КІБЕРБЕЗПЕКА В ЦИФРОВІЙ ЕКОНОМІЦІ
CYBER SECURITY IN THE DIGITAL ECONOMY

У даній статті описано важливість підвищення рівня безпеки в інтернеті, що є передумовою для більш активного використання інформаційно-комунікаційних технологій та прискорення розвитку цифрової економіки. Особливо це стосується розвинених країн, де вже відбувається широкомасштабне використання цифрових технологій у всіх сферах життя. Однак, не дивлячись на те, що кібербезпека стає все більш актуальною проблемою, існують деякі аспекти, які необхідно врахувати для повноцінного розвитку цифрової економіки. Підвищення рівня кібербезпеки – лише один з аспектів, який необхідно враховувати для успішного розвитку цифрової економіки. Для цього також потрібно забезпечити доступність технологій, забезпечити безпеку даних та сприяти розвитку цифрової грамотності. У рамках дослідження виявлено, що криптографія та штучний інтелект стають ключовими інструментами у протидії несанкціонованим мережевим атакам у сучасному цифровому середовищі. Дослідження також підтвердило, що компанії, які вкладають достатньо уваги і фінансових ресурсів у захист власних даних і інформації своїх клієнтів, мають меншу ймовірність зазнати фінансових втрат, тому вони є привабливішими та конкурентоспроможнішими на ринку для своїх клієнтів. Для досягнення цих цілей необхідна співпраця між урядовими органами, приватним сектором та громадськістю. Важливо створювати сприятливу екосистему для обміну інформацією про кіберзагрози та впроваджувати сучасні методи захисту в інформаційній сфері. Такий підхід дозволить забезпечити стабільність та безпеку у цифровому просторі, що є важливим для розвитку сучасного суспільства.
Ключові слова: *цифровізація, цифрова економіка, кібербезпека, штучний інтелект, дані, інтернет.*

This article describes the importance of increasing the level of security on the Internet, which is a prerequisite for more active use of information and communication technologies and accelerating the development of the digital economy. This is especially true of developed countries, where digital technologies are already widely used in all spheres of life. However, despite the fact that cyber security is becoming an increasingly urgent problem, there are some aspects that must be taken into account for the full development of the digital economy. Increasing the level of cyber security is only one of the aspects that must be taken into account for the successful development of the digital economy. This also requires ensuring the availability of technology, ensuring data security and promoting digital literacy. The study found that cryptography and artificial intelligence are becoming key tools in countering unauthorized network attacks in today's digital environment. The study also confirmed that companies that invest enough attention and financial resources in protecting their own data and their customers' information are less likely to suffer financial losses, so they are more attractive and competitive in the market for their customers. Achieving these goals requires cooperation between government agencies, the private sector, and the public. It is important to create a favorable ecosystem for the exchange of information about cyber threats and to implement modern protection methods in the information sphere. This approach will ensure stability and security in the digital space, which is important for the development of modern society. Continuous innovation in the field of cyber security is essential to stay ahead of evolving threats. Investing in research and development of new technologies and methodologies for detecting and mitigating cyber threats is crucial. This includes leveraging emerging technologies such as artificial intelligence and machine learning to enhance cyber security capabilities and improve incident response times. While increasing the level of cyber security is a crucial step towards enabling the full potential of the digital economy, it is only one piece of the puzzle. Ensuring the availability of technology, enhancing data security, promoting digital literacy, fostering collaboration, and driving innovation are all essential components of a comprehensive strategy to navigate the challenges of the digital age. By addressing these key considerations, we can create a safer and more resilient digital environment that fosters innovation, growth, and prosperity for all.
Key words: *digitization, digital economy, cyber security, artificial intelligence, data, Internet.*

УДК 338.2
DOI: https://doi.org/10.32782/infrastruct78-12

Завербний А.С.
д.е.н., доцент,
професор кафедри зовнішньоекономічної та митної діяльності,
Національний університет «Львівська політехніка»
Ільницький В.С.
аспірант кафедри зовнішньоекономічної та митної діяльності,
Національний університет «Львівська політехніка»

