Вісник Львівського університету. Серія філос.-політолог. студії. 2024. Випуск 55, с. 247–254
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 55, p. 247–254

УДК 327
DOI https://doi.org/10.30970/PPS.2024.55.30

СУЧАСНІ ВИКЛИКИ ГЛОБАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Олексій Буряченко
Національний авіаційний університет, факультет міжнародних відносин,
кафедра міжнародних відносин та стратегічних студій
пр-т Любомира Гузара, 1, 03058, м. Київ, Україна

У статті розглядаються ключові аспекти глобальної інформаційної безпеки в умовах сучасних загроз та викликів. Основна увага приділяється викликам, що постають перед державами, організаціями та окремими акторами в контексті стрімкого розвитку технологій, зокрема кіберсфери. Автором досліджено та проаналізовано основні тенденції, які впливають на інформаційну безпеку, зокрема еволюцію атак, нові вразливості і зміни в тактиці хакерів та зловмисників. Також автором проведено детальний аналіз сучасних кіберзагроз, таких як атаки на інфраструктуру критичного значення, фішинг, вірусне програмне забезпечення, дезінформація та інші види зловмисної діяльності. Проаналізовані технічні та організаційні заходи, які необхідно вжити для забезпечення високого рівня кіберзахисту. Підкреслюється необхідність комплексного підходу до кібербезпеки, що включає як технічні, так і організаційні заходи, а також важливість постійного моніторингу та адаптації до нових викликів. Особливу увагу в статті приділено впливу штучного інтелекту (ШІ) на сферу безпеки та зауважено, що ШІ може бути використано як для створення нових видів атак, так і для розробки інноваційних безпекових методів.

Автор ґрунтовно зауважує на необхідності комплексного підходу до забезпечення міжнародної безпеки в контексті глобальної інформаційної безпеки, що включає технічні інновації, організаційні, політико-правові стратегії та моніторинг нових загроз. Також важливим аспектом він виділяє міжнародну співпрацю та обмін інформацією для ефективної боротьби з кіберзлочинністю, інформаційними війнами, антигуманною пропагандою тощо. Автор наголошує на важливості проведення наукових досліджень та напрацюванні нових концептуальних моделей, які б враховували всі аспекти інформаційної безпеки та забезпечили системний підхід і надійний захист від сучасних загроз в постійно мінливому інформаційному просторі.

Ключові слова: глобальна інформаційна безпека, міжнародна безпека, інформаційна війна, кібератаки, кібербезпека, дезінформація, штучний інтелект (ШІ).

Вступ. У сучасному світі цифрові технології значно впливають на інформаційну безпеку, що стає критично важливою для захисту даних і стабільності суспільного розвитку загалом. Глобалізація інформаційних потоків і залежність від інтернету створюють нові загрози, такі як кіберзлочинність, фішинг, витоки даних, державні кібератаки. Державні актори, як Росія, використовують кіберпростір для досягнення геополітичних цілей, наприклад, через кібершпигунство, дезінформацію. Особливе місце серед таких сучасних викликів науковці вже традиційно відводять інформаційній війні, що ведуться через медіа та соцмережі для впливу на громадську думку, маніпулювання соціальними групами тощо. Використання штучного інтелекту (ШІ) у цих процесах ще більше ускладнює ситуацію, створюючи загрози, які можуть вплинути на міжнародну стабільність. До прикладу, Китай, Росія, США активно використовують ШІ для досягнення політичних і військових переваг, що як наслідок актуалізує питання прав і свобод громадян та питання національної безпеки. Зазначимо, автоматизація військових процесів і використання ШІ для кібератак

ускладнюють контроль за інформаційним простором. Отож, для ефективного протистояння цим викликам потрібна міжнародна співпраця, технологічні інновації та політична воля.

Тому **метою** та **завданням** цієї статті автор вбачає: дослідити вплив цифрових технологій і штучного інтелекту на інформаційну безпеку в контексті глобальних викликів; проаналізувати ключові загрози та роль держав у кіберпросторі, вплив штучного інтелекту на кібербезпеку; визначити кроки для протистояння відповідним загрозам через міжнародну співпрацю.

