Вісник Львівського університету. Серія філос.-політолог. студії. 2024. Випуск 52, с. 317–326
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 52, p. 317–326

УДК 327.7:316.77-049.5](4)
DOI https://doi.org/10.30970/PPS.2024.52.40

МЮНХЕНСЬКІ КОНФЕРЕНЦІЇ З БЕЗПЕКИ: МІСЦЕ ІНФОРМАЦІЙНОГО ФАКТОРУ

Микита Білоусов
Чорноморський національний університет імені Петра Могили,
факультет політичних наук, кафедра міжнародних відносин та зовнішньої політики
вул. 68 Десантників, 10, 54000, м. Миколаїв, Україна

У науковій статті досліджено місце інформаційного фактору під час проведення Мюнхенських конференцій з безпеки (МКБ) протягом 2014–2024 рр.

Автор зауважує, що головною темою МКБ є обговорення та обмін думками щодо розвитку трансатлантичних відносин, а також європейської та глобальної безпеки у XXI столітті. МКБ опікуються не тільки різними рівнями безпеки (європейський, глобальний), але й охоплюють різні сфери безпеки, від таких традиційних як військова безпека, до найбільш актуальних на сьогодні: інформаційну, економічну, екологічну сфери безпеки.

Особливий акцент зроблений на МКБ періоду російсько-української війни 2014–2024 рр. з метою висвітлення актуальних загроз в інформаційній сфері, породжених гібридною війною РФ. У сучасних реаліях російсько-українська війна слугує яскравою демонстрацією і підтвердженням того, що кіберпростір відіграватиме вирішальну роль у майбутніх конфліктах і, що демократії мають об'єднатися, щоб вчасно реагувати на трансформацію війни.

Автор зазначає, що під час МКБ 2023–2024 рр. наголос був зроблений на посиленні співпраці шляхом спільного встановлення стандартів у сфері технологій і кібербезпеки, особливо між ЄС і США, а також на незмінній відданості демократичному та надійному інформаційному середовищу. Надзвичайно важливим став Круглий стіл з кібербезпеки та регулювання технологій у вересні 2023 р. на якому учасники обговорили нещодавні ініціативи ЄС щодо регулювання технологій, їхній вплив на кібербезпеку та можливості для трансатлантичної співпраці в цій сфері.

Автор приходить до висновку, що в умовах зростаючої загрози, породженої гібридною війною РФ, основним завданням є зміцнення європейського цифрового суверенітету. Задля досягнення цієї мети світова спільнота повинна звернути увагу на розробку стимулів для створення та розширення інноваційних компаній у сфері інформаційної безпеки.

Ключові слова: Мюнхенська конференція з безпеки, інформаційна безпека, кібербезпека, Україна, РФ, ЄС.

Постановка проблеми. Слід зазначити, що Мюнхенські конференції з безпеки (далі – МКБ) є провідним світовим форумом для обговорення політики міжнародної безпеки та місцем для дипломатичних ініціатив щодо вирішення найгостріших світових проблем безпеки. МКБ має трансатлантичне та європейське коріння, але сьогодні її діяльність спрямована на весь глобалізований світ. МКБ опікуються не тільки різними рівнями безпеки (європейський, глобальний), але й охоплюють різні сфери безпеки, від таких традиційних як військова безпека, до найбільш актуальних на сьогодні: інформаційну, економічну, екологічну сфери безпеки [5]. МКБ проводиться починаючи з 1963 р. в м. Мюнхен (Німеччина). Але у другій половині XX ст. Конференція мала інші назви: Конференція з військових питань і Мюнхенська конференція з політики безпеки. До 1998 р. засновником і керівником Конференції був німецький

видавець Евальд-Генріх фон Клейст-Шменцин. У 1999 р. цю роль виконував Хорст Тельчик – колишній радник канцлера Німеччини Гельмута Коля за зовнішніми та оборонними питаннями. У 2009 р. керівництво взяв на себе Вольфганг Ішингер, а в 2022 р. – Крістоф Хойсген. Організатором МКБ є некомерційна організація – Фонд МКБ. У МКБ беруть участь високопоставлені політики, дипломати, військові експерти та експерти з безпеки з країн-членів НАТО та ЄС, а також з інших країн, таких як Китай, Індія, Іран, Японія та Росія [17].

Нагадаємо, що 2007 р. став роком проведення МКБ, на якій Президент РФ В. В. Путін виступив з промовою, в якій звинуватив США у створенні однополярного світу, «в якому один господар, один суверен», що на Заході розцінювалося як відновлення холодної війни [28].

