DOI: https://doi.org/10.36059/978-966-397-391-3-47

ГЛОБАЛЬНА ІНФОРМАЦІЙНА БЕЗПЕКА: СУТНІСТЬ ТА АКТУАЛЬНІ ВИКЛИКИ

Рябець Наталія Миколаївна
кандидат економічних наук,
доцент кафедри міжнародного менеджменту,
Київський національний економічний університет
імені Вадима Гетьмана
Тимків Ірина Валеріївна
кандидат економічних наук,
доцент кафедри міжнародного менеджменту,
Київський національний економічний університет
імені Вадима Гетьмана

В умовах прискорення процесу глобальної інформатизації, всеохоплюючу діджиталізацію, окреслення набули принципово нові категорії – «інформаційне суспільство» та «кіберпростір». За сучасних умов розвитку, що окрім іншого характеризуються наростанням конфліктів та геополітичної напруги між різними акторами глобальної економічної системи, уряди країн, транснаціональні корпоративні структури, міжнародні інституції та людство в цілому стикаються із потужними викликами та ризиками, що безпосередньо стосуються інформаційної гігієни та інформаційної безпеки, яка окрім іншого може мати і деструктивну дію через її практично необмежені можливості впливу на всі сфери життєдіяльності людства. Даний вплив не завжди носить мирний характер, що й спричинило виникнення таких понять як «кібербезпека» та «інформаційна безпека», актуальність яких посилюється трансформаціями, що мають місце в архітектурі міжнародних відносин, суттєвим підвищенням ролі збройного виду насильства задля забезпечення реалізації власних геополітичних амбіцій держав. Наразі є всі підстави вважати інформаційну безпеку країни невід'ємною складовою її національної безпеки, оскільки визначає не лише рівень захисту та сталості основних сфер життєдіяльності суспільства, але і динаміку його розвитку за рахунок ефективної практичної імплементації згенерованих людством знань.

На сьогодні ще не сформовано уніфікованого підходу щодо сутності категорії «інформаційна безпека», що обумовлено тим, що безпосередньо предмет, безпека якого ідентифікується, не є виявленим а ні за внутрішньою конструкцією а ні за його внутрішніми властивостями. У найбільш загальному випадку інформаційну безпеку пропонують визначати як стан протекції інформаційного простору суспільства, який

убезпечує його формування, застосування та прогрес в інтересах суспільства та держави в цілому [1, с. 97]. Водночас під інформаційним простором пропонується розуміти сферу діяльності суб'єктів інформаційних взаємовідносин, що пов'язана із генеруванням, обробкою та споживанням інформаційного контенту. Щодо глобальної інформаційної безпеки, то слід зазначити, що глобальну безпеку як таку варто асоціювати із політикою, реалізація якої спрямована на формування ефективних гарантій забезпечення миру як на рівні окремої держави, так і в глобальному масштабі, водночас, що в контексті інформаційної безпеки, зокрема й глобальної, первинною є інформаційна загроза, яка своєю чергою можна розцінюватись як визначені конкретні дії (як діяльність, так і бездіяльність), що несуть виключно високий ступень суспільної небезпеки та мають прямий причинно-наслідковий зв'язок щодо зміни відповідних умов, факторів та інших вимірів інформаційних процесів, що визначають безпечність умов життєдіяльності соціуму, держави та глобальної цивілізації в цілому. Відповідно, глобальну інформаційну безпеку слід розуміти як стан, за якого через використання міжнародних ресурсів забезпечується дієвий захист від деструктивного інформаційного впливу на свідомість глобального суспільства, повністю унеможливлюється інформаційне втручання у процес прийняття рішень на рівні держав та наднаціональних інституцій, а також цілковита недоторканість приватних, державних та міждержавних баз даних, що мають цифровий формат, можливість їхнього швидкого поновлення у випадку незаконного посягання та забезпечення карності ініціаторів такого роду замахів та посягань. Глобальна інформаційна безпека водночас може розглядатися як процес взаємодії акторів міжнародних відносин, що має на меті забезпечення сталого миру на основі протекції глобального інформаційного простору та інфраструктури, суспільної розсудливості і від реальних та ймовірних інформаційних загроз. Серед сучасних особливостей проявів загроз інформаційні безпеці можна виокремити наступні: 1) «інформаційні війни», під якими дослідники розуміють найбільш небезпечні для країни та глобальної спільноти дії, що ставлять під загрозу інформаційну безпеку, та реалізуються однією державою або групою країн; 2) «інформаційний тероризм» – дії, які як правило, реалізуються міжнародними терористичними угрупуваннями та мають на меті досягнення політичних, релігійних та інших цілей через створення дестабілізації та поширення страху в державі або в ряді держав; 3) «інформаційний злочин» – дії, що становлять загрозу інформаційній безпеці, ініційовані особами, які мають злочинний намір щодо досягнення злочинних цілей.

