

DOI: <https://doi.org/10.32782/2524-0072/2024-68-5>

УДК 65.012

ПІДХОДИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ІТ-СЕКТОРУ: МІЖНАРОДНИЙ ОГЛЯД

APPROACHES OF PROVIDING ECONOMIC SECURITY OF IT-SECTOR: AN INTERNATIONAL OVERVIEW

Блинков Володимир Геннадійович

аспірант,

ВНЗ «Університет економіки та права КРОК», м. Київ

ORCID: <https://orcid.org/0009-0001-3409-5955>**Blynkov Bolodymyr**

KROK University, Kyiv

Проведено аналіз впливу ІТ-сектору різних держав на загальні показники економіки, досліджено вплив економічної безпеки ІТ-сектору на загальну стабільність національної економіки, розглянуто підходи до забезпечення економічної безпеки ІТ-сектору, який відіграє ключову роль у підтримці стабільності та конкурентоспроможності національних економік. Проаналізовано багаторівневі стратегії, спрямовані на зміцнення кібербезпеки, розвиток національної інфраструктури, захист даних та підтримку технологічного суверенітету. Підкреслено значення координації між державою і приватним сектором, а також міжнародного співробітництва у сфері кібербезпеки. Виявлено спільні риси підходів, серед яких інвестиції в інновації, підтримка стартапів, розвиток людського капіталу та впровадження регуляторних стандартів, що підвищують стійкість ІТ-сектору до внутрішніх та зовнішніх загроз.

Ключові слова: економічна безпека сектору ІТ; економічна стабільність; інновації; національна безпека.

The article analyzes impact of IT sector on general indicators of the economy of different countries, influence of the economic security of the IT sector on the overall stability of the national economy, provides an in-depth examination of the approaches taken by the United States, European Union, and India to ensure the economic security of the IT sector, a vital component of their national economies that bolsters stability and global competitiveness. The IT sector's rapid growth and its role as a backbone for critical infrastructures make its security an essential part of national security strategies. Multi-level strategies aimed at strengthening cybersecurity, developing national infrastructure, data protection, and supporting technological sovereignty are analyzed. In the United States, the emphasis is on comprehensive cybersecurity policies, extensive research funding, and strong collaboration between government agencies and private technology firms to mitigate risks and respond effectively to cyber threats. The European Union's approach includes stringent data protection regulations, such investment in digital programs to drive innovation and reduce dependency on foreign technology. Meanwhile, India's approach prioritizes digital sovereignty through initiatives like "Digital India" and "Start-up India," aimed at fostering indigenous technologies and strengthening national data centers. The article highlights the importance of government-private sector coordination in all three regions, as well as international cooperation in addressing global cyber threats. Additionally, there is a focus on fostering an environment conducive to innovation through investment in R&D, support for startups, and comprehensive education and training programs to develop a skilled workforce in IT and cybersecurity fields. Common characteristics of these approaches include robust financial support for research and development in emerging technologies such as artificial intelligence, blockchain, and quantum computing, along with regulatory frameworks that safeguard data privacy and enhance the resilience of IT infrastructure to internal and external risks. The study concludes that these strategic approaches enable the IT sector to contribute to national economic stability by mitigating vulnerabilities, sustaining technological advancement, and enhancing long-term economic resilience and global influence.

Keywords: economic security of the IT sector; economic stability; innovations; national security.

Постановка проблеми. Сучасна економіка держав все більше й більше залежить від ІТ-сектору, який стає не лише рушійною силою для зростання, але також і ключовим

елементом стабільності національної економіки. Окрім розвитку цифрової інфраструктури ІТ-сектор забезпечує функціонування стратегічних галузей: енергетики, фінансів,

медицини, освіти тощо. Економічна безпека (ЕБ) підприємств ІТ-сектору безпосередньо впливає на стабільність національної економіки. Стабільні та успішні ІТ-компанії створюють робочі місця, сприяють зростанню податкових надходжень і стимулюють економічний розвиток, з іншого боку економічна небезпека може призвести до скорочення робочих місць, втрати інвестицій та до уповільнення економічного зростання. Отже вкрай важливим є забезпечення ЕБ підприємств ІТ-сектору для гарантування загальної стабільності національної економіки. Саме тому, огляд та аналіз міжнародного досвіду впливу ЕБ підприємств ІТ-сектору на стабільність національної економіки та заходів щодо забезпечення ЕБ сектору в національному контексті є актуальним.