Методами дослідження послугували аналіз наукових досліджень і звітів, вивчення практичних кейсів з інформаційної безпеки, аналіз даних з кібербезпекових інструментів, що доповнюється порівнянням міжнародних стандартів і стратегій, а також оцінкою ефективності існуючих заходів і рекомендацій для покращення кіберзахисту. Варто зауважити, що серед різних зацікавлених суб'єктів державні актори, зокрема активно використовують кіберпростір для досягнення своїх геополітичних цілей, здійснюючи шпигунство, саботаж через відповідні технології. Це створює додаткові виклики для міжнародної спільноти, для встановлення ефективних механізмів захисту, а також для дослідження відповідних небезпек.

Виклад основного матеріалу. Нерідко, об'єднуючи різні виклики інформаційної безпеки, у сучасних джерелах зауважується про більш комплексне поняття інформаційної війни як виду протистояння через засоби масової інформації та соціальні мережі, спрямованого на підтримку власного населення, спонукання прихильності потенційних союзників, а також на розповсюдження розгубленості та недовіри населення противника. Прикладом країни, що активно використовує методи інформаційної війни часто називають Росію, оскільки, вона застосовує кібероперації, включаючи дестабілізацію українського уряду та західних країн. Зауважимо, до повномасштабного вторгнення в Україну об'єктами дезінформаційних кампаній Росії стали українські військові, ціллю таких кампаній було створити хаос і паніку; заяви Росії про «звільнення» частини України є частиною дезінформаційної стратегії, яка була спрямована на міжнародну аудиторію [1, с. 54].

Зазначимо, в онлайн-просторі інформаційна війна є цілим комплексом впливів між соціальними групами, зорієнтована на те, щоб досягти переваг у військовій, політичній, економічній, культурній, громадській сферах. Така війна має технологічні аспекти: цифрові комунікації, технології створення, зберігання, поширення і пошуку інформації, а також психотехнології. Будь-який із цих аспектів має свої методи та інструменти, які визначають напрями досліджень і практичної діяльності.

Мотивами для застосування пропаганди та поширення фейкових новин можуть бути різні стратегії, починаючи зі свідомих спроб поширити неправдиву інформацію, закінчуючи наміром посіяти сумніви серед громадян. Кожен із методів впливу має свої інструменти та методологічні складові, які формують сучасну систему управління інформаційними процесами в умовах конфліктів.

Осмислюючи загрози інформаційній безпеці, дійсно важливо визначати чіткіше поняття. У наукових джерелах вже здійснено кілька таких важливих кроків. Зокрема зауважується, що як і будь-яка інша форма війни, війна інформаційна може впливати на міжнародні відносини в різний спосіб, відповідно йдеться й про різні терміни, такі як «інформаційна перевага», «психологічний вплив», «маніпуляція». Зокрема публічна онлайн-сфера постає складним середовищем, що сприятливе для швидкого розповсюдження фейкових новин, а маніпулятори мають змогу скористатись низьким рівнем довіри до інституцій, політиків, експертів. Тобто основою для сучасних інформаційних протистоянь

є маніпуляція. Згідно з джерелами (наприклад, глосарієм «Академічна протидія гібридним загрозам»), маніпуляція – це зміна змісту тексту, фото, відео чи аудіо з метою передачі зміненого повідомлення; це один з методів дезінформації, що передбачає навмисне розповсюдження неправдивих чи упереджених новин у політичних цілях, наприклад, вплив на майбутні голосування; це масове поширення через інтернет та служби зв'язку неправдивих даних як ключовий елемент інформаційної війни загалом [1, с. 54].

