32689/2617-2224-2022-2(30)-5

10. Держустанови й банки під шквалом кібератак. *Forbes Ukraine.* 2025. №1.
11. Баловсяк Н. Україна увійшла до переліку найбільш атакованих в кіберпросторі країн світу. *Інтернет свобода*. 2024
12. Бондар-Підгурська О. В., Хоменко І. І. Науково-методичні засади оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу: кібербезпека та інтелектуальна власність. *Проблеми економіки*. 2022. №2. С. 108–116. URL: https://doi.org/10.32983/2222-0712-2022-2-108-116
13. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html (дата звернення: 02.02.2025)
14. В Україні ринок кібербезпеки ринок кібербезпеки зросте на 50% до 2029 року. URL: https://dou.ua/lenta/news/ukraine-cybersecurity-market-review/(дата звернення: 02.02.2025)
15. Огляд ринку кібербезпеки в Україні. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf. (дата звернення: 02.02.2025)
16. Звіт Держспецзв'язку України про стан кібербезпеки (2023-2024) — щорічні звіти про фінансування та інциденти. URL: https://cip.gov.ua/uk/reports (дата звернення: 02.02.2025)

References

1. General Data Protection Regulation (GDPR). KMU, kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf. Accessed 02 Feb.2025.
2. NIS2 Cybersecurity Directive, www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua. Accessed 02 Feb.2025.
3. Kravchuk V. "Problems of cyber security of small and medium-sized businesses". tntu, elartu.tntu.edu.ua/bitstream/lib/44408/2/IMSTT_2023_Kravchuk_V-Cybersecurity_issues_for_64-65.pdf. Accessed 02 Feb.2025.
4. Kuzmenko, O., Maklyuk, O., and O.Chernyshova. "Cyber security of business during war." *Economy and society*, no.44, 2022, https://doi.org/10.32782/2524-0072/2022-44-21
5. Bilyavska Yu., and Ya. Shestak. "Cybersecurity and cyberhygiene: a new era of digital technologies." *Goods and Markets*, no. 3, 2022, p. 47–59.
6. Vyshnivskyi, V. V., and A. I. Pampukha. "Cybersecurity in Ukraine". *Digital Transformation of Cybersecurity: Scientific and Practical Internet Conference, April 20, 2022*. State University of Telecommunications Educational and Scientific Institute of Information Protection, 2022, pp. 31–33.
7. Vinnikova, I. I., and S. V. Marchuk. "Cyber risks as one of the types of modern risks in the activities of small and medium-sized businesses and their management". *Eastern Europe: Economics, Business and Management*, issue 5 (16), 2018, pp. 110-115
8. Tymoshenko, O. I., and O. V. Gavrilyuk. "Cybersecurity and artificial intelligence in the context of ensuring the security of entrepreneurship in wartime". *Current issues of ensuring cybersecurity and information protection: Materials of the IX International Scientific and Practical Conference. conference, Kyiv, March 30, 202*3. Publishing House of the European University, 2023, pp. 6 – 8.
9. Kvasniy, L. G., Kvasniy, Z. V., and O. M. Hrytsko. "Managing the effectiveness of digital business strategy." *Public Governance*, 2022, no.2 (30), pp.40-46, https://doi.org/10.32689/2617-2224-2022-2(30)-5.
10. "State institutions and banks under a barrage of cyberattacks." *Forbes Ukraine*, no.1, 2025
11. Balovsyak, N. "Ukraine is included in the list of the most attacked countries in cyberspace". *Internet Freedom*, 2024
12. Bondar-Pidhurska, O. V., and I. I. Khomenko."Scientific and methodological principles for assessing the effectiveness of the information security management process of small and medium-sized businesses: cybersecurity and intellectual property". *Problems of Economy*, no. 2, 2022, pp. 108–116, https://doi.org/10.32983/2222-0712-2022-2-108-116. Accessed 02 Feb.2025.
13. "Cybersecurity of business in conditions of instability." PWC, www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html. Accessed 02 Feb.2025.
14. "In Ukraine, the cybersecurity market will grow by 50% by 2029." Dou, dou.ua/lenta/news/ukraine-cybersecurity-market-review/Accessed 02 Feb.2025.
15. "Review of the cybersecurity market in Ukraine." It-Ukraine association, itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf. Accessed 02 Feb.2025.
16. "The State Security Service of Ukraine on Cyber Security (2023-2024)-annual financing reports and incidents." The State Security Service of Ukraine, cip.gov.ua/en/reports Accessed 02 Feb.2025.

Дата подання: 15.04.2025