Дмитро В. Мирончeнко*

МЕХАНІЗМИ ПОПЕРЕДЖЕННЯ КІБЕРЗАГРОЗ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ

У статті узагальнено наукові підходи до попередження кіберінцидентів, обґрунтовано профілактичні механізми, критичні для зниження економічних втрат. На основі огляду джерел і вивчення кейсів визначено пріоритетні напрями: дисципліна доступів (MFA/принцип найменших привілеїв), керування оновленнями й вразливостями, резервне копіювання з перевіркою відновлення, запобігання витоку даних (DLP) та безперервне навчання персоналу. Показано, що поєднання зазначених заходів із державно-приватною координацією та обміном інформацією про загрози через CERT/CSIRT скорочує простої й масштаб компрометації даних. Зроблено висновок про доцільність комплексного підходу до кібергігієни як практичного інструменту підтримання кіберстійкості критичної інфраструктури України. Застосовано методи структурно-динамічного аналізу, порівняльного аналізу, контент-аналіз та елементи сценарного моделювання.

Ключові слова: *кібербезпека, кібергігієна, кіберзагрози, ризики, економічна безпека країни, конкурентоспроможність.*

Літ. 16.

DOI: 10.32752/1993-6788-2025-1-294-218-226

Dmytro Myronchenko

CYBER THREAT PREVENTION MECHANISMS TO ENSURING THE COUNTRY'S ECONOMIC SECURITY

The article examines the prevention of cyber incidents as a practical component of economic security in conditions of high digitalization and interdependence of economies. The methodological basis is a structured review of scientific works on the economics of cybersecurity and an analysis of analytical materials on digital risk management, supplemented by an analytical summary of well-known examples of cyber incidents that demonstrate the economic consequences of failures and data compromise. The paper shows that cyber threats are transformed into economic losses through operational downtime and service interruptions, data leaks and related legal/regulatory costs, third-party and supply chain risks, as well as reputational losses that reduce trust in digital services.

As a key result, priority preventive areas relevant to the public and corporate sectors were identified: access discipline (application of MFA and the principle of least privilege), vulnerability and update management, backup with regular recovery testing, and control of sensitive data leaks through DLP in cloud and remote scenarios. The role of continuous staff training as a tool for reducing social engineering risks and increasing readiness for timely reporting of suspicious events was separately emphasized. At the level of sector interaction, the importance of public-private coordination and exchange of information about threats through CERT/CSIRT was outlined to increase readiness and reduce response time. It was concluded that the transition from fragmented measures to a combination of technical controls, cyber hygiene, and intersectoral interaction reduces the likelihood of incidents and limits their economic consequences; for Ukraine, this is a priority in the context of protecting critical infrastructure and maintaining economic stability. Methods of structural-dynamic analysis, comparative analysis, content analysis, and elements of scenario modeling were applied.

Keywords: *cybersecurity, cyber hygiene, cyber threats, risks, national economic security, competitiveness.*

Peer-reviewed, approved and placed: *05.12.2025*

* State University “Kyiv Aviation Institute”. Ukraine.

Постановка проблеми. Проблематика захисту цифрових кордонів набуває для України особливого значення з огляду на її геополітичне положення та посилення ролі у світовій цифровій економіці. Країну дедалі частіше розглядають як осередок IT-талантів і цифрових інновацій, а технологічний сектор демонструє динамічний розвиток та інтеграцію в глобальні ринки. Водночас Україна, як і багато інших держав, стикається з масштабними викликами у сфері кібербезпеки: кібератаками з боку державних і недержавних суб'єктів, а також вразливостями критичної інфраструктури й державних інформаційних систем. За таких умов розгляд цієї проблематики крізь призму «кібергігієни» є методологічно обґрунтованим, оскільки йдеться про сукупність регулярних практик та організаційно-технічних заходів, яких дотримуються особи й організації для підтримання безпеки цифрових систем, зниження ймовірності інцидентів і мінімізації їхніх наслідків.