Як свідчать дослідження фахівців корпорації Microsoft, результати якого висвітлено в Microsoft Digital Defense Report, за останні два роки приблизно 60% загальної кількості кібератак було здійснено з росії. При

цьому у звіті наголошується на зростанні питомої частки успішних атак: у 2021 році їх частка становила лише 21%, а вже наступного 2022 року – сягнула 32% [2]. Кібертаки з даної країни дедалі частіше мають за ціль міжнародні урядові інституції та державні структури інших країн (переважно ті, що відповідальні за зовнішню політику, нацбезпеку або оборону) для отримання розвідувальних даних, число яких зросло з 3% в структурі всіх цілей у 2021 році до 53%. До складу першої трійки держав-мішеней кібератак росії, увійшли США, Україна та Королівство Великобританії. В той же час рф – не єдина країна, яка займається розвитком заходів щодо підриву інформаційної безпеки та розширенням кіберзлочинності на державному рівні. Слідом за нею найбільше число атак. згідно звітності Microsoft, було реалізовано Північною Кореєю Іраном та Китаєм.

Також стрімкого розвитку протягом останнього часу набуває так звана економіка «кіберзлочинності як виду послуги», яка із швидкозростаючої індустрії перетворилась на цілком зрілий різновид злочинної діяльності. В наш час практично будь-кому, незалежно від рівня технічних знань та вмінь, може бути наданий доступ до ринку, що функціонує в онлайн форматі, щоб придбати комплекс послуг щодо проведення кібератак, що мають різноманітне цільове спрямування.

Дослідження свідчать, що наразі кардинальних змін зазнає оцінка та значення інформаційної доктрини з боку переважної більшості країн світу, адже відсутність системи дієвих заходів щодо забезпечення інформаційної безпеки на рівні однієї країни, зводить до нуля можливість її забезпечення не лише в межах держави, а й у міжнародному та глобальному вимірах. Зважаючи на масштаб проблеми щодо інформаційної безпеки, країни світу, насамперед розвинуті, започаткували дали старт реалізації довгострокових державних ініціатив та програм, що мають на меті забезпечення захисту найважливішим інформаційним структурам. Аналітики та експерти з питань безпеки альянсу НАТО виокремлюють чотири альтернативні варіанти інформаційної безпеки: 1) модель 1 передбачає створення абсолютної системи захисту країни, що виступає інформаційним лідером. Відповідно до даної моделі, в залежності від числа суб'єктів системи безпеки, можливим є три конкуруючі моделі інформбезпеки: система безпеки, що є однополярною, «концерт (альянс) держав», багатополярна модель, глобальна (універсальна) модель; 2) модель 2 – формування вагомої переваги держави-потенційного ініціатора інформаційної війни у наступальних видах озброєнь, координація дій із союзниками із використанням визначених методів інформаційної боротьби для визначення джерел та типів потенційних інформаційних загроз; 3) модель 3 виокремлює декількох країн, що є інформаційними лідерами, та наявність протистояння між ними; 4) модель 4, відповідно до якої, всі

сторони конфлікту застосовують транспарентність інформації задля формування ситуативних альянсів, що мають на меті досягнення стратегічних переваг локальних рішень, що здатні заблокувати можливості технологічного лідерства.

Варто констатувати, що країни все частіше звертаються до кібератак для реалізації будь-яких своїх політичних цілей або шпигунства, підриву чи то знищення. В контексті наростання геополітичної напруги та невизначеності, експерти прогнозують, що дедалі більше держав приєднуватимуться до числа тих, хто приймає активну участь у наступальних кібероперація, до того ж дані операції дедалі будуть ще більш зухвалими, масштабними та руйнівними, з більш глибинними та серйозними наслідками. При цьому глобальний ринок злочинності ставатиме все більш майстерним, витонченим та спеціалізованим за умови, якщо глобальна спільнота не вживатиме активних кроків щоб протидіяти його розвиткові та зміцненню. В даний час, незважаючи на те, що як з боку національних урядів, так із боку корпоративних структур докладається більше, ніж в будь-який інший період розвитку, зусиль задля протистоянню та нівелюванню даних викликів та загроз, необхідним є прагнення та досягнення того, щоб питання інформаційної безпеки та її виклики постійно залишалися фокусі уваги національних та наднаціональних порядків впродовж найближчих років.

Список використаних джерел:

1. Лук'янова В.В., Лаутар А.Ю. інформаційна безпека в умовах розвитку інформаційної системи. *Вісник Хмельницького національного університету*. 2013. № 12. Т. 3. С. 97–101.

2. Microsoft Digital Defense Report: web-site. URL: https://www.microsoft.com/en-us/security/business/microsoft-digitsl-defense-report?rtc=1