Через кілька тижнів у квітні 2007 р. Росія здійснила серію кібератак на Естонію; після чого вторглася в Грузію у 2008 р.; анексувала Крим у 2014 р., спровокувавши конфлікт на сході України, підтримала російських сепаратистів у Донецькій і Луганській областях України, а 24 лютого 2022 р. здійснила повномасштабне вторгнення в Україну. Паралельно росіяни потужно використовували інформаційний фактор: кампанії дезінформації, пропаганду, фейкові події, аби забезпечити підтримку своїм діям як в середині Росії, так і в країнах Європи, і, в межах України. Поряд з цим Президент РФ В. В. Путін жорстоко придушував опозицію на території Росії, яка була причетна до дезінформаційних кампаній, кібератак та втручань у вибори на теренах європейських держав. Сьогодні російсько-українська війна слугує яскравою демонстрацією і підтвердженням того, що кіберпростір відіграватиме вирішальну роль у майбутніх конфліктах і що демократії мають об'єднатися, щоб вчасно реагувати на трансформацію війни.

Актуальність обраної проблематики підтверджує і той факт, що війна Росії проти України створила нові загрози всій європейській системі безпеки, в результаті чого треба повністю переосмислити порядок безпеки в Європі. Це вимагатиме підготовки нових принципів і норм функціонування системи безпеки, реформування інституцій, а також переосмислення всього європейського оборонного інструменту в світлі нових або раніше невиявлених загроз, особливо у сфері інформаційної безпеки країн ЄС.

Мета наукової статті полягає в здійсненні аналізу МКБ 2014–2024 рр. та висвітленні місця останніх для європейської інформаційної безпеки.

Необхідно відмітити, що обрана проблематика майже не висвітлена у працях українських дослідників, що ще більше підсилює актуальність обраного дослідження. Під час написання статті автор використовував напрацювання зарубіжних науковців, зокрема: А. Класена [6], С. Гормана, Н. Хадсона, М. Роджерса [11], М. Хьюза [12], А. Мартіна [13], Г. Пілайя [21], К. Фолла [24]. Вказані дослідники висвітлюють саме місце інформаційного фактору в МКБ. Серед українських дослідників, які звертали увагу на Мюнхенські конференції загалом слід згадати такі прізвища: А. Лазарева [1], А. Л. Помаза-Пономаренко [2], І. Січень [3], М. В. Толстов і М. В. Фесенко [4].

Виклад основного матеріалу дослідження. Станом на 2024 р. відбулося 60 МКБ, але автор статті вважає за доцільне більш детально розглянути конференції, які проходили саме у розрізі російсько-української війни, яка почалася ще у 2014 р. і продемонструвати, яке значення вони мали для європейської інформаційної безпеки. Однак, «килимове бомбардування» суспільно-політичної думки – через соціальні медіа, впливових осіб, неурядові організації, аналітичні центри та політичні партії – триває вже понад 15 років, починаючи принаймні ще з пам'ятної Мюнхенської конференції в лютому 2007 р., коли В. В. Путін виголосив промову, в якій остаточно заперечував європейський порядок безпеки. Під час свого виступу Президент РФ В. В. Путін висловлював тези, які не відповідають дійсності, а значить займався дезінформаційною кампанією проти західного світу [28].

Варто зазначити, що починаючи з 2014 р., зусилля Росії щодо гібридної війни призвели до того, що міжнародне співтовариство не бажало визнавати глобальний характер конфлікту та очевидні загрози статус-кво світового порядку. Навпаки, протягом багатьох років можна було спостерігати наполегливі спроби кваліфікувати бойові дії як локальну чи навіть громадянську війну. Лише у лютому 2022 р., коли Росія розпочала повномасштабне вторгнення в Україну, подвійні стандарти стали очевидними [23].

Нагадаємо, що 50-та МКБ, яка відбувалася з 31 січня по 2 лютого 2014 р. була присвячена обговоренню трьох основних проблемних питань: 1) політична криза в Україні; 2) загрози європейській безпеці; 3) ядерна програма Ірану. Під час обговорення першого питання Держсекретар США Джон Керрі пообіцяв підтримати українську опозицію, а міністр закордонних справ Росії Сергій Лавров у свою чергу звинуватив країни Заходу у сприянні насильницьким зіткненням в Україні, яке вийшло з-під контролю [25]. Верховний представник ЄС із закордонних справ та політики безпеки Кетрін Ештон виступила з посередницькою ініціативою, запросивши до участі представників українських сторін конфлікту та європейських міністрів закордонних справ [22].