Аналіз останніх досліджень та публікацій. Проблематика зниження кіберзагроз та цифрової безпеки країн активно досліджується у працях як зарубіжних, так і українських науковців. Значний внесок у вивчення впливу кіберзагроз на економічну безпеку країн зробили Р. Андерсон і Т. Мур [1], а також Е. Копп, Л. Каффенбергер і К. Вілсон [2]. На рівні міжнародної політики підхід до управління цифровими ризиками як складової економічного розвитку обґрунтовано ОЕСР [3]. В українській науковій думці кібербезпеку як складову економічної безпеки держави розглядає С. Горбаченко [6], а вплив кіберзагроз на економічну стійкість через призму технологічної інфраструктури аналізують О. Пахненко та М. Божко у праці [7]. Науковці акцентують увагу на тому, що кіберзагрози здатні спричиняти економічні втрати, підривати стійкість функціонування критичної інфраструктури та знижувати довіру до цифрових сервісів, що безпосередньо впливає на економічну безпеку та конкурентоспроможність держави [1-3; 6-7].

Особливості забезпечення кібергігієни інформаційного простору досліджуються як у зарубіжних, так і в українських джерелах. Практики кібергігієни та потребу у стандартизованому «базовому рівні» таких практик систематизовано у звіті ENISA «Cyber Hygiene» [4]. Узагальнення ключових тенденцій і чинників ускладнення кіберландшафту (геополітичні напруження, залежність від ланцюгів постачання, розвиток технологій) подано у звіті Всесвітнього економічного форуму «Global Cybersecurity Outlook 2025» [5]. В українському контексті Я. І. Шестак у роботі «Кібергігієна у інформаційному просторі в умовах воєнного стану» підкреслює роль регулярних профілактичних практик (навчання, дисципліна роботи з доступами, базові налаштування захисту, обережність до соціальної інженерії) у зниженні ймовірності інцидентів та мінімізації їх наслідків [8].

Водночас, беручи до уваги ґрунтовні наукові доробки вчених-економістів, дослідження особливостей кібергігієни і забезпечення цифрової безпеки в національному науковому просторі практично відсутні, що вказує на своєчасність та актуальність вивчення питання розроблення механізмів попередження кіберзагроз та зниження їх впливу на економічні системи.

Мета дослідження полягає в пошуку та обґрунтуванні механізмів попередження кіберзагроз для забезпечення економічної безпеки країни.

Основні результати дослідження. Надійна кібербезпекова рамка забезпечує стабільність і безперервність функціонування цифрової інфраструктури, що прямо впливає на економічне зростання та здатність залучати іноземні інвестиції, а також формує довіру до цифрових сервісів і транскордонних бізнес-процесів. З урахуванням того, що кіберзагрози мають міжкраїновий характер, посилення кібергігієни в Україні не обмежується внутрішнім виміром і потребує системної взаємодії з міжнародними партнерами, обміну інформацією, узгодження підходів і участі у формуванні спільних норм та стандартів. Для держави, що перебуває в умовах підвищених ризиків, це також має безпосередній зв'язок із національною безпекою, оскільки захист урядових мереж, конфіденційної інформації та критично важливої інфраструктури є ключовим фактором стійкості. Паралельно розвиток технологічної індустрії значною мірою залежить від безпечних цифрових платформ і мереж, адже поширення практик кібергігієни підтримує культуру безпеки, зменшує операційні ризики та створює передумови для стабільного зростання інноваційного сектору.

Кібербезпека як практика захисту мереж, пристроїв і даних від несанкціонованого доступу та зловмисного використання набуває визначального значення в цифрову епоху, виконуючи роль бар'єра проти витоків даних, крадіжок ідентичності та інших форм кіберзлочинності, що загрожують як окремим особам, так і організаціям. Її фундаментальною метою є забезпечення конфіденційності, цілісності та доступності інформації – властивостей, без яких неможливі стійкі цифрові сервіси, довіра до економічних взаємодій і надійність державних та корпоративних процесів у глобальному цифровому середовищі.

