УДК 004.738.5:351.862.4:316.42
DOI: 10.31733/15-03-2024/2/343-345

Володимир МИРОШНИЧЕНКО
аспірант кафедри аналітичної
економіки та менеджменту

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

РОЛЬ ІНФОРМАЦІЙНОГО ФАКТОРА В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЙНИХ ВИКЛИКІВ

Глобалізація, високий рівень інформаційних технологій, а саме – інформаційний фактор відіграє ключову роль у забезпеченні національної безпеки. Глобалізаційні виклики створюють низку нових аспектів у цю проблематику, вимагаючи від держав їх адаптації до нових умов та посилення зусиль щодо захисту своїх інтересів та громадян.

Основні засади впливу інфрмаційного фактора на забезпечення національної безпеки в умовах глобалізаційних викликів полягають в наступному:

- динамічний інформаційний ландшафт;
- інформаційна війна та кіберзагрози;
- координація зусиль;
- безперервний аналіз та адаптація;
- етика та законність у використанні інформації;
- створення резервів та гнучких систем;
- підвищення обізнаності суспільства;
- інтеграція інформаційної безпеки у національні стратегії;
- розвиток міжнародного співробітництва;
- інновації та дослідження;
- прозорість та відповідальність;
- навчання та освіта;
- зміцнення інститутів громадянського суспільства;
- інноваційні підходи до захисту даних;
- сприяння міжнародній стабільності.

У процесі розвитку інтернету та соціальних мереж інформаційний ландшафт став більш динамічним та доступним. Це створює як нові можливості, так і нові загрози національній безпеці. Перед державами постають завдання ефективного контролю над поширенням інформації, захисту від кібератак та інформаційної війни.

Інформаційна війна стає дедалі серйознішою загрозою держав. Маніпуляції з громадською думкою, дезінформація та кібератаки можуть призвести до дестабілізації політичної ситуації, а також до економічної та соціальної шкоди. Подібні атаки можуть йти як з боку інших держав, так і з боку недержавних акторів, що ускладнює завдання національної безпеки.

Проте ефективна протидія інформаційним загрозам потребує не лише внутрішніх заходів безпеки, а й міжнародного співробітництва. Глобальні проблеми потребують глобальних рішень, і в цьому контексті важливо зміцнювати міжнародне співробітництво у сфері інформаційної безпеки, обмінюючись інформацією та найкращими практиками.

Складність інформаційних загроз вимагає постійного аналізу та адаптації стратегій безпеки. Держави та організації повинні бути готовими до швидкого реагування на нові види загроз, використовуючи передові технології та методи захисту. Це також включає постійне навчання персоналу та розробку інноваційних підходів до проблем інформаційної безпеки [1].

Одним із ключових аспектів забезпечення інформаційної безпеки є дотримання етичних та законних принципів у використанні інформації. Держави та організації повинні

діяти в рамках міжнародного права та поважати права людини під час використання інформаційних технологій. Це важливо для підтримки довіри до систем інформаційної безпеки та запобігання можливим порушенням.

Національна безпека має ґрунтуватися на принципах гнучкості та резервування. Створення запасних систем та механізмів реагування дозволить швидко компенсувати збитки від можливих інформаційних атак та мінімізувати їх наслідки. Це також включає розробку планів надзвичайних ситуацій і навчання персоналу на випадок кіберкриз.

Зрештою, важливо активно включати суспільство у процес забезпечення інформаційної безпеки. Це може бути досягнуто шляхом проведення інформаційних кампаній, навчання громадян основам кібербезпеки та розвитку медіаосвіти. Чим більше обізнані громадяни, тим ефективнішим буде опір інформаційним загрозам та захист національних інтересів.

Для ефективної протидії інформаційним загрозам необхідно інтегрувати питання інформаційної безпеки у спільні національні безпекові стратегії. Це означає врахування інформаційних аспектів при розробці та реалізації стратегій національної безпеки, а також включення інформаційних аспектів у навчання та підготовку фахівців із безпеки [2].

Інформаційні загрози часто мають транскордонний характер, тому ефективна протидія їм вимагає міжнародного співробітництва. Держави повинні активно обмінюватися інформацією про нові загрози та спільно розробляти заходи щодо їх протидії. Також важлива співпраця між державами та міжнародними організаціями у галузі розробки міжнародних стандартів та нормативів у галузі інформаційної безпеки.

Розвиток нових технологій та методів захисту інформації відіграє важливу роль у забезпеченні інформаційної безпеки. Тому держави мають інвестувати в наукові дослідження та стимулювати інновації у сфері кібербезпеки. Це дозволить розробити ефективніші технології захисту інформації та оперативно реагувати на нові загрози.

Важливим аспектом забезпечення інформаційної безпеки є прозорість дій державних та приватних структур у сфері інформаційної політики. Держави повинні здійснювати моніторинг інформаційних атак, а також інформувати громадськість про свої дії щодо захисту інформації. При цьому важливо дотримуватись принципів правової держави та захисту прав громадян на доступ до інформації.

Одним із важливих аспектів забезпечення інформаційної безпеки є освіта та навчання населення. Необхідно проводити системну роботу щодо підвищення інформаційної грамотності громадян, включаючи поінформованість про методи захисту персональних даних, впізнання фейкової інформації та вміння оцінювати надійність джерел. Це дозволить створити більш поінформоване суспільство, яке здатне ефективно захищати себе від інформаційних загроз.