На 51-й МКБ, яка проходила 6-8 лютого 2015 р. порушувалися питання війни на Донбасі і незаконної анексії Криму Росією. Зокрема, Міністр оборони Німеччини Урсула фон дер Ляйєн звинуватила Росію в агресії до України, але висловилася проти постачання озброєння в Україну [14].

Під час 52-ї МКБ, яка проходила з 12 по 14 лютого 2016 р. нідерландський політик і депутат Європейського парламенту Маріетте Шааке виступила модератором круглого столу Європейського ліберального форуму «Дует цифрової безпеки: підвищення стійкості європейського кіберзахисту за допомогою публічно-приватного партнерства». Учасники круглого столу прийшли до висновку, що кібербезпека займає важливе місце в порядку денному урядів, Європейської комісії та цифрової індустрії. Тому безсумнівно, що уряди та приватний сектор повинні співпрацювати, щоб захистити життєво важливу інфраструктуру [29].

24 і 25 листопада 2019 р. 55-та МКБ провела Саміт з кібербезпеки у Берліні. Дискусії стосувалися глобальної конкуренції за інформаційні технології, стійкості до кібератак і дезінформації, а також геополітичних аспектів управління Інтернетом. Основні проблеми, які обговорювалися на саміті: стримування та захист від кібервтручання у вибори; боротьба з поширенням дезінформації та екстремізму в Інтернеті; підтримання свободи та відкритості Інтернету; і зростаюча геополітична роль технологічних компаній, зокрема у забезпеченні інфраструктури 5G. Учасники саміту прийшли до висновку, що без взаємної довіри між урядами, компаніями та громадянами щодо безпеки технологій і кіберпростору спільний прогрес знаходиться під загрозою [30].

Знаковою подією стала 58 МКБ, яка відбулася з 18 по 20 лютого 2022 р. під девізом «Переломити ситуацію – позбутися безпорадності», що зібрала понад 30 глав держав, 100 міністрів та керівників багатьох найважливіших міжнародних організацій, таких як ЄС, НАТО та ООН. Генеральний секретар ООН Антоніу Гутерріш зазначив, що світ перебуває у більш нестабільній безпековій ситуації, ніж під час холодної війни. Віце-президент США Камала Гарріс також заявила, що США готові вдарити по Москві жорсткими санкціями у разі нападу [18].

Про значення інформаційного фактору в російсько-українській війні зазначила під час свого виступу на МКБ у 2022 р. Президент Єврокомісії Урсула фон дер Ляєн: «Ось уже сім років російське керівництво намагається дестабілізувати Україну шляхом гібридної війни, кібератак та дезінформації. Але зараз країна сильніша, ніж сім років тому. Бо

вона обрала шлях демократії та дружби інших демократій. … Процвітаючі демократії – найбільший страх для автократів, оскільки їх пропаганда зазнає поразки, коли громадяни отримують силу завдяки повідомленням незалежних ЗМІ та вільному обміну ідеями. Бо вільні громадяни говорять правду владі. Тому що довіра і впевненість є більш стійкими, ніж контроль і примус. І саме тому Європа підтримує шлях України до демократії. Це робить Україну кращим місцем для життя її людей і кращим сусідом як для ЄС, так і для Росії» [27]. Така промова Президента Єврокомісії свідчить про те, що вона не звертає уваги на інформаційну кампанію В. В. Путіна проти України, яка відкрито розпочалася на європейських теренах у 2007 р. на такій самій конференції з безпеки.

Росія не була присутня на конференції 2022 р., тоді як Президент України Володимир Зеленський попередив західні країни, що вони повинні відмовитися від політики умиротворення щодо Москви, і передбачив російський наступ, який мав відбутися лише через п'ять днів [31].

Слід зазначити, що у наш час зв'язок між геополітикою та кібербезпекою стрімко посилюється. Україна довгий час служила полігоном для кіберактивності Росії. За останнє десятиліття Росія здійснила низку нападів на Україну в тому числі і в кіберпросторі, як проти українського уряду, так і приватного сектору. Ці атаки стають все більш витонченими. Коли почалося російське вторгнення, існувало очікування, що кібервійна зіграє головну роль у конфлікті. Примітно, але масштабних російських атак на українську комунікаційну інфраструктуру досі не було. Однак російська довгострокова стратегія інформаційної війни за допомогою кіберзасобів відіграла важливу роль не лише після вторгнення до України, але й за її межами [15].

