Міністерство освіти і науки України
Сумський державний університет
Шосткинський інститут Сумського державного університету
Шосткинський фаховий коледж імені Івана Кожедуба СумДУ
Управління освіти Шосткинської міської ради
Виконавчий комітет Шосткинської міської ради

Матеріали всеукраїнської науково-методичної конференції

24 квітня 2025
Шостка



"ОСВІТА, НАУКА ТА ВИРОБНИЦТВО: РОЗВИТОК ТА ПЕРСПЕКТИВИ"

Міністерство освіти і науки України
Сумський державний університет
Шосткинський інститут Сумського державного університету
Шосткинський фаховий коледж імені Івана Кожедуба
Управління освіти Шосткинської міської ради
Виконавчий комітет Шосткинської міської ради

ОСВІТА, НАУКА ТА ВИРОБНИЦТВО: РОЗВИТОК ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ
X Всеукраїнської
науково-методичної конференції
(Шостка, 24 квітня 2025 року)

Суми
Сумський державний університет
2025

УДК 372.862

Редакційна колегія:
відповідальний редактор – к.т.н., доцент Р.В. Закусило;
заступник відповідального редактора – к.е.н, завідувач кафедри Ю.М. Мануйлович.

члени редакційної колегії:
к.х.н, ст.викладач С.В. Тимофіїв; к.філ.н, доцент Н.Ю. Бондар;
к.пед.н., доцент Ю.М. Мар'їнських; к.е.н, ст.викладач І.В. Новикова;
к.т.н., завідувач кафедри Г.М. Худолей; к.е.н, доцент О.М. Тур
к.е.н, ст.викладач І.В. Вареник;

ОСВІТА, НАУКА ТА ВИРОБНИЦТВО: РОЗВИТОК ТА ПЕРСПЕКТИВИ: матеріали X Всеукраїнської науково-методичної конференції, м. Шостка, 24 квітня 2025 року. – Суми : Сумський державний університет, 2025. – 298 с.

Збірник містить матеріали X Всеукраїнської науково-методичної конференції «Освіта, наука та виробництво: розвиток та перспективи», що проводиться на базі Шосткинського інституту Сумського державного університету. Тематика поданих матеріалів охоплює широке коло питань, присвячених актуальним проблемам сучасної освіти, науки та виробництва.
Видання корисне, викладачам, аспірантам і студентам вищих навчальних закладів, науковим співробітникам, працівникам хімічної промисловості, фахівцям інформаційних технологій виробництва, вчителям загальноосвітніх шкіл.

© Шосткинський інститут
Сумського державного університету, 2025
© Сумський державний університет, 2025

КІБЕРБЕЗПЕКА В ЕКОНОМІЦІ

Романюк О.Н., Нечипорук М.Л., Лесько О.Й., Шаманський А.А.
Вінницький національний технічний університет
rom8591@gmail.com

Кібербезпека в економіці набула особливої ваги в умовах цифрової трансформації фінансового сектору, торгівлі, логістики та державного управління.

Сучасна економіка дедалі більше залежить від цифрових технологій, що, у свою чергу, породжує нові ризики, пов’язані з витоком даних, фінансовим шахрайством, кібератаками на інфраструктуру та втручанням у критичні системи управління.

Економічна стабільність і довіра до ринку значною мірою залежать від здатності компаній та державних установ забезпечити конфіденційність, цілісність і доступність інформації, що циркулює в цифровому просторі.

Значення кібербезпеки в економіці проявляється насамперед у захисті фінансових систем. Банки, страхові компанії та фінансові платформи є основними цілями для кіберзлочинців через високий рівень цифровізації та велику кількість операцій. Внаслідок цього впровадження сучасних засобів автентифікації, шифрування, виявлення аномалій і реагування на інциденти стало ключовим напрямом розвитку. Зокрема, значного поширення набули технології багатофакторної автентифікації, поведінкової біометрії та аналізу великих даних для прогнозування загроз.

У корпоративному секторі кібербезпека відіграє критичну роль у захисті комерційної та виробничої інформації, запобіганні промисловому шпигунству та забезпеченні безперебійної роботи цифрових сервісів. Витік інтелектуальної власності або конфіденційних контрактів може мати серйозні наслідки для конкурентоспроможності підприємства. Саме тому компанії активно впроваджують політики інформаційної безпеки, навчають персонал правилам кібергігієни, проводять аудити IT-інфраструктури та застосовують системи захисту від DDoS-атак, фішингу й шкідливого програмного забезпечення.

З боку держави кібербезпека економіки розглядається як складова національної безпеки. Регуляторні органи розробляють стандарти захисту критичної інфраструктури, включаючи енергетику, транспорт, телекомунікації та фінанси. Створюються національні центри реагування на кіберінциденти, удосконалюється законодавство щодо кіберзлочинності, а також стимулюється розвиток національного кіберпростору, зменшуючи залежність від іноземних постачальників цифрових сервісів.