Аналіз останніх досліджень і публікацій. ЕБ ключовий елемент захисту національних інтересів держав, важливість економічної безпеки для підтримки стабільного розвитку економіки та забезпечення конкурентоспроможності на глобальному рівні. Розподіл загроз на внутрішні та зовнішні, які можуть негативно впливати на економічні цикли розвитку держав, є важливим фактором. Крім того, серйозною загрозою для економічної стабільності може бути тіньова економіка, для боротьби з якою може бути використана концепція «детінізації» як важлива складова підвищення ЕБ [17]. Успішні країни обирають стратегію розвитку, що базується на створенні та підтримці внутрішніх галузей промисловості, орієнтованих на національні ресурси та потенціал. Концепція "національного розвитку" як ключової основи для досягнення економічної стабільності та безпеки. Також поняття стійкості, гнучкості та здатності економічних систем до відновлення після деструктивних впливів. Стійкість розглядається як здатність економічної системи підтримувати розвиток продукції для задоволення потреб суспільства, заснованого на технологічному прогресі, національних ресурсах та міжнародній співпраці, навіть за умов невизначеності та дестабілізуючих факторів, так звана гібридна система «мир-війна» [18].

Переосмислення ЕБ в умовах глобальної турбулентності та прискорених змін технологічних укладів, що створює нові виклики для національних економік, важливість національної економічної незалежності, стійкості економічної системи, здатності до самостійного розвитку та керованості в умовах постійних змін [19] є важливою складовою забезпечення ЕБ національної економіки з урахуванням сучас-

них економічних, політичних і технологічних трансформацій.

Пошук вичерпного визначення ЕБ є складним завданням, відносні зміни в економічних можливостях впливають на пріоритети національної безпеки. Кожна країна має унікальне поєднання груп інтересів, комерційних стратегій і зовнішньої політики, які формують її погляд на потенціал і межі економічного управління державою [6].

Технологічний сектор США входить до п'ятірки найбільших економічних вкладників у 22 штатах і входить до першої десятки 42 штатів. У США частка технологічного сектора в реальному економічному зростанні постійно зростала з 2007 року. Швидкий розвиток і впровадження таких технологій, як роботизована автоматизація, хмарні обчислення, інтернет речей, штучний інтелект, машинне навчання та технології 5G, сприяють постійному зростанню ІТ-галузі. Сектор ІТ у США домінує на світовому ринку ІТ з найбільшою часткою ринку понад 40%. Економічний вплив індустрії технологій становить близько 1,879 мільярдів доларів США, тобто майже 10% [1].

Роль ІТ в економічному розвитку Індії швидко зросла експоненціальними темпами після економічної реформи 1991–1992 років. Індійські ІТ-компанії створили тисячі центрів в Індії та в багатьох країнах по всьому світу. Більшість світових корпорацій використовують ІТ послуги саме з індійського ІТ-сектору. Оскільки в 2019–2020 роках на нього припадає приблизно 55 відсотків світового ринку постачальників послуг (200–250 мільярдів доларів США). Обсяг ринку, зокрема експорту, ІТ-індустрії зріс у рази з приблизно 67 мільярдів доларів США у 2008–2009 роках до 191 мільярда доларів США у 2019–2020 роках. Очікується, що дохід зросте в наступні роки з прискоренням темпів зростання та досягне 350 мільярдів доларів США до 2025 року [2].