Зазначимо, інформаційна безпека для сучасного світу має глобальні наслідки. Вагомо змінив порядок інформаційної безпеки та інформаційної війни, а також структуру міжнародних відносин загалом, на думку багатьох дослідників – ШІ. Складними викликами, що потребують підходу та стратегії їх вирішення є використання ШІ в інформаційній війні та операціях впливу (IWIO). Активне використання ШІ в IWIO стає однією з найбільших загроз з боку держав, зокрема США, Китай, РФ. Як зазначають західні аналітики, ці держави інтегрують ШІ у свою стратегію інформаційної війни, і це дозволяє їм ефективніше впливати на інформаційний простір і маніпулювати громадською думкою. До прикладу, Росія активно використовує алгоритми ШІ для створення дезінформації, яка підриває довіру до урядів західних країн і сприяє посиленню політичних конфліктів. Китай використовує ШІ не лише для впливу на міжнародну арену, а й для внутрішньополітичного контролю: застосовуючи технології збору даних і алгоритми машинного навчання, уряд має змогу ефективно моніторити та контролювати власних громадян, а також використовувати зібрані дані для впливу на демократичні процеси всередині інших країн. Це стає причиною серйозної загрози не лише для інформаційної безпеки, але й для прав і свобод громадян, що проживають в демократичних країнах. Разом з тим, така потужна держава як США хоча і має значні можливості в інформаційних технологіях, зокрема у сфері ШІ та інформаційної безпеки, вона зіштовхується з обмеженнями, пов'язаними з демократичними інститутами та захистом прав людини, що виключає можливість ефективного збору даних і застосування ШІ у військових цілях, і ставить країну в менш вигідне становище з авторитарними режимами, які мають значно більшу свободу дій в цій сфері та користуються нею. Проте США активно працюють над розвитком захисту технологій в цілях протидії впливу дезінформації та різним кіберзагрозам, що будуть спрямовані проти країни [2, с. 2-10, 15].

Отже, сучасні виклики глобальної інформаційної безпеки пов'язані з використанням ШІ в інформаційній війні, актуалізують необхідність розробки нових підходів до захисту інформаційного простору. Це вимагає не тільки технологічних інновацій, але й політичної волі та міжнародної співпраці для створення ефективних механізмів протидії дезінформації та захисту демократичних цінностей.

Потрібно зауважити, що національні стратегії зазначених країн все більше орієнтуються на використання ШІ для досягнення військової переваги, що як наслідок, створює нові загрози для міжнародної стабільності та безпеки. Одним з основних викликів, на думку дослідників, є зростаюча автоматизація військових процесів, оскільки ШІ дозволяє автоматизацію ухвалення рішень, що може призвести до виникнення конфліктів через помилки систем або через зловмисне втручання в роботу системи. Прикладом цього є ситуації, коли рішення про застосування зброї ухвалюється автоматично, знижується можливість людського контролю та аналізу, що вагомо підвищує ризик непередбачуваних наслідків. Ще одним важливим аспектом часто згадують використання ШІ для кібератак та інформаційних війн. Серйозною загрозою стає здатність систем на основі ШІ виявляти слабкі місця та використовувати їх для отримання доступу до критичної інфраструктури держави та приватних установ. Крім того, нейромережі можуть бути використані для

створення і поширення неправдивої інформації, яка буде підривати довіру і призведе до політичної дестабілізації [2, с. 6, 8].

Погодимося з науковою думкою, що особливу увагу варто звернути на асиметричний характер загроз, які виникають в результаті розвитку ШІ. Менш потужні у військовій сфері держави чи недержавні актори можуть використовувати ці технології для створення суттєвих загроз глобальній безпеці, навіть не володіючи при цьому традиційними військовими ресурсами. Ефективно подолати ці виклики може координація на міжнародному рівні. Державам потрібно активно співпрацювати у розробці нормативно-правових актів, які б могли регулювати використання ШІ у військовій галузі, а також забезпечували прозорість і підзвітність у цій галузі. Це і створення міжнародних угод про контроль за озброєнням, що базується на ШІ, і розробка механізмів для запобігання ескалації конфліктів через автоматизовані інформаційні системи [2, с. 12, 15].

