УДК 327
Сергій Федонюк,
кандидат географічних наук, доцент,
доцент кафедри міжнародних комунікацій та політичного аналізу,
Волинський національний університет імені Лесі Українки,
ORCID ID 0000-0003-2853-8905
sergii.fedoniuk@eenu.edu.ua
DOI 10.29038/2524-2679-2021-03-144-168

ПОЛІТИКА ЄС В АСПЕКТІ ОСНОВНИХ ГЛОБАЛЬНИХ КОНЦЕПЦІЙ ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ[1]

У статті встановлено особливості політики Європейського Союзу у сфері безпеки кіберпростору з погляду домінуючих підходів до політики інформаційної (кібер) безпеки.

Політику ЄС у сфері інформаційної безпеки та безпеки інфраструктури досліджено у взаємозв'язку з переважаючими сьогодні підходами, котрі демонструють головні стейкхолдери розвитку кіберпростору. Це дві концепції, які відрізняються здебільшого поглядами на управління інтернетом, національний суверенітет над кіберпростором і принциповою позицією щодо необхідності формування спеціального домена у сфері міжнародного права задля охоплення питань безпеки кіберпростору. Ключовими послідовниками й промоторами на світовій арені ідеї суверенного розпорядження ресурсами кіберпростору та управління інтернетом, а також формування спеціального правового режиму міжнародної інформаційної безпеки є Росія й Китай. Їм опонують США та низка демократичних країн Заходу.

У цьому дослідженні проведено аналіз основних стратегічних документів вторинного права Європейського Союзу у сфері інформаційної безпеки й безпеки мереж на предмет виявлення відповідності одному з підходів. Детальніше розглянуто «Стратегію кібербезпеки для цифрової декади», прийняту наприкінці 2020 р. і пов'язані з нею документи. Установлено близькість підходів Європейського Союзу до західної моделі інформаційної (кібер) безпеки, його активність щодо її просування у світі. Також ми розглянули ініціативи держав – членів Європейського Союзу – щодо

[1]Статтю підготовлено в межах проєкту «Студії ЄС у ВНУ імені Лесі Українки» програми Європейського Союзу ERASMUS+ напряму кафедри Жана Моне (№ 611478-EPP-1-2019-1-UA-EPPJMO-CHAIR).

активного впливу на перебіг процесів міжнародної співпраці у цій сфері, зокрема з урахуванням подій і тенденцій, пов'язаних із діяльністю провідних акторів на рівні ООН.

У підсумку можемо зробити висновок про все більш чітке оформлення політики ЄС у сфері інформаційної (кібер) безпеки та просування його конструктивної позиції з цього питання на світовій арені.

Ключові слова: *кібербезпека, міжнародна політика, Європейський Союз.*

1. ВСТУП

Постановка проблеми. Існують відмінності в концептуальних підходах у сфері політики інформаційної (кібер) безпеки серед головних світових акторів у цій сфері. США, Росія, Китай і країни Європи є головними стейкхолдерами кіберпростору, а також найбільш зацікавленими сторонами у виробленні вигідних їм умов діяльності. Якщо Росія, Китай та США активно реалізують і пропагують міжнародну політику в цьому напрямі, то Європейський Союз, відповідно до його цінностей і прагматичних інтересів, більше зосереджений на актуальних питаннях внутрішньої політики відповідно до галузевих та горизонтальних пріоритетів. Але розуміння відповідних тенденцій і перспектив важливе в аспекті стратегії ЄС і євроінтеграційних планів потенційних кандидатів на вступ до унії (наприклад України).

Загалом існують два різні підходи до державної політики у сфері інформаційної безпеки. Для першого (назвемо його «західним») властива відсутність прямого втручання у сферу кіберпростору й орієнтація на забезпечення безперебійного та адекватного функціонування його інфраструктури. Держави, які практикують інший («східний») підхід, навпаки, пропонують норми, що включають сильний урядовий контроль над інформацією з декларованою метою захисту національного інформаційного простору, або інформаційного (кібер) суверенітету, а це, з погляду прихильників західного підходу, сприймається як загроза політичній стабільності.

Західний підхід, який сформувався в США, ґрунтується на розумінні інформаційної безпеки як безпеки даних і, відповідно, інформаційних систем, що з ними пов'язані.

Іншою характеристичною відмінністю між західним та східним підходами до політики інформаційної (кібер) безпеки є концептуально протилежні погляди на міжнародно-правове регулювання цієї сфери. Суть західної позиції полягає в застосуванні чинних норм, зокрема в аспекті застосування права на початок війни й міжнародного гуманітарного права.

Росія й Китай підкреслюють важкість адаптації міжнародних правил до кіберпростору та зосередилися на просуванні міжнародного «кодексу поведінки» для кіберпростору. Натомість уряд США публічно й неодноразово заявляв, що «кібердіяльність за певних обставин може бути підставою для застосування сили у значенні статті 2 (4) Статуту ООН та міжнародного звичаєвого права» [1]. Існують принципові відмінності в поглядах на цю проблему провідників західного й східного підходів [2].

Аналіз останніх досліджень і публікацій. Головними послідовниками східного підходу є Росія та Китай. Підтвердження цього – відповідні норми в національному законодавстві, діяльність країн на рівні ООН і в регіональних організаціях. Такими документами є доктрини інформаційної безпеки РФ від 2000 та 2016 рр., Військова доктрина РФ, «Концептуальні погляди на діяльність Збройних сил Російської Федерації в інформаційному просторі» (2011 р.) російський проєкт «Конвенції про забезпечення міжнародної інформаційної безпеки» (2011 р.), «Основи державної політики в галузі міжнародної інформаційної безпеки на період до 2020 року», «Основи державної політики РФ в галузі міжнародної інформаційної безпеки» (2021 р.), законодавство про обробку персональних даних про локалізацію даних на території РФ (2014), зміни до федерального законодавства під неформальною назвою «Закон про суверенний інтернет» (2019 р.), поданий Росією проєкт резолюції ГА ООН «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» – від 1998 і наст. р. та 2018 р.

У Китаї такими документами є Державна стратегія інформатизації (2006); документ Держради КНР із просування інформатизації та розвитку чинної системи захисту інформаційної безпеки (2012); Закон КНР про боротьбу з тероризмом (2015); Закон про кібербезпеку (2016); стандарти багаторівневої системи захисту кібербезпеки; Міжнародна стратегія співробітництва в кіберпросторі; Положення про нагляд та перевірку безпеки в інтернеті (2018); Закон про захист особистої інформації (2021); Закон про безпеку даних (2021).

Підходи країн Заходу до безпеки кіберпростору (кібербезпеки) ґрунтуються на концепції, прийнятій у США й відображеній, зокрема, у таких нормативних актах, як Національна стратегія захисту кіберпростору (2003); Всеосяжна національна ініціатива з кібербезпеки (2008); Огляд політики в кіберпросторі (2009); Міжнародна стратегія для кіберпростору (2011); Національна кіберстратегія Сполучених Штатів Америки (2018); поданий Сполученими Штатами у 2018 р. проєкт резолюції ГА ООН «Заохочення відповідальної політики держав у кіберпросторі в контексті міжнародної безпеки».