Польський ринок цифрової економіки оцінюється в 44 мільярди доларів і представляє значний потенціал для американських постачальників у всіх сегментах ринку. Згідно з аналізом міжнародної консалтингової компанії McKinsey & Company [3], до 2030 року цифрова економіка має зрости до 123 мільярдів доларів і становитиме 9% ВВП Польщі [4].

Українська технологічна галузь різко еволюціонувала за останні роки. З моменту появи перших ІТ-компаній у середині 1990-х років цей сектор пережив стрімке зростання. Сьогодні на нього припадає майже 5 відсотків ВВП, у ньому працює понад 200 000 людей [5].

Формулювання цілей статті. ІТ-сектор є значним важелем впливу на національну економіку багатьох держав і саме тому, є важливим, дослідження світового досвіду забезпечення ЕБ ІТ-сектору, адже ЕБ призводить до стійкого зростання сектору та стабільності що напряду впливає на національну економіку.

Виклад основного матеріалу дослідження. Світовий досвід забезпечення ЕБ ІТ-сектору свідчить про те, що країни, які прагнуть зберегти стабільність національної економіки, впроваджують різноманітні підходи та політики. Залежно від економічного розвитку, рівня технологічної залежності та масштабу ІТ-сектору, уряди країн використовують різні стратегії забезпечення безпеки.

США є одним із лідерів у сфері цифрової економіки та активно впроваджує політики, спрямовані на захист ІТ-сектору. Основні стратегії включають посилення кібербезпеки, підтримку інновацій, захист інтелектуальної власності та протидію технологічним загрозам. Уряд США підтримує програми з навчання фахівців, що працюють у сфері ІТ-безпеки, та інвестує у дослідження, спрямовані на розвиток передових технологій. З метою забезпечення протидії кібератакам було створено Департамент Внутрішньої Безпеки (DHS), який відповідає за безпеку кіберпростору та за збереження, підтримку ЕБ США [7]. Також Агентство з Кібербезпеки та Інфраструктурної Безпеки (CISA) відіграє важливу роль у захисті національної ІТ-інфраструктури, включаючи урядові мережі та критичні сектори економіки. Агентство координує заходи з кібербезпеки, проводить навчання, інформує про нові загрози та впроваджує рекомендації для бізнесу й урядових установ. Важливою складовою є спільні ініціативи уряду з приватним сектором. Уряд співпрацює з провідними технологічними компаніями та постачальниками кібербезпеки для обміну інформацією про загрози та вдосконалення захисту ІТ-сектору. Приватні компанії та федеральні відомства мають доступ до ресурсів і рекомендацій CISA для зміцнення безпеки цифрових систем. Уряд США через Національний Науковий Фонд (NSF), та інші агентства фінансує дослідження, спрямовані на розвиток нових технологій і фундаментальних наукових відкриттів [8]. Фінансування зосереджене на галузях, які мають стратегічне значення для національної безпеки та економіки, наприклад: штучний інтелект, квантові обчислення, біотехнології та альтернативна енергетика. Також США активно залучає приватний сек-

тор до досліджень через програми співфінансування, зокрема через ініціативи Національного Інституту Стандартів і Технологій (NIST) і Агентства з Передових Оборонних Дослідницьких Проектів (DARPA). США надає податкові пільги для компаній, що інвестують у науково-дослідні розробки, зокрема у вигляді податкового кредиту на дослідження та розробки. Це знижує витрати на інновації, стимулюючи компанії вкладати кошти в нові продукти та технології. Такі Програми, як-от Small Business Innovation Research (SBIR) і Small Business Technology Transfer (STTR), надають гранти малим інноваційним підприємствам для розвитку перспективних технологій і стартапів, сприяючи зростанню інноваційної екосистеми [9]. Важливою складовою також є освітні ініціативи та STEM-програми: у США здійснюється інвестування в розвиток кадрів у сферах STEM (наука, технології, інженерія, математика). Фінансуються програми для залучення студентів до цих галузей, а також професійного розвитку викладачів і дослідників. Широко розвинені імміграційні політики для висококваліфікованих спеціалістів: США залучає іноземних фахівців у галузі технологій і наукових досліджень через програми віз (наприклад, H-1B) [10], що забезпечує доступ до найкращих талантів з усього світу. Також держава створює регуляторні умови, які дозволяють інноваційним компаніям розвиватися без значного втручання. Приклади включають регулювання захисту даних, патентне право та підтримку вільного ринку. Програми підтримки стартапів і венчурного капіталу, в рамках регуляторних ініціатив США підтримує розвиток венчурного фінансування, що забезпечує стартапам доступ до капіталу для швидкого зростання та комерціалізації інновацій.