Сучасні виклики глобальної інформаційної безпеки є наслідком стрімкого розвитку технологій і їхнього проникнення в усі сфери життя. Враховуючи ці наслідки науковці додатково звертають увагу на такі нові рівні розвитку загроз як інформаційні атаки, дезінформація, Internet of things. Інформаційні атаки, що спрямовані на порушення конфіденційності, цілісності або доступності даних, стають все складнішими та різноманітнішими, що підвищує загальний рівень небезпеки для держав, компаній, окремих громадян. Серед основних викликів є зростання кіберзлочинності, зокрема хакери використовують все новіші методи, такі як фішинг, соціальна інженерія, програми-вимагачі, щоб мати доступ до конфіденційної інформації або зламати комп'ютерні системи. Такі атаки можуть завдати значної шкоди, фінансовій, репутаційній складовій. Особливо варто зважати на критичну інфраструктуру (енергетика, транспорт, сфера охорони здоров'я, тощо). Використання ШІ дозволяє злочинцям проводити атаки ще ефективніше, частіше, з більшим масштабом, що ускладнює можливість їх виявлення та нейтралізації [3].

Звертаючи увагу на характер сучасної дезінформації потрібно зауважити, що для багатьох людей соціальні мережі та інтернет-ресурси стали основним джерелом новин, тож поширення неправдивої інформації може призвести до серйозних наслідків, таких як нестабільність, економічні кризи, суспільні конфлікти. Нерідко дезінформація використовується як інструмент гібридної війни, тобто у боротьбі за вплив над думкою суспільства та маніпулювання поведінкою великих груп людей. В умовах глобалізації та цифровізації, важко контролювати потоки інформації та забезпечувати її достовірність, що робить дезінформацію одним із найнебезпечніших викликів глобальної інформаційної безпеки [3].

Важливо згадати і про розвиток Internet of things (IoT), який створює нові виклики для глобальної інформаційної безпеки. Йдеться про підключення до інтернету все більшої кількості пристроїв, включно з домашніми побутовими приладами, автомобілями, медичними пристроями, що відкриває нові вразливості для кібератак. Часто недостатній рівень захисту таких приладів може призвести до масових зламів і вагомих втрат, як матеріальних, так і людських. Відкритий доступ до систем керування інфраструктурою або персональних даних користувачів ставить під загрозу не тільки приватне життя, але й національну безпеку. Відтак є велика потреба зосередитись на захисті персональних даних у цифрову епоху. Сьогодні великі корпорації збирають величезні обсяги інформації про користувачів для комерційних цілей, тож виникає ризик неправомірного використання цієї інформації, її викрадення чи витоку. Це ставить гостре питання щодо захисту приватності та необхідності розробки нових законодавчих норм як на міжнародному так і національному рівні, що будуть направлені на регулювання обробки та зберігання персональних даних, забезпечуючи високий рівень захисту та відповідальності [3].

Буде справедливо відзначити, що у західних дослідженнях інформаційної безпеки вже тривалий час сформульоване фундаментальне питання: «Які ризики для яких критичних інфраструктур формує кіберпростір?». Це питання схоже до тих, що постають у дискусіях про роль стримування в нових умовах міжнародної безпеки. Якщо раніше стратегічне стримування було пов'язане переважно з ядерними загрозами, то сьогодні додається набуття загрози в кіберпросторі. Подібно до думок про стримування, питання про оцінку ризиків інформаційної безпеки часто набуває абстрактного характеру, коли окремі експерти безпідставно стверджують, нібито противник не наважиться чинити кібератаку глобального масштабу. Разом з тим, основуючись на різних аналітичних розробках, все ж багато вчених сходяться на думці, що оцінка ризиків інформаційної безпеки має бути зосереджена на тому, як нові загрози в кіберпросторі можуть підірвати чи зруйнувати здатність держав виконувати ключові елементи своєї національної стратегії, зокрема в умовах масштабної військової конфронтації. Це і дослідження того, як нові технології та методи інформаційної війни можуть використовуватися для атак на елементи національної інфраструктури та оборонної стратегії. Важливо враховувати, що глобальна інформаційна безпека потребує оцінки ризиків у різних сферах операцій – від національних кіберінфраструктур до міжнародних комунікаційних ліній і партнерських держав. У кожному з цих аспектів є власні унікальні вразливості, які вимагають спеціалізованих підходів до оцінки ризиків. Але, проведення достовірної міждержавної оцінки ризиків інформаційної безпеки ускладнено тим, що загрози та цілі часто перетинають традиційні кордони між національною безпекою, правозастосуванням і співпрацею між урядами. Тому вагомості набуває розроблення ефективних механізмів співпраці між державами, які б включали аспекти військової, цивільної та інформаційної безпеки. Існує потреба у створенні централізованого підходу до оцінки ризиків, де керівна роль могла б бути покладена на міжнародні організації чи спеціальні національні агенції, такі як ради національної безпеки або урядові комітети з кібербезпеки. Втім така інституціоналізація потребує потужних фінансових і політичних ресурсів [4, с. 35-36].