Громадські організації та незалежні медіа відіграють важливу роль у забезпеченні інформаційної безпеки. Вони можуть виступати в якості контролюючого органу, відстежуючи та повідомляючи про порушення правил обробки інформації та інформаційної безпеки. Тому важливо підтримувати їхню роботу та захищати їхню незалежність.

У процесі розвитку технологій штучного інтелекту та квантових обчислень постають нові виклики та можливості для захисту інформації. Інноваційні методи шифрування та аутентифікації можуть стати потужним інструментом у боротьбі з кіберзагрозами. Тому важливо інвестувати у розробку та впровадження нових технологій у галузі кібербезпеки.

Як глобальні проблеми потребують глобальних рішень, так і загрози інформаційній безпеці потребують спільних зусиль держав на міжнародному рівні. Тому важливо активно сприяти міжнародному співробітництву у сфері інформаційної безпеки, у тому числі через міжнародні організації та форуми [3].

Із урахуванням зростаючого значення інформаційного чинника важливо розвивати системи інформаційної безпеки на державному та міжнародному рівнях, що включає удосконалення законодавства в галузі кібербезпеки, розвиток технологій захисту інформації, а також підвищення інформаційної грамотності серед населення.

Таким чином, інформаційний чинник відіграє дедалі значнішу роль забезпеченні національної безпеки за умов глобалізаційних викликів. Держави повинні вживати заходів як на внутрішньому, так і на міжнародному рівнях для захисту від інформаційних загроз та забезпечення стабільності та безпеки своїх громадян. Ефективна протидія інформаційним загрозам вимагає комплексного підходу, що включає технологічні, організаційні, правові та освітні заходи. Тільки так можна забезпечити стабільність та безпеку сучасного суспільства

в умовах сучасного інформаційного суспільства.

1. Інституціональне забезпечення конкурентоспроможності національної економіки: монографія / за заг.ред. д.е.н., проф.С.Ю. Хамініч._ Дніпро : Арт-Прес.2023. 144с.

2. Alieksieieva S., Kozhusko O., Khaminich S. Information system protection as a factor in maintaining the leading positions in the enterprise development. Proceedings of the 3rd International Conference on Social, Economic, and Academic Leadership (ICSEAL 2019), Series: Advances in Social Science, Education and Humanities Research, https://doi.org/10.2991/icseal-19.2019.67. URL : https://www.atlantis-press.com/proceedings/icseal-19/articles. p.428-432/

3. Хамініч С.Ю. Інституціональні засади економічної безпеки України в умовах війни // Міжнародний науковий журнал «Інтернаука». Серія: «Економіка». 2023. № 2. URL : https://doi.org/10.25313/2520-2294-2023-2-8626.

УДК 004.738.5
DOI: 10.31733/15-03-2024/2/345-346

Олександр ТУБАНЬ
аспірант Науково-дослідного інституту
приватного права і підприємництва
імені академіка Ф. Г. Бурчака
НАПрН України

ОКРЕМІ АСПЕКТИ УБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ ВІД ЗАГРОЗ В ЕЛЕКТРОННИХ МЕРЕЖАХ

У сучасному світі надзвичайно швидко поширилися інформаційні технології, які супроводжують кожну галузь і сферу господарювання і повсякденного буття людини. Велику кількість угод можна укласти, не виходячи із дому чи офісу. Навіть сфера обігу національної валюти поступово втрачає вагу на фоні поширення обігу електронних грошей – криптовалют, ще генеруються на блокчейн-платформах. Навіть саме генерування, видобуток, виробництво або «майнінг» одиниць криптовалюти має децентралізований характер. Кожне підприємство або людина, які мають комп'ютери із сучасним програмним забезпеченням, можуть займатися «майнінгом» криптовалюти. А сама ця діяльність має значну схожість із класичними видами господарської діяльності [1]. Із п'яти ознак, що характеризують економічну сутність як правосуб'єктне утворення, чотири повною мірою притаманні таким особам та групам, а п'ята ознака має переважно суб'єктивний характер. Офіційне визнання державою законним видом господарської діяльності «майнінгу» криптовалюти та визнання господарськими операцій із її купівлі-продажу у комплексі з покладанням на «майнерів» обов'язку офіційно зареєструватись як суб'єкт підприємницької діяльності, поширенням на всіх учасників відносин на ринку криптовалюти дії законодавства про оподаткування та кримінальної, адміністративної, господарської відповідальності до порушників дасть змогу усунути невизначений або гібридний правовий статус суб'єктів та режим їхньої діяльності, а також наявні прогалини у праві та законодавстві [1]. Проте проблема у легітимації «майнерів» криптовалюти не є найскладнішою і не становить найвищої загрози кібербезпеці держави. Забезпечення кібербезпеки України важливе не лише для економічного розвитку, але й для забезпечення захисту національної безпеки та підвищення ступеня довіри громадян.

Проєктом Стратегії кібербезпеки України визначено пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [2].

Аналіз кіберзагроз та ризиків в контексті поширення обігу криптовалют у сучасному суспільстві стає критично важливим завданням для забезпечення кібербезпеки в електронних мережах України.

Сучасний кіберпростір спрямований на подальший розвиток технологій, але разом із тим породжує нові виклики та загрози. Аналіз кіберзагроз у сфері обігу криптовалют включає в себе вивчення різноманітних аспектів:

- фінансові шахрайства: передбачає дослідження методів та схем шахрайства, спрямованих на виведення коштів через використання криптовалют;
- технічні загрози: передбачає виявлення вразливостей у блокчейн-платформах, їх