У світовій практиці дедалі більшого значення набуває економічна кіберрозвідка – аналіз кіберактивності для виявлення економічних загроз, включно з санкційною політикою, транснаціональним фінансовим шахрайством і діяльністю кіберугруповань. Великі корпорації інвестують у створення центрів кіберзагроз, де фахівці аналізують поведінкові моделі атак, будують прогностичні моделі та взаємодіють з міжнародними аналітичними структурами.

Таким чином, кібербезпека стала не лише технічним, а й стратегічним фактором в економічному розвитку. Від її рівня залежать інвестиційна привабливість країни, надійність бізнес-процесів і захист інтересів споживачів. Забезпечення кіберстійкості економіки вимагає комплексного підходу, що включає технічні засоби, правове регулювання, міжнародну кооперацію та формування культури безпеки серед усіх учасників економічної діяльності.

З огляду на стрімке впровадження цифрових технологій у всі сектори економіки, зростає потреба у створенні ефективних систем управління кіберризиками. Це включає не лише технічні засоби захисту, а й стратегічне планування, оцінювання потенційних загроз, прогнозування наслідків та розробку сценаріїв реагування. Все більше підприємств формують внутрішні відділи інформаційної безпеки або залучають сторонніх експертів для побудови комплексної архітектури кіберзахисту. Особлива увага приділяється захисту ланцюгів постачання – компанії ретельно оцінюють безпеку контрагентів, аби уникнути вторинного зараження або компрометації бізнес-процесів.

Окремим напрямом стає впровадження стандартів кібербезпеки у фінансовій звітності, де прозорість і відповідальність за збереження даних вимагають підтвердження аудиторами. Великі корпорації зобов’язані публікувати інформацію про інциденти, політику безпеки та заходи запобігання атакам. Це підвищує довіру інвесторів та сприяє зміцненню репутації на ринку. Національні та міжнародні регулятори дедалі частіше вимагають сертифікації кібербезпеки фінансових установ, бірж, страхових компаній та провайдерів платіжних сервісів. Наприклад, стандарт ISO/IEC 27001 став базовим документом для підтвердження відповідності систем захисту інформації на підприємствах.

Крім того, в умовах геополітичної нестабільності цифрова економіка потребує не лише захисту від традиційних кібератак, але й стійкості до інформаційних операцій, маніпуляцій на ринках та спроб дестабілізації фінансових систем з боку ворожих суб'єктів. Тут важливу роль відіграє співпраця між державою, приватним сектором і науковими установами, що дозволяє впроваджувати інноваційні рішення, адаптовані до змін середовища.

Цифрові платформи з елементами штучного інтелекту дедалі частіше використовуються для аналізу кіберзагроз, зокрема для виявлення аномалій в економічних транзакціях, підозрілої активності на біржах або шахрайських схем у сфері онлайн-комерції. ШІ дозволяє оперативно класифікувати загрози, прогнозувати сценарії атак і будувати автоматизовані системи протидії. У контексті банківських послуг такі інструменти істотно зменшують ризики втрати активів та підвищують якість обслуговування клієнтів.

На рівні міжнародного співробітництва актуальними залишаються питання уніфікації стандартів, спільного моніторингу транскордонних кіберзагроз і взаємного визнання сертифікатів безпеки. Україна бере активну участь у програмах кіберстійкості Європейського Союзу, отримує технічну допомогу від провідних держав, а також розвиває власні ініціативи щодо захисту економічного простору. Це включає підтримку стартапів у сфері кібербезпеки, підготовку фахівців та участь у проєктах кіберсимуляції, які моделюють дії в умовах кіберкризи.

Особливу вагу набуває підготовка кваліфікованих фахівців з економічної кібербезпеки. Зростає попит на аналітиків кіберризиків, аудиторів інформаційної безпеки, консультантів з кіберстрахування та ІТ-фахівців, які володіють економічними знаннями. Освітні заклади, реагуючи на ці виклики, відкривають нові спеціальності, впроваджують міждисциплінарні програми, де поєднуються знання з кібербезпеки, фінансів, права та управління ризиками. Особливо важливою стає підготовка кадрів, здатних діяти не лише в рамках організації, а й розуміти взаємозв’язки між кібербезпекою та макроекономічними процесами – вплив кібератак на стабільність валют, фондові індекси, банківську систему та національну економіку загалом.

Зміцнення кібербезпеки в економіці також тісно пов’язане із запровадженням кіберстрахування. Це порівняно новий інструмент фінансового захисту, який дозволяє компаніям перекладати частину кіберризиків на страхові організації. Страхування охоплює витрати на відновлення після кібератак, юридичну відповідальність, компенсації третім сторонам і витрати на комунікацію після інцидентів. Зростання обсягу кіберстрахового ринку свідчить про усвідомлення бізнесом потенційної вартості кіберінцидентів і прагнення до зменшення їх впливу на фінансову стійкість.