Також потрібно зауважити, що виклики інформаційної безпеки дедалі більше пов’язані з ескалацією інформаційної війни, про що ми зазначали на початку статті, та яку все більше у сучасних наукових та аналітичних джерелах пов’язують з діяльністю державних структур РФ, оскільки це той приклад, що виходить за межі традиційного розуміння війни та охоплює широкий спектр підривних дій, спрямованих на дестабілізацію демократичних інститутів і руйнування соціальної згуртованості в західних суспільствах. Втручання Росії в виборчий процес у США 2016-го року стало однією з перших масштабних демонстрацій використання інформаційної війни для досягнення поставлених політичних цілей без необхідності прямого воєнного конфлікту. Для недемократичних режимів, на відміну від західних держав, використання дезінформації, обману та психологічного впливу не лише є допустимим, але й вважається необхідним для досягнення стратегічних цілей як у мирний час, так і під час війни. Як приклад нерідко наводять російську концепцію маскування (Maskirovka), що бере свій початок з радянської доктрини, підкреслює використання обману, маніпуляції та дезінформації в усіх сферах життя і політики. Це не просто тактичний інструмент, а частина ширшої стратегії, спрямованої на підпорядкування волі противника власним інтересам. Тож інформаційна війна розглядається на рівні з традиційними збройними силами і навіть ядерною зброєю, що робить її ключовим елементом російської військової доктрини [5, с. 56-58]. Разом з тим, приклад Китаю у зв’язку з глобальною інформаційною безпекою науковці зазначають не стільки в контексті поняття інформаційної війни, скільки зміни пріоритетів впливу через прискорені темпи використання сучасних

інформаційних технологій. Наприклад, протягом Холодної війни Близький Схід не був серед пріоритетних інтересів для Китаю, однак з ростом енергетичних потреб набув більшої ваги. Незважаючи на те, що Китай відносно новий гравець у цьому регіоні, порівняно з США та Росією, він став одним з найбільших торгових партнерів та інвесторів на Близькому Сході. Китай активно постачає сучасні технології, зокрема в галузі спостереження і продажу зброї, що має вагомий вплив на бізнес. Інтереси Китаю в регіоні класифікують: дипломатичні, економічні, військові. Скорочення американського впливу в регіоні сприяло намаганню Китаю та Росії витіснити домінування США. Зауважимо, Китай і США є близькими суперниками по розробці ШІ. Відмітимо, Китай заявив про намір стати лідером у цій технології до 2030 року, виділивши 30 мільярдів доларів. І хоч США витрачають близько 4,4 мільярда доларів на ШІ, прогнозується, що китайські дослідники скоро перевершать американських не тільки за бюджетом, а й за кількістю публікацій. До прикладу, щоб посилити свою роль Китай встановив відносини з різними країнами Близького Сходу за допомогою технологічних досягнень в сфері зброї та енергетики. За даними SIPRI, експорт «розумної зброї» з Китаю до Саудівської Аравії та Об'єднаних Арабських Еміратів зріс на 365% і 169% відповідно між 2016 і 2020 роками порівняно з 2011–2015 роками. Зазначимо, як наслідок, це підвищує ризики виникнення гонки озброєнь на основі ШІ [6, с. 106-107].