Згадані вище відмінності в підходах відображені в текстах зазначених документів і в низці наукових публікацій авторів, що репрезентують як країни Заходу [3; 4; 5; 6; 7; 8; 9; 10; 11; 12], так і ті, що демонструють східний підхід [13; 14; 15; 16; 17; 18]. Розподіл країн світу за підходами відображають і результати голосування в ООН за вказані проєкти резолюцій ГА у 2018 р. (цікаво, що географія підтримки проєктів резолюцій відповідає розподілу країн за їх демократичним статусом відповідно до щорічних звітів організації Freedom House [19], – «невільні» країни підтримали російський проєкт, а «вільні» й переважно «частково-вільні» – американський). А зусилля та результати пошуку шляхів подолання протиріч між прихильниками тих чи інших позицій у рамках обох підходів відображені у звітах груп урядових експертів (ГУЕ) та робочої групи відкритого складу (РГВС), скликаних згідно з цими резолюціями на рівні ООН.

Що стосується Європейського Союзу, то його діяльність у сфері інформаційної (кібер) безпеки досліджують автори, які зосереджені на різних аспектах, зокрема на загальних питаннях політики [20] ЄС як суб'єкта безпеки [21], співпраці ЄС з іншими акторами на тлі глобальних викликів кібербезпеки [22] й ін. У контексті позиціювання європейської політики серед різних світових векторів інформаційної (кібер) безпеки досліджено її базис (ціннісну основу) [23], принципи концептуалізації в аспекті балансу м'якої/жорсткої сили [24], основні підходи [25], її стосунок до основних сфер інтересів головних зацікавлених сторін [26] та ін. При цьому залишається широке поле для досліджень у зв'язку з новими подіями й розвитком політики в цій сфері.

Мета статті. Наше дослідження охоплює питання політики ЄС із погляду балансу між східною та західною концепціями інформаційної (кібер) безпеки з урахуванням основних тенденцій у цій сфері за останні роки, а метою є конкретизація й позиціювання підходів ЄС в аспекті міжнародної взаємодії у світлі прийнятих документів.

Методика дослідження. Для досягнення мети цього дослідження ми використали описовий, аналітичний підходи, що переважно спирається на аналіз джерел, що стосуються політики у сфері інформаційної (кібер) безпеки ЄС в аспекті основних світових концепцій. Застосовано якісний підхід із метою вивчення проблематики в цій сфері, яка потребує дослідження з погляду розвитку міжнародних відносин.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Європейський Союз як регіональне інтеграційне об'єднання є найуспішнішим і найамбітнішим проєктом міждержавної співпраці. Але

його специфіка полягає в суто прагматичних підходах до проблем, які мають суттєве й загальне значення для його учасників. Тому в такому аспекті й розробляються всі комунітарні стратегії й реалізуються політики в розрізі окремих галузей або секторів. У контексті розглянутих вище концепцій інформаційної (кібер) безпеки, які відображають суто національні прагнення до втілення певних стратегій у рамках характерних для країн моделей і шляхів розвитку, ЄС, по суті, не має чітко окреслених стратегій, орієнтованих на підтримку чи то американського, чи то російсько-китайського підходів. Але країни – члени ЄС однозначно підтримують демократичний шлях розвитку кіберпростору й відносин у сфері ІКТ. Це проявляється, наприклад, у їх підтримці американського проєкту резолюції ГА ООН «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» [27] у 2018 р. Утім, окремі країни мають свої власні бачення перспектив міждержавного узгодження проблематики кібернетичної/інформаційної безпеки.

Безпека в цій сфері розглядається на рівні ЄС в аспекті саме кібербезпеки й актуалізувалася недавно, порівняно з країнами, розглянутими вище, – фактично лише після прийняття документа про стратегію кібербезпеки ЄС у 2013 р. [28]. Але з того часу відбувається активний розвиток політики ЄС щодо кіберпростору. Починаючи з 2013 р., багато чого досягнуто з погляду політики ЄС у сфері кібербезпеки, яка поставлена в центрі політичних пріоритетів Європейської комісії та зайняла високі позиції в Стратегії єдиного цифрового ринку [29]. Кібербезпека й боротьба з кіберзлочинністю є одним із трьох стовпів Європейського порядку денного щодо безпеки (2015 р.) [30], а в Глобальній стратегії ЄС (2016 р.) [31] вона вже розглядається як горизонтальна політика унії, починаючи від загальнодоступного цифрового простору та закінчуючи елементами діяльності Європейського Союзу. Глобальна стратегія ЄС утілює новий підхід до розуміння проблеми безпеки та загроз для громадян і самого Союзу, серед яких виділено й кіберзагрози поряд із гібридними загрозами, тероризмом, економічною нестабільністю, змінами клімату та енергетичними загрозами. Уперше в питаннях безпеки проголошено курс на стратегічну автономію, що, очевидно, означає необхідність пошуку шляхів протистояння цим загрозам силами самої унії. Не виключено, що до більш автономного підходу в розв'язанні проблем об'єднання спонукали як посилення загроз у кіберпросторі внаслідок прогресу ІКТ, так і непослідовність у зовнішній політиці провідного партнера ЄС – США за часів президентства Д. Трампа [32], а також прецедент виходу зі складу ЄС Великої Британії. Імовірно, ЄС шукатиме й використовуватиме відповідні можливості також на рівні зовнішньої політики.

У сфері кібербезпеки Глобальна стратегія ЄС передбачає узгодження захисту комп'ютерних загроз із гарантією збереження «відкритого, вільного та безпечного кіберпростору» при зміцненні технологічного потенціалу для зменшення загроз, підвищення стійкості критичної інфраструктури, мереж та послуг і протидії кіберзлочинності.

Глобальна стратегія ЄС загалом окреслює декілька рівнів політики кібербезпеки: перший охоплює відносини всередині ЄС, другий стосується стосунків із третіми країнами й міжнародними організаціями, а третій відображає спільне бачення в цій сфері для узгодженої репрезентації на міжнародних майданчиках.

У відносинах із міжнародними організаціями у сфері кібербезпеки головним пріоритетом є посилення співпраці з такими основними партнерами, як США та НАТО. Але основним меседжем для міжнародного співтовариства, уміщеним у тексті стратегії, є чітко висловлена позиція, яка відповідає західному (американському) підходу до забезпечення безпеки в кіберпросторі – це реалізація своєї прагматичної мети стати «перспективним кібергравцем, захищаючи свої найважливіші активи та цінності в цифровому світі, зокрема шляхом просування вільного й безпечного глобального інтернету через прогресивний альянс між державами, міжнародними організаціями, промисловістю, громадянським суспільством та технічними експертами». І найголовніше – це те, що ЄС «шукатиме угод про відповідальну поведінку держав у кіберпросторі на основі наявного міжнародного права. Він підтримуватиме багатостороннє цифрове управління та глобальні рамки співпраці з кібербезпеки, поважаючи вільний потік інформації» [31]. Тому можна стверджувати, що Європейський Союз виступає одним фронтом з іншими країнами Заходу в питанні політики інформаційної (кібер) безпеки, що проявляється, зокрема, в успішному розвитку концепції заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки, згодом представленої Сполученими Штатами у вигляді проєкту резолюції ГА ООН.

