УДК 331.108:316.422.44
DOI: 10.31733/15-03-2024/2/311-313

Катерина ГЛУХОВЕРЯ
начальник відділу
докторантури та аспірантури,
кандидат юридичних наук

Світлана ХАМІНІЧ
професор кафедри аналітичної
економіки та менеджменту
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ЕКОНОМІКА ЗНАНЬ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У сучасному інформаційному суспільстві економіка знань стає ключовим фактором розвитку національної економіки та забезпечення національної безпеки. Економіка знань спирається на створення, передачу та використання знань та інформації як основних ресурсів для досягнення конкурентних переваг та сталого економічного зростання. У контексті національної безпеки ця концепція набуває особливого значення, оскільки знання відіграють важливу роль у сферах освіти, науки, технологій, інновацій, культури та інформаційної безпеки.

Однією з основних концепцій економіки знань є ідея про те, що знання можуть бути розглянуті як окремий ресурс, подібний до традиційних ресурсів виробництва, таких як праця, капітал та земля. Це означає, що знання можуть бути використані для створення нових продуктів та послуг, покращення продуктивності та підвищення конкурентоспроможності компаній.

Ключовим елементом економіки знань є освіта. Високоякісна система освіти сприяє формуванню кваліфікованих кадрів, здатних працювати у сучасній економіці та суспільстві. Інвестиції в освіту та розвиток людського капіталу є не лише джерелом конкурентоспроможності, а й фундаментом національної безпеки, оскільки освічені та поінформовані громадяни сприяють стабільності та процвітанню країни [1].

Іншим важливим аспектом економіки знань є науково-технологічний розвиток. Інновації та технологічні досягнення відіграють ключову роль у підвищенні продуктивності праці, скороченні витрат, створенні нових товарів та послуг, а також у зміцненні оборонної спроможності держави. Підтримка та стимулювання наукових досліджень, розробок нових технологій та їх комерціалізації є невід'ємною частиною стратегії забезпечення національної безпеки.

Крім того, інформаційна безпека відіграє дедалі важливішу роль у контексті економіки знань. В умовах цифрової економіки та поширення інформаційних технологій захист інформації та даних стає пріоритетним завданням для держави та бізнесу. Кібератаки, витікання конфіденційної інформації та кібершпигунство можуть завдати серйозної шкоди економіці та національній безпеці, тому необхідно розвивати заходи щодо кіберзахисту, сприяти забезпеченню інформаційної безпеки.

Крім того, необхідно приділяти увагу розвитку цифрової грамотності та забезпечення інформаційної безпеки громадян. Підвищення рівня обізнаності населення про кіберзагрози, навчання навичок безпечного використання інформаційних технологій та захисту особистих даних є важливою складовою стратегії забезпечення національної безпеки у сфері економіки знань.

У сучасному світі, де знання та інформація стають основними ресурсами, економіка знань набуває все більшого значення в контексті національної безпеки. Інвестиції в освіту, науку, технології та інформаційну безпеку стають стратегічними пріоритетами для державної політики, оскільки вони сприяють зміцненню економічної та технологічної бази країни, підвищенню її конкурентоспроможності та забезпечення стабільності та безпеки у довгостроковій перспективі [2].

Важливо відзначити, що економіка знань також відіграє важливу роль у формуванні

культури та ідентичності нації. Розвиток національної культури, мистецтва, літератури та наукової спадщини сприяє збереженню культурного різноманіття та національної самоідентифікації. Підтримка та стимулювання творчої діяльності та інтелектуальної творчості також сприяє зміцненню національної ідентичності та згуртованості суспільства, що є важливим для забезпечення стабільності та солідарності всередині країни.

Крім того, економіка знань сприяє зміцненню зовнішньої безпеки держави. Країни, які мають сильну науково-технологічну базу та інноваційний потенціал, мають більше можливостей для встановлення партнерських відносин з іншими державами, а також для активної участі в міжнародних економічних та політичних процесах. У свою чергу це сприяє зміцненню міжнародного престижу та впливу країни, а також формуванню сприятливих зовнішніх економічних відносин, що є важливим фактором для її забезпечення національної безпеки.

Однак, незважаючи на численні переваги, економіка знань стикається з певними викликами та ризиками. Нерівномірний розподіл знань та доступу до них може призвести до поглиблення відмінностей між різними верствами суспільства та регіонами, що може створити напруженість та конфлікти. Більше того, загрози кібербезпеці, крадіжка інтелектуальної власності та недобросовісна конкуренція у сфері наукових досліджень та технологічного розвитку також потребують уваги та вжиття відповідних заходів для захисту національних інтересів та безпеки.

Отже, економіка знань відіграє важливу та багатогранну роль у забезпеченні національної безпеки. Вона сприяє розвитку людського капіталу, науково-технологічному прогресу, культурному розмаїттю та зовнішній безпеці держави. Однак, для максимізації користі від економіки знань та мінімізації ризиків необхідно розробити та реалізувати комплексні стратегії, що враховують інтереси держави, суспільства та людства загалом [3].

Важливим аспектом економіки знань у контексті національної безпеки є захист інтелектуальної власності та інноваційних розробок. Інтелектуальна власність відіграє ключову роль в економічному розвитку, оскільки сприяє стимулюванню інновацій та розвитку нових технологій. Проте загрози піратства, крадіжки технологій та порушення авторських прав можуть суттєво підірвати конкурентоспроможність та безпеку країни. Тому важливо розробити та реалізувати ефективні механізми захисту інтелектуальної власності, у тому числі за допомогою юридичних та технічних засобів, а також посилити міжнародне співробітництво у цій галузі.