Звернемо та акцентуємо увагу, Україна в умовах гібридної війни стикається з потужними інформаційними загрозами. Погодимося з науковцями, які зауважують на політико-правовому вимірі питання. Зазначимо, стратегія національної безпеки України визначає ключові загрози в цій сфері (інформаційно-психологічна війна, приниження української мови і культури, фальсифікація української історії, формування російською пропагандою викривленої інформаційної картини світу тощо). Протидіяти цим загрозам пропонується через наступальні дії проти всіх форм інформаційної агресії, створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидію маніпуляціям суспільною свідомістю та поширенню спотвореної інформації, а також захист національних цінностей та зміцнення єдності суспільства. Також, важливе значення має координація інформаційної політики органів державної влади та виявлення і нейтралізація суб'єктів (агентів впливу), яких використовують для ведення інформаційної війни проти України. Доктрина інформаційної безпеки України також підкреслює важливість захисту від агресивного впливу деструктивної пропаганди, зокрема з боку РФ, яка спрямована на розпалювання національної та релігійної ворожнечі, порушення суверенітету і територіальної цілісності України. Слушно провадити моніторинг медіа та Інтернет-ресурсів, виявлення загроз національним інтересам, координацію діяльності державних органів у сфері інформаційної безпеки, розробку стратегічних наративів та їх введення. Попри низку здобутків у цих стратегічних питаннях, погодимося, що необхідність подальшого вдосконалення нормативно-правової бази для ефективного реагування на загрози глобальній інформаційній безпеці є очевидною [7, с. 263-264].

Україна водночас вимушено випробовує на собі усі найактуальніші інформаційні виклики. Як слушно зауважують вітчизняні дослідники, однією з найбільших проблем сучасної інформаційної безпеки є постійна еволюція загроз. Раніше основною формою кіберзагроз були віруси та хакерські атаки, спрямовані на отримання доступу до конфіденційних даних. Сьогодні спектр загроз значно розширився, у арсеналі злочинців кіберзброя, кібершпигунство, а також складні гібридні загрози, які поєднують традиційні та цифрові методи впливу. Російська агресія проти України є прикладом того, як інформаційні загрози можуть використовуватися для дестабілізації держав та цілих регіонів. У цьому контексті Україна стикається з різноманітними викликами, серед яких кібератаки на критичну

інфраструктуру, дезінформаційні кампанії, спрямовані на підрив довіри до уряду, політиків та поширення хаосу, а також спроби маніпулювання думкою суспільства як всередині країни, так і на міжнародному рівні. Кібератаки несуть за собою катастрофічні наслідки для державної та економічної системи. Напади на енергетичні мережі, фінансові інститути та комунікаційні системи можуть паралізувати країну, завдаючи значної шкоди економіці, створюючи паніку серед населення. Дезінформаційні кампанії стають потужним інструментом у руках держав, що прагнуть вплинути на політичну ситуацію всередині інших країн. В ситуації з Україною подібні атаки та кампанії здійснювалися неодноразово, і продовжують залишатися однією з головних загроз національній безпеці, спрямовані на дискредитацію уряду, підрив міжнародної підтримки та створення серед населення відчуття безнадії й страху [8, с. 65-67].

Висновки та перспективи подальших досліджень. Сучасні виклики глобальної інформаційної безпеки вимагають від держав та міжнародної спільноти рішучих дій та тіснішої співпраці. Це як розробка та впровадження нових технологій захисту, так і розвиток ефективних стратегій протидії дезінформації. Важливу роль відіграє освіта та підготовка фахівців у галузі кібербезпеки, тісна співпраця між державним і приватним секторами.

У висвітленні ключових глобальних аспектів і сучасних викликів у сфері інформаційної безпеки, варто підкреслити, що кіберзлочинність продовжує еволюціонувати, ставлячи нові вимоги до захисту інформаційних систем. Сучасні загрози, такі як атаки на критичну інфраструктуру, фітинг, зловмисне програмне забезпечення, стають все більш складними і небезпечними, що вимагає постійного вдосконалення методів захисту. ШІ відіграє подвійну роль у кібербезпеці: з одного боку, він сприяє розвитку нових загроз, з іншого – відкриває нові можливості для захисту. Машинне навчання та інші технології ШІ можуть суттєво підвищити ефективність виявлення аномалій і автоматизації процесів реагування на непередбачування ситуації та конфлікти. Однак, ШІ може бути застосоване зловмисники для створення більш адаптивних і складних атак, що підкреслює важливість постійного вдосконалення технологій захисту. Отже, ми можемо ґрунтовно зазначити на необхідності комплексного підходу до забезпечення глобальної інформаційної безпеки, що включає технічні інновації, організаційні, політико-правові стратегії та активний моніторинг нових загроз. Також, важливим аспектом є міжнародна співпраця та обмін інформацією для ефективної боротьби з кіберзлочинністю, інформаційними війнами, антигуманною пропагандою тощо. Тому, дуже важливо проведення наукових досліджень та напрацювання нових концептуальних моделей, які б враховували зауважені аспекти забезпечили системний підхід та надійний захист від сучасних загроз в постійно мінливому інформаційному просторі.