Від початку розробки політики у сфері кібербезпеки ЄС орієнтувався більшою мірою на так звану м'яку безпеку: посилення зовнішнього виміру політики ЄС у сфері кібербезпеки, підвищення стійкості мереж і систем ІКТ до кіберзагроз, розробку можливостей та інструментів реагування на кібератаки, співпрацю в боротьбі з кіберзлочинністю, просування стандартів і цінностей у кіберпросторі. У 2016 р. Директивою про безпеку мереж та інформаційних систем (NIS) [33] прийнято перші загальні правила безпеки інформаційних систем. Директива NIS передбачає правові заходи для підвищення рівня кібербезпеки ЄС,

забезпечуючи те, щоб країни-члени були готові реагувати на інциденти з кібербезпеки за допомогою групи реагування на інциденти комп'ютерної безпеки (CSIRT) і компетентних національних органів NIS; підтримували стратегічне співробітництво та обмін інформацією щодо конкретних питань про інциденти й ризики; сприяли розвитку кібербезпеки серед операторів критичної інфраструктури. У цій сфері працюють спеціалізоване Агентство ЄС із питань безпеки мережі та інформації (ENISA), Європейський центр кіберзлочинності (EC3) у структурі Європолу, Команда ЄС з питань комп'ютерного реагування на надзвичайні ситуації (CERT-EU) та Європейське оборонне агентство.

Однак згадана вище концепція стратегічної автономії, представлена в Глобальній стратегії ЄС, у найближчі роки, очевидно, вимагатиме певних заходів, підтриманих відповідним рівнем фінансування. Практичну реалізацію цього нового підходу розпочато з прийняттям у вересні 2017 р. так званого пакета кібербезпеки, із пропозицією низки заходів, які надалі координовано зміцнюватимуть структури й можливості ЄС у сфері кібербезпеки при повній співпраці держав-членів і різних зацікавлених структур ЄС [34].

Наприкінці 2020 р. Європейська комісія та Високий Представник Союзу із закордонних справ і політики безпеки презентували нову «Стратегію кібербезпеки для цифрового десятиліття» [35], яка має на меті посилити колективну стійкість об'єднання до кіберзагроз і гарантувати надійність цифрових послуг та інструментів. Також Комісія внесла дві нові пропозиції – оновлену Директиву NIS2 [36] про заходи щодо високого загального рівня кібербезпеки в усьому Союзі та нову Директиву щодо стійкості критичних організацій [37]. Разом ці документи становлять новий пакет із кібербезпеки. Доповнення європейського вторинного права у сфері кібербезпеки стало логічним кроком після врахування виявлених недоліків попередніх нормативних актів і викликів, що з'явились у зв'язку з пандемією Covid-19.

Стратегія описує кібербезпеку як багаторівневу проблему, для розв'язання якої сформовано сфери діяльності: стійкість, технологічний суверенітет та лідерство; нарощування оперативного потенціалу для запобігання, стримування й реагування; просування глобального та відкритого кіберпростору.

ЄС планує побудувати мережу Оперативних центрів безпеки на всій своїй території, що працює на основі штучного інтелекту, щоб створити європейський «щит кібербезпеки» [38], розгорнути надзвичайно безпечну інфраструктуру квантового зв'язку для Європи для передачі

конфіденційної інформації й упровадити низку інших інструментів і заходів, наприклад зміцнити інструменти кібердипломатії, розробити план дій на випадок надзвичайних ситуацій для вирішення екстремальних сценаріїв, що впливають на цілісність і доступність глобальної кореневої системи DNS, установити стандарти безпеки.

Відзначимо, що ЄС реагує на посилення кіберзагроз розгортанням системи засобів та інструментів протидії, охоплюючи все більше сфер, пов'язаних із кіберпростором. Так, у резолюції, прийнятій 10 червня 2021 р., Європарламент закликає забезпечити захист пов'язаних продуктів і супутніх послуг, уключаючи ланцюжки поставок в аспекті стійкості до кіберінцидентів, наголошує на необхідності встановлення вимог кібербезпеки щодо програм, програмного забезпечення, убудованого програмного забезпечення (яке контролює різні пристрої та машини, що не є комп'ютерами) та операційних систем (програмне забезпечення, котре виконує основні функції комп'ютера) до 2023 р. [39] Цілком імовірно, що реалізація таких вимог матиме наслідки, подібні до обмеження присутності на ринку відповідних продуктів іноземного виробництва, як це було в США.

У березні 2021 р. Комісія виклала своє бачення цифрової трансформації Європи до 2030 р. в Комюніке «Цифровий компас: європейський шлях до Цифрового десятиліття» [40], у якому фактично виклала «європейське» бачення цифрового суверенітету, що полягає в амбітному плані щодо проведення цифрової політики, яка передбачає усунення вразливих місць та залежностей, а також прискорення інвестицій задля випереджаючого розвитку ЄС у відкритому й взаємопов'язаному світі. Поставлено цілі, орієнтовані на пришвидшений розвиток цифрової економіки та суспільства й запропоновано скласти набір цифрових принципів, що охоплюють такі сфери, як доступ до інтернет-послуг, безпечне й надійне онлайн-середовище, цифрові медичні послуги, цифрові державні послуги та адміністрація, орієнтовані на людину. Ці принципи доповнять наявні права, які вже захищають і розширюють можливості європейців в інтернеті, такі як захист особистих даних та конфіденційності, свобода вираження поглядів, свобода створення й ведення бізнесу в інтернеті та захист інтелектуальної власності.

На перший погляд, європейська стратегія за масштабом нагадує підхід Китаю, який полягає в державному управлінні й спрямовуванні економіки та всього суспільства, але насправді її суть – у перерозподілі стимулів і фактичній відсутності геополітичних амбіцій. І «суверенітет» ЄС у цифровому світі – це лише певна технологічна незалежність,

заснована на інвестиціях у європейські дослідницькі й інвестиційні проєкти у сферах ІКТ та телекомунікацій.

Натомість ЄС залишається орієнтованим на західну (американську) концепцію в питаннях розвитку кіберпростору і його безпеки. Відповідно до нової стратегії, унія активізуватиме роботу з міжнародними партнерами щодо зміцнення, заснованого на правилах глобального порядку, сприяння міжнародній безпеці та стабільності в кіберпросторі й захисту прав людини та основних свобод в інтернеті, просуватиме міжнародні норми й стандарти, які відображають ці основні цінності ЄС, співпрацюючи зі своїми міжнародними партнерами в ООН та на інших відповідних форумах.

Важливо, що, переслідуючи власні цілі, ЄС бере активну участь у поширенні західної концепції розвитку кіберпростору. Але при цьому розробляються й просуваються власні позиції з актуальних для міжнародної взаємодії питань. Це стосується, наприклад, позиції ЄС щодо кіберстримування, яка ще виробляється й, відповідно до стратегії кібербезпеки 2020 р., «повинна сприяти відповідальній поведінці держави та співробітництву в кіберпросторі, а також давати особливі вказівки щодо протидії тим кібератакам, які мають найбільш значний ефект, особливо тим, що впливають на нашу критичну інфраструктуру, демократичні інститути та процеси» [35]. Окрім того, розглядаються можливості подальших варіантів обмежувальних заходів у рамках набору інструментів у сфері кібердипломатії й режим горизонтальних санкцій проти кібератак.

У стратегії ЄС надалі зміцнить свій набір інструментів ЄС із кібернетичної дипломатії (сукупність дипломатичних практик, що стосуються широко визначеного управління кіберпростором) для забезпечення її функціонування на регулярній основі, подальшого інтегрування інструментарію кібердипломатії в кризові механізми ЄС, забезпечення синергії в зусиллях щодо протидії гібридним загрозам, дезінформації та зовнішнього втручання в рамках Спільної рамки протидії гібридним загрозам [41].