Важливою складовою є також розвиток цифрових інструментів для оцінювання кіберекономічних ризиків. Аналітичні платформи, які об'єднують дані про транзакції, поведінку користувачів, вразливості ІТ-систем та геополітичні чинники, дозволяють будувати інтегровані

моделі оцінювання ризиків. Це дає змогу економічним агентам приймати більш зважені рішення щодо інвестування, структурування бізнес-процесів та управління активами.

У сфері державного регулювання впроваджуються механізми кіберекономічного нагляду, які дозволяють оперативно реагувати на загрози, що мають потенціал системного впливу на економіку. Зокрема, це стосується кіберінцидентів у банківському секторі, енергетиці, телекомунікаціях і транспорті – сферах, від яких безпосередньо залежить економічна діяльність усіх суб'єктів.

На національному рівні створюються інтегровані платформи взаємодії між банками, IT-компаніями та регуляторами для обміну інформацією про інциденти, моделі загроз та засоби реагування.

В умовах війни та глобальної нестабільності питання економічної кібербезпеки в Україні постає як пріоритетне. Постійні атаки на критичну інфраструктуру, банківські установи, державні реєстри та сервіси змушують державу інвестувати у побудову стійкої цифрової архітектури. Це включає як фізичну децентралізацію дата-центрів, так і створення цифрових копій критичних активів у хмарних інфраструктурах, захищених за міжнародними стандартами. Розвивається партнерство з іноземними технологічними компаніями, а також формується власна кіберрезервна спроможність.

У підсумку, кібербезпека в економіці – це не лише питання захисту окремих інформаційних систем, а цілісна стратегія збереження стабільності фінансової системи, підтримки цифрових інновацій, формування довіри на ринку та забезпечення сталого економічного зростання. Її ефективність визначатиметься здатністю економіки не лише реагувати на загрози, а й запобігати їм, інтегруючи передові технології та міжсекторальну співпрацю.

В умовах глобалізації особливої актуальності набуває участь України в міжнародних кіберекономічних ініціативах. Це не лише дозволяє отримувати доступ до технологій, аналітичних інструментів та професійної підготовки, а й підвищує рівень інтеграції української економіки до світових ринків, які дедалі частіше ставлять високі вимоги до інформаційної безпеки бізнесу. Українські компанії, які прагнуть працювати з партнерами з ЄС, США чи Японії, мають відповідати вимогам міжнародних стандартів захисту даних, зокрема Загального регламенту захисту даних (GDPR), норм NIST, а також європейської директиви NIS2, що регулює безпеку критичних інформаційних систем.

Ще одним важливим чинником є розвиток довіри в цифровій економіці. Успішна комерційна діяльність в онлайн-середовищі залежить не лише від якості товарів чи послуг, а й від того, наскільки

споживачі впевнені у безпеці своїх даних та транзакцій. Саме тому компанії інвестують у публічну звітність з кібербезпеки, прозорі політики конфіденційності, системи реагування на інциденти з негайним інформуванням клієнтів. Формується нова економічна категорія – «цифрова репутація», яка визначає вартість бренду, впливає на ринкову капіталізацію та інвестиційну привабливість.

З практичної точки зору, підприємства впроваджують методології оцінки вартості цифрових активів та потенційних втрат у разі порушення їхньої безпеки. Використовуються моделі Threat Assessment and Remediation Analysis, Factor Analysis of Information Risk, які дозволяють кількісно оцінити ризики і планувати бюджет на кіберзахист з урахуванням економічної доцільності. Це забезпечує перехід від реактивного до проактивного управління ризиками, коли бізнес сам формує свою кіберекосистему з урахуванням стратегічних і фінансових інтересів.

Не менш важливою є роль цифрової ідентичності в економічному житті. Електронні підписи, цифрові сертифікати, біометричні платформи – все це стало базовою інфраструктурою для безпечного укладення договорів, реєстрації угод, подання звітності. Успішне функціонування електронного документообігу та онлайн-держпослуг також неможливе без відповідного рівня кіберзахисту. Саме тому розвиваються національні інфраструктури довіри, як-от Українська система електронної ідентифікації, що сприяє економічній діджиталізації з урахуванням принципів безпеки.

Таким чином, кібербезпека стає не додатковим елементом, а невід’ємною складовою всієї економічної діяльності – від малого бізнесу до транснаціональних корпорацій.

У майбутньому цей тренд лише посилюватиметься, а здатність економіки адаптуватися до кіберзагроз стане одним з ключових показників її ефективності та життєздатності. Україні вкрай важливо продовжувати інвестиції в цифрову інфраструктуру, кіберосвіту, нормативну базу та міжнародне співробітництво.

Перелік використаних джерел

1. Лісовська Ю.П. Кібербезпека: ризики та заходи. – Кондор, 2024. – 272 с.

2. Когут Ю. І. Кібертероризм (історія, цілі, об'єкти) : практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2023. – 304 с