Під час МКБ у лютому 2023 р. наголос був зроблений на посиленні співпраці шляхом спільного встановлення стандартів у сфері технологій і кібербезпеки, особливо між ЄС і США, а також на незмінній відданості демократичному та надійному інформаційному середовищу. У центрі уваги опинилося європейське технологічне регулювання, включно із Законом про цифрові послуги та цифрові ринки, які спрямовані на створення безпечнішого цифрового простору, захист фундаментальних прав користувачів, виявлення та ліквідацію гейткіперів та вирівнювання умов для бізнесу. На цьому заході обговорювалася роль українських контрстратегій у розвитку стійкості проти кібератак Росії та роль іноземної допомоги [24].

6 вересня 2023 р. МКБ організувала Круглий стіл з кібербезпеки та регулювання технологій у Представництві Баварії при ЄС в Брюсселі. Під час двох сесій учасники обговорили нещодавні ініціативи ЄС щодо регулювання технологій, їхній вплив на кібербезпеку та можливості для трансатлантичної співпраці в цій сфері. Перша дискусія, яка була зосереджена на кібербезпеці, почалася зі встановлення труднощів регулювання та захисту кібердомену. *Підсумки першої сесії Круглого столу з кібербезпеки та регулювання технологій:*

1. Повсюдність кіберризиків і відповідні вразливості вимагають від демократій дій. Оскільки всі аспекти життя та політики стають все більш цифровими, то найбільший ризик безпеці завжди походить від найслабшої ланки (чи то люди в корпорації чи одна єдина крихітна частина військового обладнання, яка підключена до всіх інших і, яка стає вектором для здійснення атаки).

2. Загрози можуть надходити як у межах національних кордонів, так і за їх межами, і очевидною є менша різниця між атаками під час війни та мирного часу. Раптове зростання кількості зловмисних програм і кібератак, що підтримуються штучним інтелектом, загострило і так складну картину загроз.

3. Учасники підкреслили вирішальну роль технологічної освіти для підвищення стійкості населення в цілому.

4. З метою зміцнення трансатлантичних демократій проти супротивників, учасники закликали до кращої координації між ЄС і НАТО. Ці дві інституції можуть доповнювати одна одну в технологічній сфері, оскільки НАТО вносить перспективу військової безпеки в питання, пов'язані з технологіями, а ЄС має законодавчі повноваження для впровадження законів, які борються з цими загрозами безпеці. Слід зазначити, що в останній Стратегії безпеки НАТО також наголошено на співпраці з ЄС як раз в сфері інформаційної безпеки [20].

5. Висунута ідея створення посади головного офіцера з питань безпеки в ЄС, щоб забезпечити чітку відповідальність однієї особи, якій доручено інтегрувати питання безпеки та геополітичні міркування в усі зусилля ЄС.

6. Учасники закликали трансатлантичних партнерів, а особливо європейські країни, посилити свої координаційні зусилля в Європі та за її межами, більш відкрито ділитися розвідданими про кіберзагрози та інвестувати більше в персонал для ефективного впровадження правил [16].

Основними підсумками другої сесії Круглого столу з кібербезпеки та регулювання технологій стали:

1. Джоаннеке Бальфорт, директор політики безпеки та оборони Європейської служби зовнішніх дій, підкреслила, що між США та ЄС не повинно бути конкуренції у сфері безпеки, але що економічна конкуренція між ними є нормальною та навіть здоровою [10].

2. Учасники знову висловили свою критику щодо наслідків технічних правил ЄС для безпеки, таких як вимога повідомляти про вразливі місця в безпеці відповідно до Закону ЄС про кіберстійкість [7]. Кілька учасників також зазначили, що залишення технологічного сектора виключно на ринкову динаміку несе ризики для безпеки, адже приватний сектор, насамперед, має стимул до інновацій та отримання прибутку, а не ставить безпеку на перше місце.

3. Учасники погодилися з важливістю подальшого трансатлантичного співробітництва у сфері технологічного регулювання, але також визнали численні виклики, пов'язані з цим. Зокрема, був зроблений акцент на уроках, пов'язаних з інформаційними технологіями під час російської війни проти України. Відзначено, що українці демонструють неабиякий інноваційний дух у залученні до нових технологій на полі бою [10].