Зовнішній вимір нової стратегії кібербезпеки ЄС заснований на традиційно прагматичному підході, що полягає в продовженні співпраці з міжнародними партнерами для просування політичної моделі та свого бачення кіберпростору як заснованого на верховенстві права, правах людини, основних свободах і демократичних цінностях задля соціального, економічного та політичного розвитку. Одним із пріоритетів визначено активізацію діяльності у сфері міжнародних стандартизаційних процесів

і лідерство в них. Це пояснюється технологічними й економічними перевагами тих, хто отримує пріоритет у розробці й затвердженні таких стандартів, а також тим, що міжнародна стандартизація все частіше використовується третіми країнами для просування своєї політичної й ідеологічної програми, зокрема спираючись на розробки в таких сферах, як штучний інтелект, хмарні та квантові обчислення й квантова комунікація, що часто не відповідає цінностям ЄС. Наприклад, перспективні технологічні розробки Китаю в зазначених сферах застосовуються для обмеження свободи слова, громадянських і політичних прав [42].

Нова кіберстратегія однозначно вказує на продовження курсу співпраці з міжнародними партнерами для просування концепції глобального, відкритого, стабільного та безпечного кіберпростору, де поважається міжнародне право, зокрема Статут ООН, а також добровільні необов'язкові норми, правила та принципи відповідальної поведінки держав у кіберпросторі відповідно до доповідей групи урядових експертів у галузі інформації й телекомунікацій у контексті міжнародної безпеки, схвалених Генеральною асамблеєю ООН. Очевидно, у загальних рисах така позиція відповідає й консенсусному звіту Робочої групи відкритого складу 2021 р. [43]

Із загостренням багатосторонніх дебатів із питань міжнародної безпеки в кіберпросторі, зокрема після представлення конкуруючих проєктів резолюції ГА ООН у 2018 р. Росією та США, виникла очевидна необхідність, зайняття Європейським Союзом і державами-членами більш активної позиції в дискусіях в ООН та на інших відповідних міжнародних форумах. ЄС має найкращі можливості для просування, координації й закріплення позицій держав-членів на міжнародних форумах, а також, як зазначено в Стратегії кібербезпеки 2020 р., «...має виробити позицію ЄС щодо застосування міжнародного права в кіберпросторі»[35].

У зв'язку з цим особливо варто відзначити проактивну позицію окремих держав-членів і самого ЄС. У жовтні 2020 р. Франція з Єгиптом і 40 інших держав (Аргентина, Колумбія, Еквадор, Габон, Грузія, Японія, Марокко, Норвегія, Сальвадор, Сінгапур, Республіка Корея, Республіка Молдова, Республіка Північна Македонія, Сполучене Королівство, ЄС та його держави-члени), запропонували програму дій (ПД) [44] для просування відповідальної поведінки держав у кіберпросторі. У світлі багаторічної конкуренції між російсько-китайським і західним підходами до інформаційної безпеки/ безпеки кіберпростору це виглядало як спроба подолати роздвоєність дискусій із кіберпитань в ООН у рамках групи урядових експертів та робочої групи відкритого складу. Ця ініціатива

оформлена не у вигляді проєкту резолюції, а як записка, опублікована в рамках РГВС. Її основним прихильником, очевидно, є Франція, підтримана ЄС і всіма його членами, а також низкою держав, орієнтованих переважно на підтримку західного підходу в питаннях кібербезпеки. Ці країни заявляють, що вони хотіли б, замість розділеної між ГУЕ й РГВС дискусії, бачити один постійний форум, який займався би питаннями використання державами ІКТ у контексті міжнародної безпеки. Як модель вони пропонують узяти формат, власне, програм дій – за аналогією з Програмою дій щодо запобігання й викорінення незаконної торгівлі стрілецькою зброєю та легкими озброєннями у всіх її аспектах і боротьби з нею.

Заснований цими сторонами «Постійний форум ООН для розгляду питання використання ІКТ державами в контексті міжнародної безпеки» передбачає, що ПД має діяти «в єдиному, довгостроковому, інклюзивному та орієнтованому на прогрес форматі; чиї умови можуть бути обговорені поточними ГУЕ й РГВС», тоді як упровадження та подальші заходи можуть бути згодом схвалені Генеральною асамблеєю ООН. Відповідно до пропозиції, ПД може «створити рамки та політичні зобов'язання» на основі наявних міжнародних рамок, тобто рекомендацій, норм і принципів, які вже узгоджені, зокрема, у звіті ГУЕ ООН 2015 р. Відповідно, проводитимуться регулярні щорічні зустрічі на робочому рівні, зосереджені на впровадженні рамок, котрі існують. ПД має сприяти посиленню співробітництва, а також ініціювати консультації з іншими зацікавленими сторонами, регіональними організаціями й установами ООН, а також залучати інші зацікавлені сторони. Запропоновано кожні п'ять років проводити регулярні конференції, орієнтовані на консенсус, на яких держави можуть вирішити, чи слід розробляти додаткові норми.

У Стратегії кібербезпеки ЄС 2020 р., яка побачила світ майже відразу після згаданої вище ініціативи щодо ПД, є безпосередня прив'язка до останньої. ЄС оголошує про просування консенсусної пропозиції відповідно до Програми дій щодо покращення відповідальної поведінки держав у кіберпросторі, в ООН. Спираючись на цей доробок ГУЕ 2015, 2013 та 2010 рр., схвалений Генеральною асамблеєю ООН, ЄС підтримує пропозицію платформи для співпраці й обміну кращими практиками в рамках ООН, а також пропонує створити механізм для впровадження на практиці норм відповідальної поведінки держав.

Про відповідність такої позиції Євросоюзу якомусь із двох домінантних підходів до кібербезпеки свідчить те, що ініціативу ПД не підтримали ні Росія, ні Китай, що зрозуміло з їх просування концепцій

міжнародної інформаційної безпеки та кіберсуверенітету. Але й США також не підтримали цю пропозицію, що, однак, не виключає ймовірності певного маневру, оскільки французько-єгипетський проєкт і за назвою, і по суті наближений саме до американської ініціативи на рівні ООН щодо заохочення відповідальної поведінки держав у кіберпросторі. І, врешті, у досягненні консенсусу на рівні РГВС у березні 2021 р., коли було прийнято консенсусну доповідь РГВС, імовірно, певну роль відіграли саме поява зазначеної ПД та її потужна підтримка з боку ЄС. У такій ситуації представники західної концепції безпеки кіберпростору отримали явну перевагу.

Відповідно до західного (демократичного) підходу до розвитку кіберпростору, ЄС ставить стратегічні цілі протидіяти цензурі, масовому стеженню, порушенню конфіденційності даних і репресіям проти громадянського суспільства й громадян із застосуванням ІКТ, лідируючи у сфері захисту та просування прав людини й основних свобод в інтернеті.

Із цією метою ЄС має сприяти подальшому дотриманню міжнародного законодавства та стандартів у сфері прав людини, зокрема Статуту ООН і Загальної декларації прав людини, а також упроваджувати в життя прийнятий у ЄС у листопаді 2020 р. План дій із прав людини та демократії на 2020–2024 рр. [45]. Також у цьому контексті варто згадати прийняті в ЄС у 2014 р., але актуальні й у стратегічній перспективі Настанови з прав людини щодо свободи вираження поглядів в інтернеті та офлайн [46].