Список використаної літератури

1. Пахота Н. В. Інформаційні війни в сучасних міжнародних відносинах. *Бізнес Інформ.* 2022. Вип. 1, № 528. С. 53–58. https://doi.org/10.32983/2222-4459-2022-1-53-58.
2. Hunter L., Albert C., Henningan C., Rutland J. The military application of artificial intelligence technology in the United States, China, and Russia and the implications for global security. *Defense & Security Analysis.* 2023. 39(2). P. 207–232. https://doi.org/10.1080/14751798.2023.2210367.
3. Johnson J. Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*. 2019. 35(2). P. 147–169. https://doi.org/10.1080/14751798.2019.1600800.
4. Molander R. C., Riddile A. S., Wilson P. A. Strategic information warfare: a new face of war. Parameters. 1996. 26(3). https://doi.org/10.55540/0031-1723.1794

5. Bryczek-Wróbel P., Moszczyński M. The evolution of the concept of information warfare in the modern information society of the post-truth era. *Przegląd nauk o obronności.* 2022. No. 13. P. 48–62. https://doi.org/10.37055/pno/152620.
6. Sarkin J., Sotoudehfar S. Artificial intelligence and arms races in the Middle East: the evolution of technology and its implications for regional and international security. *Defense & Security Analysis.* 2024. 40(1). P. 97–119. https://doi.org/10.1080/14751798.2024.2302699.
7. Трофименко А. Протидія російській інформаційній агресії в Україні: правовий вимір. *Вісник Маріупольського державного університету. Серія: Історія. Політологія.* 2020. Вип. 10, № 28-29. С. 261–270. https://doi.org/10.34079/2226-2830-2020-10-28-29-261-270
8. Галіпчак В. Д. Сучасні виклики та стратегії забезпечення інформаційної безпеки в Україні в умовах російської агресії: перспективи та завдання. *Науковий журнал «країнознавство».* 2023. № 35. С. 65–69. https://doi.org/10.32782/2663-6170/2023.35.10.

MODERN CHALLENGES OF GLOBAL INFORMATION SECURITY

Oleksii Buriachenko
National Aviation University, Faculty of International Relations,
Department of International Relations and Strategic Studies
Liubomyra Huzara Ave, 1, 03058, Kyiv, Ukraine

The article discusses key aspects of global information security in the context of current threats and challenges. The main focus is on the challenges faced by states, organisations and individual actors in the context of rapid development of technologies, in particular the cyber sphere. The author researched and analysed the main trends affecting information security, including the evolution of attacks, new vulnerabilities and changes in the tactics of hackers and intruders. The author also provides a detailed analysis of modern cyber threats, such as attacks on critical infrastructure, phishing, virus software, disinformation and other types of malicious activity. The author analyses the technical and organisational measures that need to be taken to ensure a high level of cyber defence. The author emphasises the need for a comprehensive approach to cybersecurity, including both technical and organisational measures, as well as the importance of continuous monitoring and adaptation to new challenges. The article pays special attention to the impact of artificial intelligence (AI) on the security sector and notes that AI can be used both to create new types of attacks and to develop innovative security methods.

The author thoroughly notes the need for a comprehensive approach to international security in the context of global information security, including technical innovations, organisational, political and legal strategies, and monitoring of new threats. He also highlights international cooperation and information exchange as an important aspect of effective counteraction to cybercrime, information warfare, inhumane propaganda, etc. The author emphasises the importance of conducting research and developing new conceptual models that would take into account all aspects of information security and provide a systematic approach and reliable protection against modern threats in the ever-changing information space.

Key words: global information security, international security, information warfare, cyberattacks, cybersecurity, disinformation, artificial intelligence (AI).