Zaverbnyi Andrii
Lviv Polytechnic National University
Ilnytskyi Vitalii
Lviv Polytechnic National University

Постановка проблеми. В плані тематики розвитку цифрової економіки слід звернути увагу на забезпечення належного рівня кібербезпеки. У зв'язку зі швидким розвитком цифрових технологій, захист інформації та комунікацій стає все важливішим для забезпечення безпеки як держави, так і приватних осіб, бізнесу. Оскільки все більше аспектів життя переходять до цифрового формату, захист даних стає ключовою проблемою, що потребує комплексного підходу та постійного удосконалення. Одним із основних аспектів кібербезпеки є захист від кібератак, які стають все більш складними та винахідливими. Хакери та зловмисники постійно шукають нові способи для отримання доступу до конфіденційної інформації, такої як особисті дані, банківські реквізити та комерційна інформація. Це ставить під загрозу як безпеку окремих осіб, так і стабільність фінансових та інших секторів економіки. Тому важливо розробляти та впроваджувати ефективні заходи кібербезпеки, які б забезпечували відповідний рівень захисту. Загалом, підвищення рівня кібербезпеки вимагає комплексного підходу та співпраці між урядовими структурами, приватним сектором та громадськістю. Тільки за умови взаємодії всіх сторін можна забезпечити стабільність та безпеку в цифровому просторі, що є важливим для розвитку економіки.

Аналіз останніх досліджень та публікацій. Проаналізувавши наукові праці, можна відзначити про велику зацікавленість дослідників тематикою кібербезпеки, як вагомого фактора, розвитку

цифрової економіки. Комова С. у своїй науковій праці виділяє можливі проблеми кібермереж, що є потенційним ризиком національних економік [1]. Іваненко В. у своїй праці акцентує увагу на тісному зв'язку сучасної економічної сфери з цифровими змінами [2]. Кіндзерський Ю. аналізує методи пізнання процесів цифрової трансформації економіки та розкриває значення кібербезпеки у її формуванні [3]. Ревак І. у своїй праці розкриває особливості, за яких повинен формуватись безпечний кіберпростір в умовах цифрової економіки [4].

Формулювання цілей статті. Основною метою даного дослідження можна назвати виявлення того який вплив кібербезпека має на розвиток цифрової економіки та що потрібно реалізувати задля його збільшення.

Виклад основного матеріалу дослідження. Розвиток цифрового середовища суттєво впливає на всі сфери сучасного життя, зокрема на виробництво. Діджиталізація виробничих процесів стає не просто тенденцією, але і необхідністю для успішного функціонування бізнесу у існуючих умовах. Цей процес передбачає використання сучасних цифрових технологій та інструментів для оптимізації виробничих процесів, зменшення витрат та підвищення продуктивності. Успішність сучасного бізнесу в значній мірі залежить від здатності компаній до інновацій та впровадження новаторських рішень у свою діяльність. Інновації стали важливим стимулом розвитку багатьох галузей економіки, адже вони дозволяють вдосконалити існуючі продукти та послуги, випустити на ринок нові товари та забезпечити конкурентні переваги. Проте інновації самі по собі не є гарантом успіху. Для їх успішної реалізації потрібна гнучкість та здатність до імпровізації. Гнучкість управління дозволяє швидко реагувати на зміни у внутрішньому та зовнішньому середовищі компанії, а імпровізація дозволяє знаходити нестандартні рішення для вирішення проблем та досягнення поставлених цілей. Національний кіберпростір в сучасному світі відіграє важливу роль у формуванні цифрової економіки. Це інфраструктура, яка забезпечує доступ до інформації та електронних послуг для громадян і бізнесу. Важливою складовою кіберпростору є захист від кіберзагроз, оскільки в сучасних умовах компанії та організації часто стають об'єктами кібератак. Кібератаки – це спрямовані дії в кіберпросторі, які мають на меті порушення роботу інформаційно-телекомунікаційних систем задля втручання у конфіденційність, цілісність, доступність, авторство інформації [1]. Цифрові фахівці шукають способи захисту від компрометації мережевих систем. Для організацій доступні найпоширеніші інструменти захисту від кіберзагроз, особливо у поєднанні з оновленням програмного забезпечення. До таких інструментів відносять [2]:

– фаєрволи – це програмне забезпечення, яке контролює вхідні та вихідні мережеві з'єднання, фільтруючи їх за певними правилами безпеки;

– антивіруси – це програми, які виявляють та намагаються вилучити віруси та інші шкідливі програми з комп'ютерів та мереж;

– системи виявлення вторгнень – це програмне забезпечення, яке моніторить мережу на предмет незвичайних або підозрілих активностей, що можуть свідчити про вторгнення;

– криптографія або системи шифрування – це методи захисту інформації шляхом перетворення її в нечитабельний формат, який може бути прочитаний тільки за допомогою спеціального ключа;

– безпечні паролі – використання унікальних та складних паролів є важливим аспектом безпеки, оскільки вони ускладнюють завдання злочинцям щодо незаконного доступу до даних.

Ці інструменти становлять основу для створення надійного захисту від кіберзагроз та забезпечують безпеку комп'ютерних систем та мереж у сучасному цифровому світі. Однак важливо пам'ятати, що безпека мережі – це постійний процес, і для успішного захисту важливо постійно вдосконалювати та оновлювати захисні механізми. Варто відзначити, що законодавча основа є фундаментальною для забезпечення кібербезпеки. Правова ситуація оцінюється через кількість інститутів і організацій, що відповідають за кібербезпеку. Її забезпечення неможливе без відповідних технічних знань для виявлення та реагування на кібератаки. Для ефективного функціонування системи кібербезпеки важливими елементами є: національна стратегія; модель управління, що відповідає складності завдань; наглядові органи, укомплектовані кваліфікованими фахівцями. Можливості підвищення потенціалу кібербезпеки оцінюються за кількістю досліджень та розробок у цій галузі, наявністю освітніх та навчальних програм, а також сертифікованих фахівців та державних установ. Для ефективної боротьби з кіберзлочинністю важливою умовою є розширення співпраці на національному та міжнародному рівні, що оцінюється за кількістю інформаційних партнерств [3].

Кіберзлочинність, як і кібервійна, являють собою нові форми деструктивних явищ. Кіберзлочинність охоплює злочини, здійснені у віртуальному просторі, через інтернет або проти нього. До цього типу загроз належать незаконне отримання, розголошення або витік інформації, несанкціоновані зміни даних, неналежне використання техніки, створення, використання та розповсюдження шкідливих програм, несанкціонований доступ до даних, поширення спаму тощо.

Для надійного захисту кіберпростору застосовуються новітні технології. Двофакторна автентифікація зараз широко використовується у хмарній

електронній пошті і стає все більш популярною у роздрібному та інтернет-банкінгу; кіберрозвідка та аналіз є технічними засобами, що викликають підвищений інтерес до обміну інформацією та аналізу загроз. Запобігання таким загрозам, як фішингові атаки, крадіжка особистих даних і недопущення кіберінцидентів на національному рівні, на наш погляд, є пріоритетними напрямами зміцнення кібербезпеки [4].

Висновки з проведеного дослідження. У сучасній цифровій економіці кібербезпека стає ключовим елементом для забезпечення стабільності, захисту даних та безперервності бізнес-процесів. Розвиток інформаційних технологій відкриває нові можливості для економічного зростання, проте водночас породжує і нові загрози. Кіберзлочинність, як складова частина кіберпростору, вимагає постійного моніторингу та вдосконалення захисних механізмів. Ефективне забезпечення кібербезпеки передбачає комплексний підхід, що включає правові, технічні та організаційні заходи. Законодавча база повинна бути адаптована до сучасних викликів, забезпечуючи чіткі рамки для виявлення, розслідування та покарання кіберзлочинів. Технічні аспекти включають впровадження передових технологій, таких як двофакторна автентифікація, шифрування даних, використання систем штучного інтелекту для аналізу загроз та кіберрозвідки.