Ще одним пунктом, у якому позиція ЄС збігається з американською й протилежна російській, є міжнародна співпраця у сфері протидії кіберзлочинності. ЄС дотримується Будапештської конвенції Ради Європи про кіберзлочинність і заявляє про підтримку третіх країн, які бажають приєднатися до неї, а також про необхідність доопрацювання Другого додаткового протоколу до Будапештської конвенції, що включає заходи та гарантії для покращення міжнародної співпраці між правоохоронними й судовими органами, а також між органами влади та постачальниками послуг в інших країнах. Водночас Євросоюз виступає проти створення нового правового інструменту щодо кіберзлочинності на рівні ООН, ініційованого Росією в постаті поданого нею у 2017 р. проєкту конвенції ООН «Про співпрацю у сфері протидії інформаційній злочинності», який «ризикує посилити розбіжності та уповільнити настільки необхідні національні реформи та зусилля з розбудови спроможності, що потенційно може перешкоджати ефективному міжнародному співробітництву у сфері боротьби з кіберзлочинністю: ЄС не бачить необхідності у будь-якому новому правовому інструменті щодо кіберзлочинності на рівні ООН» [35].

Стратегія кібербезпеки ЄС передбачає створення Порядку денного розбудови зовнішнього кіберпотенціалу ЄС. Відповідно до прийнятих у 2018 р. керівних напрямів [47] для розробки цього Порядку денного, «створення кіберпотенціалу стає однією з найважливіших тем у порядку денному міжнародної кіберполітики». А розбудова кіберпотенціалу третіх країн за участі ЄС передбачає «систематичні зусилля з партнерами країн та відповідних організацій для покращення національних, інституційних й організаційних можливостей, які покращують стійкість критичних цифрових послуг та мереж, а також захист критичної інформаційної інфраструктури; підтримку реформ кримінального правосуддя у сфері кіберзлочинності; боротьбу з використанням інтернету в терористичних цілях; удосконалення навичок і компетенцій кібербезпеки; сприяння підвищенню обізнаності та ефективній співпраці з цих питань на національному, регіональному та міжнародному рівнях»[47]. Також передбачається посиленням цивільних аспектів Спільної політики безпеки та оборони шляхом уключення в неї заходів із кібербезпеки з акцентом на зміцнення стійкості й можливості третіх країн.

На відміну від Китаю, ЄС орієнтується на підтримку країн не за їх прихильністю до певного курсу (як-от китайська концепція «Пояс і шлях»), а чітко визначає серед пріоритетних, щодо яких буде здійснено підтримку ЄС у справі розбудови кібернетичного потенціалу, країни-сусіди й загалом ті, що розвиваються.

Для практичної реалізації своїх цілей у сфері розвитку зовнішнього кіберпотенціалу ЄС утворює мережу EU CyberNet [48], яка повинна посилити глобальну реалізацію, координацію та узгодженість проєктів Європейського Союзу щодо створення кіберпотенціалу й можливості Європейського Союзу надавати технічну допомогу третім країнам у сфері кібербезпеки та кіберзлочинності. Необхідність такої мережі стала актуальною після безпрецедентних за масштабами глобальних атак зловмисного програмного забезпечення навесні 2017 р., коли в комюніке «Стійкість, стримування, оборона: створення міцної кібербезпеки для ЄС» [49] Європейська комісія закликала створити мережу ЄС із розбудови кіберпотенціалу, яка підтримуватиме поточні й майбутні зусилля ЄС у сфері кібернетичного потенціалу в третіх країнах. Запущена у 2019 р., EU CyberNet має намір досягти чотирьох основних результатів за чотири роки: створення мережі експертів і зацікавлених сторін у сфері кібербезпеки, розробка технічної платформи, забезпечення навчання та допомоги й перетворення на центр знань про зовнішні відносини ЄС у сфері кібербезпеки.

Пріоритетними для ЄС у цьому аспекті є країни Західних Балкан, країни сусідства, а також країни-партнери, які демонструють швидкий цифровий розвиток. Зокрема у рамках EU CyberNet розпочато діяльність щодо розбудови потенціалу на Африканському континенті та в Латинській Америці для розробки законодавства й політики країн-партнерів у взаємозв'язку з відповідною політикою й стандартами ЄС у сфері кібернетичної дипломатії. Наприклад, у 2021 р. в Домініканській Республіці проведено перші національні навчання з кібербезпеки «Кіберполум'я» й проведено роботу зі створення майбутнього центру кіберкомпетентності для країн Латинської Америки й Карибського басейну [50].

Важливого значення ЄС надає співпраці з питань безпеки кіберпростору і з регіональними організаціями, такими як Африканський Союз, Регіональний форум АСЕАН, Організація американських держав та ОБСЄ, а також з іншими партнерами – із питань, що становлять спільний інтерес. Поставлено мету – за участі представництв ЄС, а також посольств держав – членів у всьому світі, створити неформальну мережу ЄС із кібернетичної дипломатії для популяризації європейського бачення кіберпростору, обміну інформацією й координації щодо подій у кіберпросторі.

І основним у стратегії міжнародної співпраці ЄС із питань безпеки кіберпростору є те, що, відповідно до своїх цінностей, унія рішуче підтримує та пропагує модель управління інтернетом із багатьма зацікавленими сторонами: «Жодна окрема організація, уряд чи міжнародна організація не повинні прагнути контролювати інтернет».

Особливе значення для ЄС має співпраця в питаннях безпеки з НАТО, організації, яка об'єднує більшість країн-членів унії. У цьому напрямі в липні 2016 р. у Варшаві підписано Спільну декларацію [51] з метою надати нового імпульсу та нової сутності стратегічному партнерству ЄС – НАТО, зокрема й у сферах протидії гібридним загрозам, кібербезпеки та оборони. На основі мандату Спільної декларації Європейський Союз і НАТО створили спільний набір пропозицій щодо її імплементації, який був схвалений Радами ЄС та НАТО в грудні 2016 р. У сфері кібербезпеки й оборони оголошено про розширення координації, уключаючи контекст місій та операцій, навчань та освіти а також щодо сумісності у сфері кіберзахисту. Серед напрямів співпраці – підвищення здатності протидіяти гібридним загрозам, у тому числі шляхом посилення стійкості, спільної роботи над аналізом, запобіганням і раннім виявленням шляхом своєчасного обміну інформацією, співпраця у сфері стратегічної комунікації та реагування.

З огляду на концептуальний підхід до питань інформаційної (кібер) безпеки виняткове значення має те, що країни ЄС, які одночасно є членами НАТО, по суті, приймають оголошену у форматі необов'язкового, але принципово важливого документа, позицію щодо застосування чинного міжнародного права в кіберпросторі. Ідеться про так званий «Талліннський посібник» («The Tallinn Manual on the International Law Applicable to Cyber Warfare») [52], розроблений за участі Центру передового досвіду кіберзахисту НАТО. Документ являє собою думки учасників робочої групи фахівців, які, зважаючи на відсутність загальновизнаних міжнародних норм із кібербезпеки, наводять оцінку застосовності чинних норм до цієї сфери. У «Таллінському посібнику» дається чітка позиція щодо застосовності чинних норм міжнародного права й поняття суверенітету в кіберпросторі, – відповідно до західної концепції кібербезпеки.

Також важливим індикатором європейського підходу в політиці інформаційної (кібер) безпеки є тісна співпраця ЄС зі Сполученими Штатами Америки. ЄС і США мають подібні погляди у сфері безпеки кіберпростору відтоді, коли вона стала актуальною в міжнародному вимірі, відзначаючи, що міжнародне співробітництво є центральним елементом кібербезпеки. Головною ознакою спільного для них західного підходу в питанні безпеки кіберпростору є дотримання принципу свободи обміну інформацією в мережі та демократичної концепції організації самого кіберпростору [12].