Не можливо не відмітити той факт, що протягом останнього десятиліття Мюнхенська конференція з кібербезпеки була ключовою платформою для сприяння глобальному діалогу щодо кіберзагроз. 16 травня 2024 р. Мюнхенська конференція з кібербезпеки зібрала найбільшу в історії делегацію кіберпрофесіоналів з усього корпоративного світу та громадянського суспільства. Провідним європейським компаніям важко зрозуміти з якими загрозами, породженими Росією, Китаєм, Іраном, Північною Кореєю, вони зіштовхуються та як захиститися від них. Компанії також не знають, як найкраще взаємодіяти з різними регулюючими органами, органами влади та агентствами національної безпеки, якщо їх атакує держава [11].

Кіберризики разом із кліматичними ризиками постійно займають високі позиції через їх системний характер. Відповідно до Мюнхенського індексу безпеки [19], передбачувана загроза кібератак зросла на п'ять позицій у порівнянні з 2023 р. Для прикладу, індекс також показав, що 74% респондентів Німеччини вважають кібератаки неминучим ризиком, що є найвищим показником серед усіх загроз. Згідно з Мюнхенським індексом безпеки 2024 р., кібератаки сприймаються як найбільша загроза в США. Це занепокоєння відображає глобальну тенденцію зростання страху перед кампаніями дезінформації та

негативними наслідками штучного інтелекту. У міру того як цифровий світ стає все більш взаємопов'язаним, потенціал для кібератак, які можуть завдати широкомасштабної шкоди, продовжує зростати [13].

Джон Доу, експерт з кібербезпеки, зазначає: «Кібератаки стають все більш витонченими, тому їх важко виявити. Для країн вкрай важливо інвестувати в заходи кібербезпеки та співпрацювати на міжнародному рівні для захисту від цих загроз» [21].

Професор Й. Мюллер-Куаде вважає загрозу кібератак, яку сприймають німецькі респонденти, реалістичною, водночас зазначивши, що багато компаній, особливо малі та середні підприємства, недостатньо підготовлені до кіберризиків [6].

Протягом 16–18 лютого 2024 р. проходила 60-та МКБ, на якій близько 60 глав держав і понад 85 урядовців обговорили найактуальніші проблеми безпеки у світі, включно з високопоставленими спікерами, такими як віце-президент США Камала Харріс і Президент України Володимир Зеленський. На зустрічі європейські лідери висловили свою відданість НАТО, заявивши, що зміцнення оборони ЄС є життєво важливим і що країни-члени повинні виділяти більше грошей для досягнення цієї мети. Голова конференції Крістоф Хойсген зазначив, що Європа «не може дозволити собі розкіш чекати більше, щоб організувати європейську оборону» [9].

Оскільки світові лідери, політики та експерти зібралися в Мюнхені, конференція стала платформою для обговорення та співпраці у вирішенні нагальних проблем, які визначають сучасний геополітичний ландшафт.

МКБ 2024 р. стала основою для критичних дискусій щодо двох найбільш постійних і нестабільних конфліктів у світі: російсько-української війни та триваючої напруженості між Газою та Ізраїлем, яка набула гарячої фази з жовтня 2023 р.. Також, головними темами, які опинилися у центрі дискусій стали інформаційні війни, які займають центральне місце в конфліктах у Європі та на Близькому Сході, а також потенційні шляхи їх розв'язання. Геополітичні зміни та інформаційна війна, як це спостерігається в Україні за останні кілька років, викликають побоювання щодо виборів. З огляду на те, що у 2024 р. очікуються вибори у 76 країнах, існує величезний потенціал для політичних кампаній маніпулювати соціальними алгоритмами.

Дві основні доповіді, які виголосив Алехандро Майоркас [26], міністр внутрішньої безпеки США, і Кріс Рей [8], директор ФБР, повторили важливість міцної позиції в галузі кібербезпеки. Поглиблена співпраця шляхом обміну дієвою інформацією про загрози в поєднанні з ретельнішим звітуванням про інциденти дозволить усім організаціям, які обізнані з безпекою, які цінують свою кібервідмовостійкість (а саме здатність системи забезпечувати прийнятний рівень обслуговування за наявності кіберризиків), бути на крок попереду ворогів [12].