У сучасному взаємопов'язаному світі цифрові технології пронизують практично всі сфери особистого й професійного життя – від спілкування та освіти до фінансів, державних послуг і комерції – тому кібербезпека набуває особливої актуальності. Попри те, що цифровий прогрес відкриває нові можливості, він одночасно розширює поверхню атак: кіберзлочинці та інші зловмисні суб'єкти використовують уразливості, здійснюють атаки й здатні завдавати шкоди системам, від яких залежить функціонування організацій і суспільства. В таких умовах кібербезпека виконує роль механізму зниження ризиків і збереження цілісності інформаційної інфраструктури, а ефективний захист дедалі частіше потребує не разових рішень, а комплексної та проактивної стратегії, що охоплює інформування й обізнаність, запобігання, виявлення, реагування та відновлення. Даний підхід передбачає дотримання найкращих практик, стандартів і нормативних рамок, а також системні інвестиції в технології, компетенції та дослідження.

Зростання важливості кібербезпеки зумовлене кількома взаємопов'язаними тенденціями. Масове поширення онлайн-платформ і сервісів зробило цифрову ідентичність та персональні/фінансові дані постійною ціллю для шахрайства, вимагання й інших форм зловживань. Критичні ланцюги постачання та операційні процеси в різних секторах значною мірою залежать від ІТ, тому кібератаки можуть спричиняти збої, простої та значні фінансові втрати. Додатково зростає кількість підключених

до Інтернету пристроїв і програм (IoT, "розумні" системи, корпоративні хмарні сервіси), що підвищує зручність та ефективність, але водночас створює нові точки проникнення й вектори атак, через які під загрозою опиняються як самі пристрої, так і дані, що ними обробляються.

Кіберзагрози є поширеною проблемою, яка постійно еволюціонує та не обмежується державними кордонами, впливаючи на окремих осіб, корпорації та уряди. Наслідки мають багатовимірний характер: компрометація даних може означати викрадення, підміну або витік персональної, фінансової чи конфіденційної інформації з подальшими ризиками крадіжки особистих даних, шахрайства, шантажу або вимагання; операційні збої виникають тоді, коли атаки порушують роботу систем і мереж, спричиняючи затримки, втрати або навіть фізичні наслідки в кіберфізичних середовищах; репутаційна шкода проявляється через втрату довіри клієнтів і партнерів, юридичні ризики та довготривалі фінансові наслідки. Практика останніх років демонструє, що атаки можуть зачіпати як критичну інфраструктуру та великі компанії, так і цілі галузі: інцидент із Colonial Pipeline [9] показав, як атака типу ransomware може призводити до зупинки операцій і масштабних непрямих наслідків. Компрометація ланцюга постачання у випадку SolarWinds [10] підкреслила системний характер ризику для державних та приватних організацій, а витік даних Equifax [11] став прикладом того, як порушення безпеки здатне мати довготривалий вплив на мільйони людей і репутацію компанії. У ширшому вимірі кіберзагрози впливають на економічну стабільність і конкурентоспроможність, стримуючи інновації та продуктивність і формуючи значні сукупні витрати для глобальної економіки. Під загрозою опиняються також національна безпека й суверенітет, коли атаки спрямовуються на оборонні, дипломатичні та демократичні процеси або на критичну інфраструктуру, що підтверджується, зокрема, атаками на енергетичні системи України [12]. На цьому тлі кібербезпека як системна діяльність із запобігання, виявлення, реагування та відновлення потребує узгоджених зусиль різних стейкхолдерів і постійного посилення практик, стандартів та інституційних механізмів захисту.

Кібербезпека є комплексною сферою, яка спрямована на захист цифрових активів (даних, мереж, пристроїв і сервісів) та зниження ризиків від широкого спектра загроз. Найпоширеніші сценарії атак включають соціальну інженерію (зокрема фішинг), коли зловмисники через оманливі повідомлення намагаються отримати доступ до облікових даних або примусити користувача встановити шкідливе програмне забезпечення (ПЗ); програмне забезпечення-вимагач, яке блокує роботу систем або шифрує дані з вимогою викупу; шпигунське ПЗ, що приховано збирає конфіденційну інформацію; а також інші типи malware (трояни, черв'яки тощо), які можуть призводити до втрати даних і компрометації інфраструктури. Окрему групу становлять атаки на вебзастосунки та мережеві взаємодії: "людина посередині" (перехоплення й підміна трафіку), SQL-ін'єкції та XSS (використання вразливостей у вебсистемах), DDoS (перевантаження сервісів трафіком), а також експлойти нульового дня, що експлуатують ще невідомі або неусунені вразливості. Сукупно такі загрози спричиняють не лише витоки

й маніпуляції даними, а й операційні збої, фінансові втрати та репутаційні наслідки, а їхній вплив посилюється через розвиток віддаленої роботи, масштабування хмарних сервісів і поширення IoT-пристроїв.