Стратегія Європейського Союзу (ЄС) в підтримці інновацій та забезпеченню ЕБ спрямована на створення єдиного інноваційного простору, що об'єднує ресурси, технології, фінансування та кадри для стимулювання економічного зростання і конкурентоспроможності. ЄС реалізує стратегію через масштабні фінансові програми, розбудову науково-дослідної інфраструктури, розвиток людського капіталу та підтримку регіональних інноваційних кластерів. Фінансування досліджень і розробок через програму Horizon Europe [11] яка є найбільшою дослідницькою програмою ЄС з бюджетом понад 95,5 мільярдів євро на 2021-2027 роки. Ця програма фінансує міждисциплінарні дослідження в таких пріоритет-

них напрямках, як зміни клімату, цифровізація, охорона здоров'я, енергетика та інші стратегічні галузі. Horizon Europe забезпечує гранти для досліджень на ранніх стадіях, що дозволяє вченим і підприємцям розвивати інноваційні ідеї. Також підтримуються партнерства з промисловістю для комерціалізації нових технологій. EIC Accelerator – частина Horizon Europe це ще одна ініціатива спрямована на підтримку стартапів та малих і середніх підприємств, які працюють над проривними інноваціями. EIC надає фінансову підтримку, експертні консультації та мережу контактів для розвитку та масштабування інноваційних проектів. EIC фокусується на високоризикових і високопотенційних технологіях, які можуть мати значний вплив на ринок і забезпечити ЄС конкурентні переваги в таких сферах, як штучний інтелект, квантові обчислення та біотехнології. З іншого боку Європейський Інститут інновацій та технологій (EIT) формує спільноти, що об'єднують дослідників, підприємців і освітні установи, створюючи регіональні інноваційні екосистеми [12]. Вони сприяють розповсюдженню інновацій та формують умови для розвитку нових стартапів у різних регіонах ЄС. Програма "Digital Europe" підтримує розвиток цифрової інфраструктури, таких як штучний інтелект, кібербезпека та передові обчислювальні технології. ЄС також фінансує програми підготовки кадрів у галузі наук, технологій, інженерії та математики (STEM). Програми Erasmus+ [14] і Marie Skłodowska-Curie [13] Actions надають гранти для молодих дослідників та обміну студентами для підвищення кваліфікації.

Модель ЕБ ІТ-сектору в Індії спрямована на забезпечення стабільності, кібербезпеки та технологічного суверенітету країни. Індія прагне не лише посилити захист свого ІТ-сектору, а й створити умови для його сталого розвитку та глобальної конкурентоспроможності. Ця модель поєднує регуляторні заходи, інвестиції в цифрову інфраструктуру, підвищення стійкості від кібератак та розвиток людського капіталу. Національна програма Digital India, яка спрямована на створення доступної цифрової інфраструктури, розвиток електронних послуг та інтеграцію ІТ-рішень у повсякденне життя громадян. Вона забезпечує ІТ-сектор основою для зростання та безпеки завдяки розвитку широкосмугового доступу до інтернету, цифрових платіжних систем і хмарних технологій. Індія активно підтримує створення та використання національних технологічних рішень для зниження