На МКБ 2024 р. А. Майоркас запропонував створити новий кіберсоціальний договір – угоду між усіма членами цифрового суспільства про те, що спільні інтереси держав в інформаційній безпеці вимагають як регулювання, так і індивідуальної відповідальності, а також взаємного зобов'язання виконувати обидві вимоги [26].

К. Рей зазначив, що: «Сьогодні не тільки Китай, а й Росія, Іран і Північна Корея також сповнені рішучості використати кіберзасоби, щоб атакувати речі, які ми всі вважаємо святими – наші свободи, процвітання та демократичні норми» [8]. Для прикладу директор ФБР згадав про кібератаку 2022 р. спонсорованої Іраном групи на дитячу лікарню у США, яка продемонструвала безсердечне і мерзенне нехтування безпекою найбільш уразливих верств суспільства – дітей.

Також був зроблений акцент на тому, що Росія продовжує атакувати критично важливу інфраструктуру, включаючи підводні кабелі та промислові системи управління як

у США, так і в ЄС. Наприклад, після неспровокованого вторгнення в Україну Росія проводить розвідку в енергетичному секторі США. І це є тривожною тенденцією, бо як тільки доступ буде встановлено, хакер може перейти від збору інформації до швидкої атаки [8].

Але, нещодавнє опитування проведене в рамках Мюнхенського індексу безпеки виявило зміну суспільного сприйняття загроз безпеці. Зараз Китай і Росія вважаються такими ж загрозливими як і нетрадиційні ризики, зокрема масова міграція та радикальний іслам. Незважаючи на цю зміну, традиційні жорсткі ризики безпеки залишаються вищими, ніж протягом 2021–2023 рр. [21].

МКБ 2024 р. забезпечила ще одну важливу платформу для вирішення складних питань поточного геополітичного ландшафту. Конференція послужила каталізатором для міжнародної співпраці та розробки інноваційних рішень, починаючи від зміни динаміки влади та викликів епохи цифрових технологій, зміни клімату та сучасної глобальної кризи.

Висновки. Підсумовуючи, варто зазначити, що трансатлантична політика безпеки та європейська оборона є одними з ключових тем МКБ. МКБ стане важливим форумом для вирішення цих проблем і розробки стратегій захисту від потенційних загроз для країн ЄС. Оскільки громадське сприйняття загроз безпеці продовжує розвиватися, європейським політикам важливо враховувати ці зміни та відповідно адаптувати свої підходи. Слід зазначити, що інформаційному фактору до 2021 р. взагалі не приділяли уваги на МКБ, і тільки з 2022 р. відводиться особливе місце під час проведення МКБ.

Поряд з цим на МКБ протягом 2022–2024 рр. порушувалися питання щодо відновлення довіри в цифровому суспільстві, а також аналізувалися нові сценарії загроз для європейської інформаційної безпеки. Так, кіберзахист стає критично важливою основною навичкою для приватного бізнесу європейських країн.

Під час проведення МКБ 2022–2024 рр. європейські політики взяли на себе чіткі зобов'язання щодо зміцнення цифрового суверенітету Європи, особливо там, де залежності впливають на безпеку. Сьогодні існує потреба в рішучих діях, задля забезпечення цифрових можливостей Європи в майбутньому.

Автор вважає, що в умовах зростаючої загрози, породженої гібридною війною РФ, основним завданням є зміцнення європейського цифрового суверенітету, тобто звернення уваги на політику інформаційної безпеки ЄС. Для цього Європа має сильні сторони в деяких технологіях, але їй потрібно прискорити темп інновацій, комерціалізації та впровадження інших більш високих технологій. Європейські недоліки в основних можливостях цифрового суверенітету становлять ризики для трансатлантичної безпеки та спільного цифрового порядку денного. МКБ, в свою чергу, покликана розробити стратегії захисту від потенційних загроз. Щоб зміцнити європейський цифровий суверенітет, політики повинні звернути увагу на розробку стимулів для створення та розширення інноваційних компаній. Інструменти для цього добре розроблені й варіюються від конкурсів до цільових програм розвитку технологій. Сектор безпеки може виступати каталізатором інновацій через багатонаціональні та європейські програми безпеки.

Список використаної літератури

1. Лазарева А. Незгоди та суперечки: чому Мюнхенська безпекова конференція виявила чимало протиріч між провідними політичними гравцями світу. Український тиждень. 2020. № 8. С. 40–41.
2. Помаза-Пономаренко А. Л. 53 Мюнхенська безпекова конференція: нові акценти у забезпеченні соціальної безпеки та розвитку. Вісник Національного університету цивільного захисту України. Серія : Державне управління. 2017. Вип. 1. С. 42–48. URL: http://nbuv.gov.ua/UJRN/VNUCZUDU_2017_1_8 (дата звернення: 29.02.2024).