В такому контексті кібергігієна розглядається як регулярна дисципліна дій, що підвищує рівень онлайн-безпеки та зменшує ймовірність успішних атак, захищаючи дані, пристрої й мережі. Її практичний зміст зводиться до базових, але системних кроків: своєчасних оновлень операційних систем і програм, використання захисних засобів і сканувань, застосування унікальних складних паролів і багатофакторної автентифікації, обережної взаємодії з листами/посиланнями/вкладеннями, регулярного резервного копіювання, шифрування конфіденційної інформації та безпечного доступу до мереж (зокрема у публічних Wi-Fi). Постійне навчання й підвищення обізнаності доповнює технічні заходи та формує стійкість як на рівні окремих користувачів, так і на рівні організацій.

Економіка кібербезпеки є багатогранним викликом, що виходить далеко за межі прямих фінансових втрат окремих компаній і охоплює збої в глобальній торгівлі, роботу критичної інфраструктури та рівень суспільної довіри до цифрових сервісів. У дослідженнях на кшталт аналізу CSIS у співпраці з McAfee підкреслюється масштаб економічних втрат від кіберзлочинності, які оцінюються сотнями мільярдів доларів щороку (часто наводиться орієнтир близько 600 млрд дол. на рік [13]), що корелює з помітною часткою світового ВВП і відображається на прибутковості бізнесу та макроекономічній стабільності. Зростання такого тиску посилюється «демократизацією» шкідливих інструментів і тактик: завдяки підпільним ринкам і сервісним моделям на кшталт “malware-as-a-service” зловмисникам дедалі частіше не потрібні глибокі технічні компетенції для запуску руйнівних атак, а доступність ransomware і супутньої інфраструктури фактично перетворює кіберзлочинність на сталу економічну індустрію. Паралельно експоненційне зростання обсягів даних і накопичення конфіденційної інформації організаціями підвищує «вартість цілі» – наслідки інцидентів проявляються не лише у негайних збитках, а й у компрометації інтелектуальної власності, регуляторних санкціях, перериванні бізнес-процесів та ерозії довіри споживачів, що зменшує готовність до онлайн-транзакцій і впливає на економічну поведінку. Додатковий вимір формує фінансоване державами економічне шпигунство, коли незаконне отримання технологій, комерційних таємниць і фінансової розвідки підриває конкурентні переваги цілих галузей і створює геополітичні напруження з відчутними економічними наслідками.

Оцінювання реального економічного ефекту ускладнюється заниженим повідомленням про інциденти: компанії можуть уникати публічності через ризики репутаційних втрат або регуляторної уваги, що зменшує прозорість ринку та ускладнює розробку ефективних стратегій пом’якшення. Тому витрати на кібербезпеку в багатьох секторах зростають, а організації дедалі частіше переглядають IT-бюджети на користь посилення захисту; окремим трендом стає активне впровадження рішень на основі штучного інтелекту (ШІ), ринок яких, за прогнозами галузевих аналітиків, демонструє значну

динаміку до кінця десятиліття. Український контекст потребує окремого фокусу через тривалі й інтенсивні кіберзагрози, зокрема з боку ворожих суб'єктів. Це стимулює інвестиції у кіберстійкість та розвиток інституційної спроможності, зокрема через міжнародні програми підтримки: у червні 2023 року США оголосили додаткові 37 млн дол. США на кібербезпеку України, що доводить сукупний обсяг кібердопомоги США з 2016 року до 120 млн дол. США [14].