залежності від іноземних постачальників у критичних галузях, зокрема через розвиток власних програмних платформ та систем кібербезпеки. Національна стратегія кібербезпеки запроваджена урядом Індії, зосереджена на захисті критичної інфраструктури, розвитку навичок в сфері кібербезпеки, підвищенні обізнаності та захисті персональних даних. Вона передбачає створення центрів у ключових регіонах для моніторингу загроз та реагування на інциденти. Прийняття Закону про захист персональних даних спрямоване на підвищення відповідальності компаній за збереження персональних даних користувачів. Це зміцнює довіру до цифрових послуг і дозволяє забезпечити захист від витоку інформації, що критично важливо для ЕБ ІТ-сектору. Ініціатива Start-up India [15], уряд підтримує стартапи, надаючи гранти, податкові пільги та доступ до фінансування для нових компаній у сфері ІТ. Ця ініціатива стимулює інновації, допомагаючи новим підприємцям розвивати технологічні рішення, що зміцнюють національну економіку. Індія розвиває інфраструктуру для підтримки стартапів, включаючи створення інкубаторів та акселераторів, що забезпечують доступ до капіталу, менторства та інноваційних ресурсів для малих і середніх підприємств. Skill India Mission – ініціатива спрямована на підготовку кваліфікованих кадрів у сфері ІТ, кібербезпеки та новітніх технологій, таких як штучний інтелект, машинне навчання і блокчейн [16]. Програма забезпечує доступ до навчання для молоді та перепідготовки кадрів, що підтримує стійкість ІТ-сектору. Індія стимулює розвиток інженерних та ІТ-навичок через університетські програми та партнерства з іноземними освітніми закладами, що сприяє підготовці висококваліфікованих фахівців. Індія розширює широкосмуговий доступ і модернізує телекомунікаційні мережі, що сприяє безпечній цифровій економіці. Це знижує ризики для ІТ-сектору, пов'язані з обмеженим доступом до інтернету в регіонах. Створення національних центрів обробки даних дозволяє Індії зберігати дані в межах країни, що забезпечує кращий захист від кіберзагроз та дозволяє уникнути залежності від іноземних хмарних сервісів.

Підсумовуючи міжнародний досвід можна виокремити основні підходи щодо забезпечення ЕБ ІТ-сектору:

1. Кібербезпека та захист критичної інфраструктури: розробка стратегій кібербезпеки; створення спеціалізованих агентств,

що відповідають за розробку стандартів безпеки та моніторинг кіберзагроз; впровадження освітніх програм щодо протидії кібератакам; створення механізмів співпраці між урядом і приватними компаніями для обміну інформацією та швидкого реагування на кіберзагрози.

2. Підтримка технологічного суверенітету та зниження залежності від іноземних технологій: впровадження інвестицій у власні технології; стимулювання національного виробництва; розробка локальних технологій для зниження ризиків; фінансування досліджень і розробок новітніх технологій через різноманітні програми.

3. Захист даних та правове регулювання: забезпечення правового захисту персональних даних; регулювання діяльності ІТ-компаній щодо обробки даних; зниження ризиків витоку даних; впровадження регуляторних стандартів для цифрових платформ, для забезпечення захисту користувачів; зниження монополістичних практик та створення рівних умов для конкуренції.

4. Підтримка інновацій та стартапів: створення програм для підтримки стартапів та інновацій; створення венчурних програм фінансування; створення акселераторів, інкубаторів для стартапів.

5. Розвиток людського капіталу: створення програм підготовки кваліфікованих кадрів; інвестування в освіту та розвиток навичок у

галузі ІТ та кібербезпеки; підвищення рівня підготовки спеціалістів у галузях, важливих для ЕБ; підтримка програм з підготовки кадрів.

6. Міжнародне співробітництво та обмін інформацією: встановлення партнерських відносин з іншими країнами в ІТ галузі; співпраця на міжнародному рівні; обмін досвідом, інформацією та технологіями; участь у міжнародних форумах та ініціативах.