Одним із перших спільних інтересів ЄС і США стала боротьба з кіберзлочинністю. Відповідну ініціативу Ради Європи 2001 р. (Будапештська конвенція) обидві сторони спільно підтримують на рівні ООН, координують свої зусилля на практиці й спільно діють для просування цього стандарту на міжнародному рівні. Конвенцію ратифіковано багатьма країнами, що не є членами Ради Європи, уключаючи Сполучені Штати, які мають статус спостерігача в Раді. В інституційному плані сторони співпрацюють через створену у 2010 р. Робочу групу ЄС і США з питань кібербезпеки та кіберзлочинності, програми співпраці, спільні навчання між ЄС та США для протидії кіберінцидентам, залучення приватного сектору. Утіленням західного підходу до кібербезпеки стала співпраця в розслідуванні й боротьбі з кіберзлочинністю. Наприклад сторони започаткували «Глобальний альянс проти сексуального насильства над дітьми в інтернеті», який мав на меті посилити боротьбу цих країн проти сексуальної експлуатації дітей в інтернеті, що після об'єднання у 2016 р. з американсько-британським альянсом WePROTECT став одним

із найбільших у сфері координації зусиль щодо кібербезпеки й сьогодні об'єднує 98 країн, десятки компаній, громадських і міжнародних організацій [53].

Здійснюється координація між ЄС та США і в практичних напрямах координації мережі, зокрема між спеціалізованими інституціями. Обидві сторони поділяють спільні принципи та візії щодо управління інтернетом, такі як відкритість, свобода та сумісність, а також гарантії прав і свобод людини у сфері кібербезпеки. І США, і ЄС визнають єдино багатостороннє управління інтернетом, децентралізоване й демократичне в прийнятті рішень. Цей підхід передбачає політику «знизу вгору» в інтересах усіх зацікавлених сторін на рівних умовах. Європейські політики високо оцінюють значення інституційної співпраці з американськими колегами щодо кібербезпеки, небезпідставно зважаючи на їхній великий досвід і високі компетентності в цій сфері [54].

Ще одним результатом розвитку євроатлантичної співпраці у сфері кібербезпеки став Кібердіалог між ЄС та США, який розпочав роботу в грудні 2014 р., орієнтований, зокрема, на координацію зовнішньої політики сторін із кіберпитань і стратегічні аспекти глобальної кібербезпеки, у тому числі встановлення норм поведінки та заходів щодо зміцнення довіри в кіберпросторі й застосування наявних норм міжнародного права в кіберпросторі [55].

Важливою характеристичною ознакою американсько-європейського підходу до безпеки кіберпростору є активне залучення до управління ним приватного сектору, науки й громадянського суспільства. У цьому напрямі Європейський Союз та США започаткували Трансатлантичну ініціативу з дослідження кіберполітики, що об'єднує академічні, промислові й експертні центри для розв'язання ключових проблем кіберполітики та збільшення потенціалу досліджень у сфері кіберпитань..

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Загальна концепція інформаційної (кібер) безпеки в ЄС схожа з такою в США й відповідає західному підходу в політиці в цій сфері. Ураховуючи діяльність і стратегію ЄС щодо протидії основним загрозам, пов'язаним із розвитком кіберпростору, а також його взаємодію з міжнародними партнерами, зокрема НАТО й США, помітне протистояння між ЄС та США, з одного боку, і Росією й Китаєм – з іншого, із питань, пов'язаних з управлінням інтернетом та правами людини в інтернеті. У контексті конкуренції за встановлення глобальних стандартів ЄС і США протистоять

зусиллям Росії й Китаю в їх намаганні контролювати та цензурувати вміст інтернету й підривати нинішню модель управління інтернетом (уключно з іншими зацікавленими сторонами, замінюючи її на міжурядові та державно-центричні структури). Також непорушною є принципово «західна» позиція ЄС щодо застосовності норм міжнародного права у сфері кібербезпеки, яка, зокрема, підтверджується країнами-членами в утвердженні такої концепції на рівні їхньої діяльності в НАТО. Найімовірніше, що спільні інтереси сприятимуть розвитку співпраці й консолідації країн Заходу, зміцненню й поширенню західної концепції інформаційної (кібер) безпеки.

Проте великий інтерес викликає розвиток ситуації на рівні міжнародної взаємодії головних акторів у сфері інформаційної (кібер) безпеки, де залишаються актуальними давно наявні протиріччя й з'являються нові виклики. У цьому аспекті, очевидно, перспективним є дослідження діяльності стейкхолдерів кожного із зазначених підходів із погляду стратегічних інтересів учасників європейської інтеграції і пов'язаних із нею сторін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Koh, Harold Hongju (2012). International Law in Cyberspace. *Harvard International Law Journal*, 54 (December 2012). URL: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

2. Ku, Julian (2017). How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare. Hoover Working Group on National Security, Technology, and Law. *Aegis Series Paper*, No. 1707. A hoover Institution Essay. URL: https://www.hoover.org/sites/default/files/research/docs/ku_webreadypdf.pdf

3. Anagnostakis, Dimitrios (2021). The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. *Journal of Cyber Policy*. DOI: 10.1080/23738871.2021.1916975

4. Brousseau, Eric, Marzouki, Meryem, MéadeL, Cécile (editor/s) (2012). *Governance, regulations and powers on the Internet.* Cambridge: Cambridge University Press.

5. Holdorf Polly, M. (2015). *Prospects for an International Cybersecurity Regime.* INSS. USAF Academy, Colorado. URL: https://apps.dtic.mil/sti/citations/AD1070618

6. Kshetri, Nir (2014). *Cybersecurity and International Relations: The U.S. Engagement with China and Russia.* Prepared for FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina, July 23–25. URL: http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf

7. Mueller, Milton (2013). Are we in a digital Cold War?, paper presented at the GigaNet workshop, *'The global governance of the internet: intergovernmentalism, multistakeholderism and networks',* Graduate Institute, Geneva, 17 May.

8. Nocetti, Julien (2015). *Contest and conquest: Russia and global internet governance. International Affairs*, 91 (1), January, 111–130.

9. Risen, T. (2015). *China, Russia Seek New Internet World Order. US News and World Report.* 14.05.

10. Ristow, B. (2013). *The New Gatekeepers: Controlling Information in the Internet Age.* Center for International Media Assistance, 25 p.

11. Sadowsky, J., Zambrano, R., Dandjinou, P. (2004). *Intrenet Governance:* a Discussion Document: Prepared for the UN ICT Task Force. Nev-York.

12. Taylor, Emily, and Hoffmann, Stacie (2019). *EU–US Relations on Internet Governance. Chatham House.* URL: https://www.chathamhouse.org/publication/eu-us-relations-internet-governance.

13. Евдокимов, Е. (2011). Политика Китая в глобальном иформационном пространстве. *Международные процессы,* 1 (25).

14. Зиновьева, Елена (2014). Международное сотрудничество по обеспечению информационной безопасности. *Право и управление. XXI век,* 1 (33), 44–52.

15. Карасев, П. А. (2015). *Политика безопасности США в глобальном информационном пространстве.* Автореф. дис .... канд. полит. наук спец.: 23.00.04. Москва: ИМЭМО РАН.

16. Крутских, А. В. (2007). К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы,* 1 (5), 28–37.

17. Мозолина, О. В. (2006). США и международное сообщество: борьба за управление Интернетом. *США и Канада: экономика, политика, культура,* 4, 111–119.