Запобігання втраті даних (DLP) є одним із базових механізмів захисту інформації, спрямованим на виявлення та зниження ризиків несанкціонованого обміну, передавання або використання конфіденційних даних. До таких даних можуть належати відомості про клієнтів, фінансова інформація, інтелектуальна власність, внутрішня документація та записи співробітників, тобто будь-які категорії інформації, витік або неправомірне використання яких створює для організації фінансові, юридичні та репутаційні наслідки. Практична цінність DLP полягає у підвищенні видимості та контролю над даними в різних середовищах – у локальних системах, хмарних сховищах та на кінцевих пристроях, а також у можливості застосовувати політики доступу й обмеження в умовах віддаленої роботи та BYOD (Bring Your Own Device — використання працівниками власних персональних пристроїв для доступу до корпоративних ресурсів), коли дані виходять за межі традиційного периметра. Захищаючи чутливі активи та зменшуючи ризик витоків, DLP підтримує збереження конкурентних переваг, зміцнює довіру клієнтів і партнерів та сприяє виконанню вимог регуляторики у сфері конфіденційності даних зокрема GDPR (General Data Protection Regulation — Загальний регламент ЄС про захист даних) та CCPA (California Consumer Privacy Act — Закон штату Каліфорнія про конфіденційність персональних даних споживачів), знижуючи ймовірність штрафів і судових ризиків. Ефективність DLP забезпечується поєднанням технічних засобів (у тому числі механізмів виявлення підозрілих дій, аналітики, інколи ШІ/ML) та чітко визначених політик, які регламентують класифікацію, маркування, правила обміну й методи захисту інформації.

Паралельно з технічними контролями, фундаментальним елементом цілісної безпекової стратегії є кібергігієна, зокрема навчання та програми підвищення обізнаності співробітників. Вони формують у персоналу розуміння типових загроз, уразливостей і ризиків, навчають розпізнавати фішинг і соціальну інженерію, безпечно працювати з обліковими даними та пристроями, застосовувати надійні унікальні паролі, використовувати багатофакторну автентифікацію, а також діяти відповідально у випадку підозрілих подій. Важливою складовою таких програм є культура повідомлення про інциденти та дотримання процедур реагування, що підвищує швидкість локалізації загроз і зменшує ймовірність ескалації до витоку або компрометації систем. Оскільки ландшафт загроз змінюється, навчання має бути безперервним і адаптивним, із використанням різних форматів (курси, вебінари, короткі нагадування, внутрішні комунікації, тести), щоб забезпечити практичне засвоєння навичок і підтримувати стійкість організації до нових ризиків. Інвестиції в обізнаність персоналу,

поєднані з технічними механізмами контролю на кшталт DLP, зменшують ймовірність витоків і кібератак, знижують потенційні фінансові втрати та репутаційну шкоду й посилюють довіру стейкхолдерів.

Вирішення кіберзагроз у ширшому масштабі також потребує узгоджених зусиль і співпраці між державою, бізнесом та суспільством, оскільки загрози мають транскордонний характер і швидко еволюціонують. Співпраця передбачає обмін інформацією, координацію дій і поширення найкращих практик, що допомагає підвищувати рівень обізнаності, покращувати можливості виявлення та запобігання атакам, зміцнювати стійкість критичної інфраструктури та прискорювати відновлення після інцидентів. Важливими умовами для цього є довіра, прозора комунікація, спільне бачення безпечного кіберпростору та відчуття розподіленої відповідальності; у практичній площині це реалізується через державно-приватні партнерства, розвиток правових і нормативних рамок, інвестиції в інфраструктуру кібербезпеки, підготовку фахівців та підтримку відповідальної поведінки користувачів у цифровому середовищі.