Ще одним аспектом, який слід враховувати, є створення сталої інфраструктури інформаційних технологій. В умовах дедалі більшої цифровізації економіки та суспільства, уразливості інформаційної інфраструктури стають об’єктом пильної уваги для кібератак та кіберзлочинності. Захист критично важливих інформаційних систем та інфраструктури зв’язку стає невід’ємною частиною забезпечення національної безпеки.

Захист інтелектуальної власності, зміцнення інформаційної безпеки, розвиток цифрової грамотності та створення сталої інформаційної інфраструктури є ключовими напрямками діяльності у цій галузі. Реалізація ефективних заходів щодо безпеки у сфері економіки знань дозволить державам мінімізувати ризики та загрози, а також максимізувати користь від розвитку інтелектуального потенціалу та інноваційної активності.

Додатковим важливим аспектом, який слід розглянути в контексті економіки знань та національної безпеки, є роль науково-освітніх інститутів та дослідницьких центрів. Ці організації відіграють ключову роль у створенні нових знань, інновацій та технологій, які у довгостроковій перспективі стають фундаментом для економічного розвитку та національної безпеки.

Однак, для забезпечення національної безпеки необхідно також забезпечити свободу наукових досліджень та збереження інтелектуальної незалежності. Підтримка наукової свободи та захист прав інтелектуальної власності сприяють розвитку інновацій та залученню кращих розумів до країни. Однак це також вимагає уважного контролю за можливим зловживанням дослідженнями та розробками в галузі науки та технологій для військових чи шкідливих цілей.

Важливим аспектом забезпечення національної безпеки в контексті економіки знань є також міжнародне співробітництво та обмін знаннями. Взаємодія з іншими країнами в галузі науки, технологій та освіти може сприяти поширенню кращих практик, обміну досвідом та зміцненню взаєморозуміння. Однак, необхідно також враховувати можливі ризики та загрози для національної безпеки, пов’язані з передачею технологій та знань у чутливих галузях.

Таким чином, економіка знань відіграє важливу роль у забезпеченні національної безпеки, але потребує балансування різних інтересів та врахування можливих ризиків. Підтримка інновацій, захист інтелектуальної власності, забезпечення наукової свободи та міжнародне співробітництво є ключовими елементами стратегії забезпечення національної безпеки у сфері економіки знань. Реалізація ефективних заходів у цих сферах дозволить країнам максимізувати користь від розвитку знань та інновацій, мінімізуючи при цьому можливі загрози та ризики.

1. Хамініч С.Ю. Основні тренди освіти в системі економіки знань // Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки». 2023. №5. https://doi.org/10.25313/2520-2294-2023-5-8886.

2. Khaminich S., Heti K. (2023), The knowledge economy as a factor for enterprise development in management system. *Philosophy, Economics and Law Review*. Volume 3, no. 1, 103-115. DOI: 10.31733/2786-491x-2023-1-103-115.

3. Kovalenko-Marchenkova Y. (2022). Management of the national economy as an element of the socio-economic space of the country. *Philosophy, Economics and Law Review*. Volume 6, no. 3, 30-37. DOI: 10.31520/2616-7107/2022.6.3-4.

УДК 004.056.57
DOI: 10.31733/15-03-2024/2/313-315

Андрій ГРЕБЕНЮК
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

DDoS АТАКИ В УКРАЇНІ:ВИКЛИКИ ТА ДОКУМЕНТУВАННЯ ЗАГРОЗ

У сучасному цифровому світі, де залежність від технологій надто велика, інтернет-простір стає ареною для різноманітних кіберзагроз. Однією з таких загроз є атаки типу DDoS (розподілені атаки на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам), які в Україні виявилися особливо проблематичними. Це явище не тільки порушує безпеку в Інтернеті, але і викликає серйозні наслідки для українського суспільства та економіки. Однією з основних проблем, пов'язаних з DDoS атаками, є їх розподіленість і широка масштабність. Кіберзлочинці використовують ботнети для організації атак, що робить важким визначення точного джерела нападу. Україна, будучи цифрово розвиненою країною, стала привабливою мішенню для таких атак підчас військової агресії близького сусіда. Захист від DDoS атак в Україні став питанням національної безпеки.

Захист від DDoS атак в Україні є надзвичайно важливою задачею для бізнесу, урядових організацій та інших важливих інфраструктурних об'єктів. Нижче подано кілька ключових стратегій та заходів для захисту від DDoS атак:

– Встановлення систем моніторингу та ідентифікації аномалій, які можуть вказувати на DDoS атаку. Використання спеціалізованих програм та апаратних засобів для виявлення надмірної активності.

– Застосування фільтрів на рівні мережі для блокування небажаних пакетів. Використання пристроїв із вбудованими системами фільтрації DDoS-трафіку.

– Встановлення та оновлення відповідного програмного забезпечення для виявлення та захисту від DDoS атак.

– Використання веб-файрволів та веб-безпеки для фільтрації та блокування небажаних трафіку.

– Забезпечення еластичності і масштабованості мережевої інфраструктури для можливості реагування на збільшену активність. Використовувати запасні інтернет-канали для перехоплення трафіку у разі атаки та забезпечення безперервності послуг.

– Використання хмарних служб захисту від DDoS, які можуть фільтрувати трафік