Висновки. ІТ-сектор є суттєвою частиною багатьох економік світу і має безпосередній вплив на загальну стабільність економік держав, саме тому питання забезпечення ЕБ ІТ-сектору стає ключовим в політиках світових держав. Аналіз світового досвіду забезпечення ЕБ ІТ-сектору в різних державах свідчить про багаторівневий підхід, що включає кібербезпеку, підтримку інновацій, розвиток цифрової інфраструктури, захист даних і технологічний суверенітет. Хоча кожна з країн реалізує власну стратегію з урахуванням своїх національних пріоритетів та умов, основні елементи цих підходів є схожими і вказують на універсальні рішення для зміцнення ЕБ ІТ-сектору. Таким чином, забезпечення ЕБ ІТ-сектору потребує поєднання стратегічного планування, інвестицій в інновації, розбудови національної інфраструктури та зміцнення людського капіталу. Це дозволяє державам адаптуватися до глобальних економічних змін і забезпечити стійкий розвиток у довгостроковій перспективі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Technology Sector's Impact on USA Economy (2024). URL: <https://www.deltetechnology.com/news-and-insights/technology-sectors-impact-on-usa-economy/#:~:text=The%20IT%20sector%20in%20the,%241%2C879%20billion%2C%20nearly%2010%25%20>
2. Information technology and its role in india's economic development (2022). URL: <https://community.nasscom.in/communities/it-services/information-technology-and-its-role-indias-economic-development#:~:text=IT%20industry%20boosting%20India's%20growth&text=Since%20it%20accounts%20for%20approximately,US%20dollars%20in%202019%2D20>
3. Polska jako Cyfrowy Challenger i lider handlu cyfrowego (2022). URL: <https://www.mckinsey.com/pl/our-insights/digital-challengers-3>
4. Poland Digital Economy (2024). URL: <https://www.trade.gov/country-commercial-guides/poland-digital-economy#:~:text=Digital%20Economy%20Overview&text=The%20Polish%20digital%20economy%20market,comprise%209%25%20of%20Poland's%20GDP>
5. У ВВП України майже 5% припадає на ІТ (2023). URL: <https://skilky-skilky.info/u-vvp-ukrainy-mayzhe-5-grupadaie-na-it/>
6. Gilpin, R. (1981). War and Change in World Politics. Cambridge University Press. DOI: <https://doi.org/10.1017/cbo9780511664267>
7. Homeland Security. U.S. Department of Homeland Security, Mission (2023). URL: <https://www.dhs.gov/mision>
8. The U.S. National Science Foundation (2024). URL: <https://new.nsf.gov/funding>
9. About America's Seed Fund powered by NSF (2024). URL: <https://seedfund.nsf.gov/our-program/>

16. Skill India Mission: All you need to know (2021). Available at: <https://www.bajajfinserv.in/insights/skill-india-scheme>
17. Kadala, V., Guzenko, O., Bondarenko, O. (2023). Economic security as a tool for the protection of national interests. *Baltic Journal of Economic Studies*. 9(4), 113-116. DOI: <https://doi.org/10.30525/2256-0742/2023-9-4-111-118>
18. Hrytsenko, A. (2024). Mekhanizmy zabezpechennia ekonomichnoi stiikosti ta bezpeky na zasadakh natsionalnoi ukorinenosti ekonomichnoho rozvytku. *Ekonomichna teoriia*. 3(1), 7–17. DOI: <https://doi.org/10.15407/etet2024.03.005>
19. Diachkov, O. (2022). Ekonomichna bezpeka natsionalnoi ekonomiky: sutnist, osoblyvosti, struktura. *Ekonomichni horyzonty*. 1(19), 85–91. DOI: [https://doi.org/10.31499/2616-5236.1\(19\).2022.267022](https://doi.org/10.31499/2616-5236.1(19).2022.267022)