Організаційний аспект кібербезпеки включає підготовку кваліфікованих фахівців, створення національних стратегій та розбудову інфраструктури, яка дозволяє ефективно протидіяти кіберзагрозам. Співпраця між державним і приватним секторами є критично важливою для створення надійної системи кібербезпеки. Обмін інформацією та досвідом, спільні дослідження та розробки сприяють підвищенню рівня захисту в цифровому середовищі.

Особливу увагу слід приділяти питанням освіти та підвищення обізнаності користувачів про потенційні загрози та методи їх уникнення. Навчальні програми, семінари та тренінги повинні стати невід'ємною частиною стратегії кібербезпеки на всіх рівнях – від індивідуальних користувачів до великих корпорацій. Важливо розуміти, що кібербезпека не є статичним станом, а динамічним процесом, який потребує постійного вдосконалення та адаптації до нових викликів. Лише системний підхід та координація зусиль національних та міжнародних організацій дозволять ефективно захистити цифрову економіку від зростаючих загроз кіберпростору. У цьому контексті роль наукових досліджень є надзвичайно важливою, оскільки вони сприяють розробці нових методів та інструментів для забезпечення кібербезпеки, що відповідають сучасним викликам та тенденціям цифрового світу.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Комова С. Кібербезпека в цифровій економіці, *Матеріали XVI всеукраїнської студентської науково-технічної конференції «Сталий розвиток міст»*, 2023. URL: https://science.kname.edu.ua/images/dok/konferentsii/stalyirozvytok2019/2023/Ch3-Economica_23.pdf#page=67 (дата звернення: 03.04.2024).

2. Іваненко В. Кібербезпека в економіці: захист від кіберзагроз у диджиталізованому світі, *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2023. URL: https://nzlubp.org.ua/index.php/journal/article/view/941/839 (дата звернення: 03.04.2024).

3. Кіндзерський Ю. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічна теорія*, 2020. URL: https://ev.nmu.org.ua/docs/2020/3/EV20203_018-026.pdf (дата звернення: 03.04.2024).

4. Ревак І. Особливості формування безпечного кіберпростору в умовах розвитку цифрової економіки, *Інноваційна економіка*, 2021. URL: http://inneco.org/index.php/innecoua/article/view/784 (дата звернення: 03.04.2024).

REFERENCES:

1. Komova S. (2024) Kiberbezpeka v tsyfrovii ekonomitsi [Cyber security in the digital economy]. *Materialy XVI vseukrainskoi studentskoi naukovo-tekhnichnoi konferentsii «Stalyi rozvytok mist».* Available at: https://science.kname.edu.ua/images/dok/konferentsii/stalyirozvytok2019/2023/Ch3-Economica_23.pdf#page=67 (accessed April 3, 2024).

2. Ivanenko V. (2023) Kiberbezpeka v ekonomitsi: zakhyst vid kiberzahroz u dydzhytalizovanomu sviti [Cyber Security in the Economy: Protecting Against Cyber Threats in a Digitized World]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna. Seriia yurydychna.* Available at: https://nzlubp.org.ua/index.php/journal/article/view/941/839 (accessed April 3, 2024).

3. Kindzerskyi Yu. (2020) Kiberbezpeka ta stanovlennia tsyfrovoi ekonomiky: problemy vzaiemozviazku [Cyber Security and the Emergence of the Digital Economy: Interrelationship Issues]. *Economic theory.* Available at: https://ev.nmu.org.ua/docs/2020/3/EV20203_018-026.pdf (accessed April 3, 2024).

4. Revak I. (2021) Osoblyvosti formuvannia bezpechnoho kiberprostoru v umovakh rozvytku tsyfrovoi ekonomiky [Peculiarities of the formation of a safe cyberspace in the conditions of the development of the digital economy]. *Innovatsiina ekonomika.* Available at: http://inneco.org/index.php/innecoua/article/view/784 (accessed April 3, 2024).