Висновки. Таким чином, кібергігієна в глобальній економіці постає не як суто технічний набір рекомендацій, а як системний інструмент підвищення стійкості держави, бізнесу й суспільства в умовах цифрової взаємозалежності та транскордонних загроз. Для України, яка одночасно інтегрується у світові цифрові ринки й перебуває в середовищі підвищеного ризику, пріоритетність кібергігієни визначається поєднанням економічних і безпекових чинників: безперервність роботи цифрової інфраструктури, довіра до сервісів і транзакцій, захист критичних систем та державних мереж, а також стабільність технологічного сектору прямо залежать від здатності знижувати імовірність інцидентів і обмежувати їх наслідки. Масштаб і еволюція кіберзагроз, у тому числі соціальна інженерія, шкідливе ПЗ, атаки на вебзастосунки, DDoS та використання вразливостей "нульового дня", підсилюють потребу в переході від фрагментарних заходів до комплексної моделі управління ризиками, що поєднує запобігання, виявлення, реагування та відновлення. Економічний вимір кіберінцидентів – від прямих збитків до втрат довіри, регуляторних санкцій, компрометації інтелектуальної власності й збоїв ланцюгів постачання – робить інвестиції в кіберстійкість не витратами "на ІТ", а елементом конкурентоспроможності та економічної безпеки. У практичному вимірі такий підхід передбачає одночасне посилення технічних контролів (зокрема DLP для захисту конфіденційних даних у хмарних та віддалених сценаріях), розвиток культури безпеки через навчання й підвищення обізнаності, а також інституційну й міжнародну взаємодію, без яких неможливі ефективний обмін інформацією, узгодження стандартів і координація дій у протидії кіберзлочинності.

1. Anderson R., Moore T. The Economics of Information Security // Science. 2006. Vol. 314, No. 5799. P. 610–613. DOI: 10.1126/science.1130992. URL: https://www.science.org/doi/10.1126/science.1130992

2. Kopp E. A., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability : IMF Working Paper WP/17/185. Washington, DC : International Monetary Fund, 2017. URL: https://www.imf.org/-/media/files/publications/wp/2017/wp17185.pdf

3. OECD. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Paris : OECD, 2015. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc/9789264245471-en.pdf

4. ENISA. Review of Cyber Hygiene practices. December 2016. ISBN 978-92-9204-219-6. DOI: 10.2824/352617. URL: https://www.enisa.europa.eu/sites/default/files/publications/WP2016%202-3%201%20Cyber%20Hygiene.pdf

5. World Economic Forum. Global Cybersecurity Outlook 2025. 2025. URL: https://reports.weforum.org/ docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

6. Горбаченко С. Кібербезпека як складова економічної безпеки України // Галицький економічний вісник. 2020. Т. 66, № 5. С. 180–186. URL: https://galicianvisnyk.tntu.edu.ua/pdf/66/903.pdf

7. Пахненко О., Божко М. Кіберзагрози як виклик економічній безпеці: потенціал технологічної інфраструктури України // Економіка і регіон. 2025. № 2(97). С. 191–197. DOI: 10.26906/EiR.2025.2(97).3857. URL: https://journals.nupp.edu.ua/eir/article/view/3857

8. Шестак Я. І. Кібергігієна у інформаційному просторі в умовах воєнного стану // Інформаційна безпека та комп'ютерні технології : тези доп. V Міжнар. наук.-практ. конф. Кропивницький : ЦНТУ, 2022. С. 5–6. URL: https://kbpz.kntu.kr.ua/file/content/6625/2022-v-mizhnarodna-naukovo-praktychna-konferentsiia-informatsiina-bezpeka-ta-komp-yuterni-tekhnolohii-.pdf

9. Parfomak P. W., Jaikaran C. Colonial Pipeline: The DarkSide Strikes : CRS Insight IN11667 (VERSION 2). 11 May 2021. URL: https://www.congress.gov/crs_external_products/IN/PDF/IN11667/IN11667.2.pdf

10. Cybersecurity and Infrastructure Security Agency (CISA). Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise. 2020. URL: https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

11. Federal Trade Commission. Equifax Data Breach Settlement. November 2024. URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

12. Hauet J.-P., Bock P., Foley R., Franзoise R. Ukrainian power grids cyberattack // InTech (ISA). March/April 2017. URL: https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack

13. Lewis J. Economic Impact of Cybercrime—No Slowing Down. February 2018. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

14. США нададуть $37 млн на кібербезпеку України // Фінансовий клуб. 05.06.2023. URL: https://finclub.net/news/ssha-nadadut-usd37-mln-na-kiberbezpeku-ukrainy.html

15. Мирончeнко Д.В. Етичні аспекти кібербезпеки у світовій економіці та міжнародних відносинах. Збірник наукових праць "Вчені записки". 2025. № 40(3). С. 133-140. http://doi.org/10.33111/vz_kneu.40.25.03.12.081.087