3. Січень І. Мюнхенська конференція з питань безпеки: висновки для України. Незалежний аналітичний центр геополітичних досліджень «Борисфен Інтел». 2024. URL: https://bintel.org.ua/analytics/myunhenska-konferenciya-z-pitan-bezpeki-visnovki-dlya-ukraini/ (дата звернення: 29.02.2024).
4. Толстов М.В., Фесенко М.В. Актуальні оцінки та підходи щодо світових процесів у контексті 59-ої Мюнхенської конференції з питань безпеки (17–19 лютого 2023 року). Державна установа «Інститут Всесвітньої історії НАН України». 2023. URL: https://ivinas.gov.ua/viina-rf-proty-ukrainy/aktualni-otsinky-ta-pidkhody-shchodo-svitovykh-protsesiv-u-konteksti-59oi-miunkhenskoi-konferentsii-z-pytan-bezpeky-1719-liutoho-2023-roku.html (дата звернення: 29.02.2024).
5. About the Munich Security Conference. 2024. URL: https://securityconference.org/en/about-us/about-the-msc/ (дата звернення: 23.02.2024).
6. Clasen A. Munich Security Report: Perceived threat of cyberattacks reaches all-time high. 2024. URL: https://www.euractiv.com/section/cybersecurity/news/munich-security-report-perceived-threat-of-cyberattacks-reaches-all-time-high/ (дата звернення: 23.02.2024).
7. Cyber Resilience Act. 2022. URL: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (дата звернення: 29.02.2024).
8. Director Wray's Remarks at the Munich Security Conference. 2024. URL: https://www.fbi.gov/news/speeches/director-wray-s-remarks-at-the-munich-security-conference (дата звернення: 24.02.2024).
9. EU must strengthen its defence: Munich Security Conference. 2024. URL: https://www.euronews.com/2024/02/19/eu-must-strengthen-its-defence-munich-security-conference (дата звернення: 23.02.2024).
10. EU-US Security Talks 2023: The United States, Europe, and Germany Adjusting for an Unknown Future. 2023. URL: https://brussels.fes.de/e/eu-us-security-talks-2023-the-united-states-europe-and-germany-adjusting-for-an-unknown-future (дата звернення: 29.02.2024).
11. Gorman S., Hudson N., Rogers M. Munich Cyber Security Conference 2024. URL: https://www.brunswickgroup.com/munich-cyber-security-conference-i26374/ (дата звернення: 23.02.2024).
12. Hughes M. Going Beyond the Cybersecurity Headlines from This Year's Munich Security Conference. 2024. URL: https://www.linkedin.com/pulse/going-beyond-cybersecurity-headlines-from-years-munich-mark-hughes-aouif?trk=public_post_main-feed-card_feed-article-content (дата звернення: 23.02.2024).
13. Martin A. The 'Munich Spirit': What to expect from this year's security conferences. 2024. URL: https://therecord.media/munich-security-and-cybersecurity-conference-2024-what-to-expect (дата звернення: 24.02.2024).
14. Munich Security Conference 2015. URL: https://securityconference.org/en/msc-2015/ (дата звернення: 29.02.2024).
15. Munich Security Conference 2023 List of Selected Side Events. 2023. URL: https://securityconference.org/assets/user_upload/MSC2023_ListOfSelectedSideEvents.pdf (дата звернення: 23.02.2024).
16. Munich Security Conference Brings Together Tech Experts and Policymakers in Brussels for a Roundtable on Cyber Security and Tech Regulation. 2023. URL: https://securityconference.org/en/news/full/munich-security-conference-brings-together-tech-experts-and-policymakers-in-brussels-for-a-roundtable-on-cyber-security-and-tech-regulation/ (дата звернення: 24.02.2024).
17. Munich Security Conference Foundation. 2024. URL: https://securityconference.org/en/munich-security-conference-foundation/ (дата звернення: 29.02.2024).