18. Шариков, П. А. (2019). Подходы США, ЕС и России к проблеме информационной безопасности. *Современная Европа,* 2, 73–83.

19. *Global Freedom Status. Freedom House.* https://freedomhouse.org/explore-the-map?type=fiw&year=2021.

20. Bendiek, A. (2012). European Cyber Security Policy. *SWP Research Paper,* No. 13. URL: http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paper-detail/article/european_cyber_security_policy.htm

21. Carrapico, Helena, Barrinha, André (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies*, Vol. 55, issue 6, November, p. 1254–1272. URL: https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.12575

22. Ilves, l. K., Evans, t. J., Cilluffo, f. J., & Nadeau, a. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. *PRISM*, 6 (2), 126–141. URL: http://www.jstor.org/stable/26470452

23. Schaake, Marietje & Vermeulen, Mathias (2016). Towards a values-based European foreign policy to cybersecurity. *Journal of Cyber Policy*, 1:1, 75–84. DOI: 10.1080/23738871.2016.1157617

24. Kok, Ayse (2018). Conceptualizing Cyber-Security From EU Perspective. *In Proliferation of Open Government Initiatives and Systems*, 143–154.

25. Christou, George (2017). *The EU's Approach to Cybersecurity. EU-Japan Security Cooperation: Challenges and Opportunities.* University of Essex. Online paper series, Spring/Summer 2017. http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf

26. Bendiek, Annegret, Porter Andrew, L. (2013). European Cyber Security Policy within a Global Multistakeholder Structure. *European Foreign Affairs Review*, 18 (2), 155–180. URL: https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/18.2/EERR2013011

27. 73/266. *Advancing responsible State behaviour in cyberspace in the context of international security.* Resolution adopted by the General Assembly on 22 December 2018. URL : https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266

28. *EU Cyber Security strategy: An open, safe and secure Cyberspace,* 7 February, 2013. URL: https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

29. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe* /* COM/2015/0192 final */. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

30. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS.* The European Agenda on Security. Strasbourg, 28.4.2015, COM (2015), 185 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

31. *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy,* June 2016. URL: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

32. Haass, Richard (2020). Present at the Disruption. How Trump Unmade U.S. Foreign Policy. *Foreign Affairs,* September/October 2020. URL: https://www.foreignaffairs.com/articles/united-states/2020-08-11/present-disruption

33. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

34. *Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU',* publication 19 September 2017. URL: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu

35. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL *The EU's Cybersecurity Strategy for the Digital Decade. European Commission.* Brussels, 16.12.2020 JOIN (2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

36. *Revised Directive on Security of Network and Information Systems (NIS2). European Commission.* Publication 16 December 2020. URL: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2

37. *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities.* Brussels, 16.12.2020 COM(2020) 829 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

38. *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. European Commission*, 16 December 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

39. *European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade* (2021/2568(RSP)). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html

40. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital Compass: the European way for the Digital Decade.* COM/2021/118 final. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

41. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats. European Commission.* Brussels, 6.4.2016 JOIN(2016) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

42. Wakefield, Jane (2021). AI emotion-detection software tested on Uyghurs. *BBC News*, 26 May. URL: https://www.bbc.com/news/technology-57101248

43. *Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report.* A/AC.290/2021/CRP.2. 10 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

44. *The future of discussions on ICTs and cyberspace at the UN. Updated version: 10/08/2020*. URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

45. *EU Action Plan on Human Rights and Democracy 2020–2024. Council of the European Union.* Brussels, 18 November 2020. URL: https://www.consilium.europa.eu/media/46838/st12848-en20.pdf

46. *EU Human Rights Guidelines on Freedom of Expression Online and Offline. Council of the European Union.* Brussels, 12 May 2014. https://www.consilium.europa.eu/media/28348/142549.pdf

47. *EU External Cyber Capacity Building Guidelines. Council of the European Union.* Brussels, 26 June 2018. URL: https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

48. *EU CyberNet – the bridge to cybersecurity expertise in the European Union.* URL: https://www.eucybernet.eu/

49. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission.* Brussels, 13.9.2017 JOIN(2017) 450 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

50. *EU CyberNet work in Dominican Republic, first national cybersecurity exercise «Cyber llamas». EU CyberNet*, 21.05.2021. URL: https://www.eucybernet.eu/eu-cybernet-work-in-dominican-republic-first-national-cyber-llamas-exercise/

51. *JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL, THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION.* URL: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

52. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* General editor Michael N. Schmitt (2013). Cambridge University Press.

53. *The Alliance.* URL: https://www.weprotect.org/alliance/

54. SPEECH/12/315 Cecilia Malmström. European Commissioner responsible for Home Affairs. The European Response to the rising Cyber Threat. *Transatlantic Cyber Conference organised by the Center for Strategic and International Studies, the European Secu-*

rity Roundtable and SRA International. Washington, 2 May 2012. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_315

55. *EU-U.S. Cyber Dialogue Bruxelles. EEAS. Press Release,* 16/12/2016. URL: https://www.statewatch.org/media/documents/news/2016/dec/eu-eeas-eu-us-cyber-dialogue-pr-16-12-16.pdf

EU POLICY WITHIN THT BASIC GLOBAL CONCEPTS OF INFORMATION (CYBER) SECURITY

This study identifies the specifics of the European Union's cyber security policy in terms of dominant approaches to information (cyber) security policy.

EU information security and infrastructure security policy has been examined in conjunction with the dominant approaches, demonstrated today by the main stakeholders in cyberspace development. These approaches are two concepts that differ mainly in views on Internet governance, national sovereignty over cyberspace, and the principled position on the need to form a special domain in the field of international law to cover cyber security issues. On the world stage, Russia and China are key followers and promoters of the idea of sovereign management of cyberspace resources and Internet governance, as well as the formation of a special legal regime for international information security. They are opposed by the United States and a number of democracies in the West.

This study analyzes the main strategic documents of the secondary law of the European Union in the field of information security and network security in order to identify compliance with one of the approaches. The study reviews and discusses in detail The EU's Cybersecurity Strategy in the Digital Decade, adopted in late 2020, and related documents. We also determined the proximity of the European Union's approaches to the Western model of information (cyber) security and analyzed how cyber security is being promoted in the world. We also considered the initiatives of the member states of the European Union to actively influence the course of international cooperation in this area, in particular, taking into account the events and trends related to the activities of leading actors at the UN level.

As a result, we can conclude that the EU policy in the field of information (cyber) security is becoming more defined and that the EU's constructive position on this issue is being actively promoted on the world stage.

Key words: cybersecurity, international policy, European Union.

REFERENCES

1. Koh, Harold Hongju (2012). International Law in Cyberspace. *Harvard International Law Journal,* 54 (December 2012). URL: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

2. Ku, Julian (2017). How China’s Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare. Hoover Working Group on National Security, Technology,

and Law. *Aegis Series Paper,* 1707. A hoover Institution Essay. URL: https://www.hoover.org/sites/default/files/research/docs/ku_webreadypdf.pdf

3. Anagnostakis, Dimitrios (2021). The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. *Journal of Cyber Policy.* DOI: 10.1080/23738871.2021.1916975

4. Brousseau, Eric, Marzouki, Meryem, MéadeL, Cécile (editor/s), *Governance, regulations and powers on the Internet.* Cambridge: Cambridge University Press, 2012.