16. Мирончeнко Д. В., Сидоренко К. В. Роль ІТ-сектору України в системі забезпечення глобальної кібербезпеки // Економічний простір. 2023. № 186. С. 13–17. DOI: 10.32782/2224-6282/186-2. URL: https://prostir.pdaba.dp.ua/index.php/journal/article/view/1283

---

1. Anderson R., Moore T. The Economics of Information Security // Science. 2006. Vol. 314, No. 5799. P. 610–613. DOI: 10.1126/science.1130992. URL: https://www.science.org/doi/10.1126/science.1130992

2. Kopp E. A., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability : IMF Working Paper WP/17/185. Washington, DC : International Monetary Fund, 2017. URL: https://www.imf.org/-/media/files/publications/wp/2017/wp17185.pdf

3. OECD. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Paris : OECD, 2015. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc/9789264245471-en.pdf

4. ENISA. Review of Cyber Hygiene practices. December 2016. ISBN 978-92-9204-219-6. DOI: 10.2824/352617. URL: https://www.enisa.europa.eu/sites/default/files/publications/WP2016%202-3%201%20Cyber%20Hygiene.pdf

5. World Economic Forum. Global Cybersecurity Outlook 2025. 2025. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

6. Horbachenko S. Kiberbezpeka yak skladova ekonomichnoi bezpeky Ukrainy // Halytskyi ekonomichnyi visnyk. 2020. T. 66, No. 5. S. 180–186. URL: https://galicianvisnyk.tntu.edu.ua/pdf/66/903.pdf

7. Pakhnenko O., Bozhko M. Kiberzahrozy yak vyklyk ekonomichnii bezpetsi: potentsial tekhnolohichnoi infrastruktury Ukrainy // Ekonomika i rehion. 2025. No. 2(97). S. 191–197. DOI: 10.26906/EiR.2025.2(97).3857. URL: https://journals.nupp.edu.ua/eir/article/view/3857

8. Shestak Ya. I. Kiberhihiiena u informatsiinomu prostori v umovakh voiennoho stanu // Informatsiina bezpeka ta kompiuterni tekhnolohii : tezy dop. V Mizhnar. nauk.-prakt. konf. Kropyvnytskyi : TsNTU, 2022. S. 5–6. URL: https://kbpz.kntu.kr.ua/file/content/6625/2022-v-mizhnarodna-naukovo-praktychna-konferentsiia-informatsiina-bezpeka-ta-komp-yuterni-tekhnolohii-.pdf

9. Parfomak P. W., Jaikaran C. Colonial Pipeline: The DarkSide Strikes : CRS Insight IN11667 (VERSION 2). 11 May 2021. URL: https://www.congress.gov/crs_external_products/IN/PDF/IN11667/IN11667.2.pdf

10. Cybersecurity and Infrastructure Security Agency (CISA). Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise. 2020. URL: https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

11. Federal Trade Commission. Equifax Data Breach Settlement. November 2024. URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

12. Hauet J.-P., Bock P., Foley R., Franɜoise R. Ukrainian power grids cyberattack // InTech (ISA). March/April 2017. URL: https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack

13. Lewis J. Economic Impact of Cybercrime-No Slowing Down. February 2018. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

14. SShA nadadut $37 mln na kiberbezpeku Ukrainy // Finansovyi klub. 05.06.2023. URL: https://finclub.net/news/ssha-nadadut-usd37-mln-na-kiberbezpeku-ukrainy.html

15. Myronchenko D. V. Etychni aspekty kiberbezpeky u svitovii ekonomitsi ta mizhnarodnykh vidnosynakh. Zbirnyk naukovykh prats “Vcheni zapysky”. 2025. No. 40(3). S. 133–140. DOI: 10.33111/vz_kneu.40.25.03.12.081.087. URL: https://doi.org/10.33111/vz_kneu.40.25.03.12.081.087

16. Myronchenko D. V., Sydorenko K. V. Rol IT-sektoru Ukrainy v systemi zabezpechennia hlobalnoi kiberbezpeky // Ekonomichnyi prostir. 2023. No. 186. S. 13–17. DOI: 10.32782/2224-6282/186-2. URL: https://prostir.pdaba.dp.ua/index.php/journal/article/view/1283