18. Munich Security Conference opens – without Russia. 2022. URL: https://www.dw.com/en/munich-security-conference-opens-without-russia/a-60827995 (дата звернення: 24.02.2024).
19. Munich Security Index. 2024. URL: https://securityconference.org/assets/01_Bilder_Inhalte/03_Medien/02_Publikationen/2024/MSR_2024/MunichSecurityIndex2024.pdf (дата звернення: 23.02.2024).
20. NATO 2022 Strategic Concept. 2022. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (дата звернення: 29.02.2024).
21. Pillai G. Global Security Threats: Shift in Public Perception and Rising Non-Traditional Risks. 2024. URL: https://bnnbreaking.com/world/global-security-threats-shift-in-public-perception-and-rising-non-traditional-risks (дата звернення: 24.02.2024).
22. Press release of 3312th Council meeting. 2014. URL: https://www.consilium.europa.eu/media/28335/142563.pdf (дата звернення: 29.02.2024).
23. Pyshnyy A. Global war and its manifestations. 2023. URL: https://voxukraine.org/en/global-war-and-its-manifestations
24. Rogers M., Fall K., Peter J. What to Expect From the 2023 Munich Security Conference. 2023. URL: https://www.brunswickgroup.com/what-to-expect-from-the-2023-munich-security-conference-i24031/ (дата звернення: 23.02.2024).
25. Russia's Sergei Lavrov: Ukraine getting 'out of control'. 2014. URL: https://www.bbc.com/news/world-europe-25823091 (дата звернення: 29.02.2024).
26. Secretary Mayorkas Delivers Keynote Remarks at Munich Cyber Security Conference. 2024. URL: https://www.dhs.gov/news/2024/02/16/secretary-mayorkas-delivers-keynote-remarks-munich-cyber-security-conference (дата звернення: 24.02.2024).
27. Speech by President von der Leyen at the Munich Security Conference. 2022. URL: https://ec.europa.eu/commission/presscorner/detail/es/speech_22_1221 (дата звернення: 24.02.2024).
28. The Speech In Which Putin Told Us Who He Was. 2022. URL: https://www.politico.com/news/magazine/2022/02/18/putin-speech-wake-up-call-post-cold-war-order-liberal-2007-00009918 (дата звернення: 29.02.2024).
29. The Munich Security Conference 2016. URL: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vk0jgec527ni?ctx=vhydm9r2w9p3&tab=1&start_tab1=15
30. MSC hosting Cyber Security Summit 2019 in Berlin. 2019. URL: https://securityconference.org/en/news/full/msc-hosting-cyber-security-summit-2019-in-berlin/
31. Zelensky's full speech at Munich Security Conference. 2022. URL: https://kyivindependent.com/zelenskys-full-speech-at-munich-security-conference/ (дата звернення: 24.02.2024).

THE MUNICH SECURITY CONFERENCES: PLACE OF INFORMATION FACTOR

Mykyta Bilousov
Petro Mohyla Black Sea National University,
Faculty of Political Sciences, Department of International Relations and Foreign Policy
68 Desantnykiv str., 10, 54000, Mykolaiv, Ukraine

The scientific article examines the place of the information factor during the Munich Security Conferences (MSC) which took place in 2014–2024.

The author notes that the main theme of the MSC is the discussion and exchange of views on the development of transatlantic relations, as well as European and global security in the twenty-first century. The MSC cares not only about different levels of security (European, global), but also covers different areas of security, from such traditional ones as military security, to the most relevant today: information, economic, environmental security areas.

Particular emphasis is placed on the MSC which took place during the Russian-Ukrainian war of 2014–2024 in order to highlight current threats in the information sphere generated by the hybrid war of the Russian Federation. In modern realities, the Russian-Ukrainian war serves as a clear demonstration and confirmation that cyberspace will play a decisive role in future conflicts and that democracies must unite to respond in time to the transformation of war.

The author notes that during the MSC which took place during 2023–2024 the emphasis was on enhancing cooperation through joint standard-setting in technology and cybersecurity, especially between the EU and the US, as well as a continued commitment to a democratic and trusted information environment. The Roundtable on Cybersecurity and Technology Regulation in September 2023 was extremely important. During this event, representatives from different countries discussed recent EU initiatives in terms of technology regulation, their impact on cybersecurity and opportunities for active transatlantic cooperation in this area.

The author comes to the conclusion that in the context of the growing threat generated by the hybrid war of the Russian Federation, the main task is to strengthen European digital sovereignty. To achieve this goal, the global community must pay attention to developing incentives for the creation and expansion of innovative companies in the field of information security.

Key words: the Munich Security Conference, information security, cybersecurity, Ukraine, Russian Federation, EU.