5. Holdorf Polly, M. (2015). *Prospects for an International Cybersecurity Regime. INSS. USAF Academy, Colorado.* URL: https://apps.dtic.mil/sti/citations/AD1070618

6. Kshetri, Nir (2014). *Cybersecurity and International Relations: The U.S. Engagement with China and Russia.* Prepared for FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina, July 23–25. URL: http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf

7. Mueller, Milton (2013). Are we in a digital Cold War?, paper presented at the GigaNet workshop, '*The global governance of the internet: intergovernmentalism, multistakeholderism and networks'*, Graduate Institute, Geneva, 17 May 2013.

8. Nocetti, Julien (2015) Contest and conquest: Russia and global internet governance. *International Affairs*, 91 (1), January 2015, 111–130.

9. Risen, T. (2015). China, Russia Seek New Internet World Order. *US News and World Report*, 14.05.

10. Ristow, B. (2013). *The New Gatekeepers: Controlling Information in the Internet Age.* Center for International Media Assistance, 25 p.

11. Sadowsky, J., Zambrano, R., Dandjinou, P. (2004). *Intrenet Governance:* a Discussion Document: Prepared for the UN ICT Task Force. Nev-York.

12. Taylor, Emily, and Hoffmann, Stacie (2019). *EU–US Relations on Internet Governance. Chatham House.* URL: https://www.chathamhouse.org/publication/eu-us-relations-internet-governance.

13. Evdokimov, E. (2011). Politika Kitaja v global'nom iformacionnom prostranstve. *Mezhdunarodnye processy,* 1 (25).

14. Zinov'eva, Elena (2014). Mezhdunarodnoe sotrudnichestvo po obespecheniju informacionnoj bezopasnosti. *Pravo i upravlenie. XXI vek,* 1 (33), 44–52.

15. Karasev, P. A. (2015). *Politika bezopasnosti SShA v global'nom informacionnom prostranstve.* Avtoreferat dis. na soiskanie .... k.polit.n. po special'nosti 23.00.04. Moskva: IMJeMO RAN.

16. Krutskih, A. V. (2007). K politiko-pravovym osnovanijam global'noj informacionnoj bezopasnosti. *Mezhdunarodnye process,* 1 (5), 28–37.

17. Mozolina, O. V. (2006). SShA i mezhdunarodnoe soobshhestvo: bor'ba za upravlenie Internetom. *SShA i Kanada: jekonomika, politika, kul'tura*, 4, 111–119.

18. Sharikov, P. A. (2019). Podhody SShA, ES i Rossii k probleme informacionnoj bezopasnosti. *Sovremennaja Evropa*, 2, 73–83.

19. Global Freedom Status. Freedom House. https://freedomhouse.org/explore-the-map?type=fiw&year=2021.

20. Bendiek, A. (2012). European Cyber Security Policy. *SWP Research Paper,* No. 13. URL: http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paper-detail/article/european_cyber_security_policy.htm

21. Carrapico, Helena, Barrinha, André (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies,* 55 (6), November 2017, 1254–1272. URL: https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.12575

22. Ilves, l. K., Evans, t. J., Cilluffo, f. J., & Nadeau, a. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. *PRISM,* 6 (2), 126–141. URL: http://www.jstor.org/stable/26470452

23. Schaake, Marietje & Vermeulen, Mathias (2016). Towards a values-based European foreign policy to cybersecurity. *Journal of Cyber Policy,* 1:1, 75–84. DOI: 10.1080/23738871.2016.1157617

24. Kok, Ayse (2018). Conceptualizing Cyber-Security From EU Perspective. *In Proliferation of Open Government Initiatives and Systems*, 143–154.

25. Christou, George (2017). The EU's Approach to Cybersecurity. EU-Japan Security Cooperation: Challenges and Opportunities. University of Essex. Online paper series, Spring/Summer 2017. http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf

26. Bendiek, Annegret, Porter, Andrew L (2013). European Cyber Security Policy within a Global Multistakeholder Structure. *European Foreign Affairs Review,* 18 (2), 155–180. URL: https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/18.2/EERR2013011

27. *73/266. Advancing responsible State behaviour in cyberspace in the context of international security. Resolution adopted by the General Assembly on 22 December 2018.* URL : https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266

28. *EU Cyber Security strategy: An open, safe and secure Cyberspace,* 7 February, 2013. URL: https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

29. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS* A Digital Single Market Strategy for Europe /* COM/2015/0192 final */. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

30. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS* The European Agenda on Security. Strasbourg, 28.4.2015, COM(2015), 185 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

31. Shared Vision, Common Action:A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy, June 2016. URL: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

32. Haass, Richard (2020). Present at the Disruption. How Trump Unmade U.S. Foreign Policy. *Foreign Affairs,* September/October 2020. URL: https://www.foreignaffairs.com/articles/united-states/2020-08-11/present-disruption

33. Directive (EU)2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

34. *Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Publication 19 September 2017. URL: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu

35. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL *The EU's Cybersecurity Strategy for the Digital Decade. European Commission, Brussels,* 16.12.2020 JOIN(2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

36. *Revised Directive on Security of Network and Information Systems (NIS2). European Commission*, Publication 16 December 2020. URL: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2

37. *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities.* Brussels, 16.12.2020 COM(2020) 829 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

38. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. *European Commission,* 16 December 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

39. E*uropean Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade* (2021/2568(RSP)). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html

40. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital Compass: the European way for the Digital Decade. COM/2021/118 final.* URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

41. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats. European Commission.* Brussels, 6.4.2016 JOIN (2016) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

42. Wakefield, Jane (2021). AI emotion-detection software tested on Uyghurs. *BBC News,* 26 May. URL: https://www.bbc.com/news/technology-57101248

43. *Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report.* A/AC.290/2021/CRP.2, 10 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

44. *The future of discussions on ICTs and cyberspace at the UN.* Updated version: 10/08/2020. URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

45. *EU Action Plan on Human Rights and Democracy 2020–2024. Council of the European Union.* Brussels, 18 November 2020. URL: https://www.consilium.europa.eu/media/46838/st12848-en20.pdf

46. *EU Human Rights Guidelines on Freedom of Expression Online and Offline. Council of the European Union.* Brussels, 12 May 2014. https://www.consilium.europa.eu/media/28348/142549.pdf

47. *EU External Cyber Capacity Building Guidelines. Council of the European Union,* Brussels, 26 June 2018. URL: https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

48. *EU CyberNet – the bridge to cybersecurity expertise in the European Union.* URL: https://www.eucybernet.eu/

49. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission.* Brussels, 13.9.2017 JOIN(2017) 450 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

50. *EU CyberNet work in Dominican Republic, first national cybersecurity exercise «Cyber llamas».* EU CyberNet. 21.05.2021. URL: https://www.eucybernet.eu/eu-cybernet-work-in-dominican-republic-first-national-cyber-llamas-exercise/

51. *JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL, THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION.* URL: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

52. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* General editor Michael N. Schmitt (2013). Cambridge University Press.

53. *The Alliance.* URL: https://www.weprotect.org/alliance/

54. SPEECH/12/315 Cecilia Malmström. European Commissioner responsible for Home Affairs. The European Response to the rising Cyber Threat. *Transatlantic Cyber Conference organised by the Center for Strategic and International Studies, the European Security Roundtable and SRA International.* Washington, 2 May 2012. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_315

55. EU-U.S. Cyber Dialogue Bruxelles. EEAS. Press Release. 16/12/2016. URL: https://www.statewatch.org/media/documents/news/2016/dec/eu-eeas-eu-us-cyber-dialogue-pr-16-12-16.pdf

Матеріал надійшов до редакції 06.09.2021 р.