ISSN 2078–4333. Вісник Львівського університету. Серія міжнародні відносини. 2019. Випуск 46 С. 123–136
Visnyk of the Lviv University. Series International Relations. 2019. Issue 46. P. 123–136

УДК 327.7
DOI 10.30970/vir.2019.46.0.10365

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО В ГАЛУЗІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Оксана Фролова

Інститут міжнародних відносин
Київського національного університету імені Тараса Шевченка,
вул. Юрія Іллєнка, 36/1, м. Київ, Україна, 04119, тел. 044 481 4437,
e-mail: sancha279@ukr.net

Загрози у сфері інформаційної безпеки належать до найсерйозніших проблем сучасної системи світопорядку. Інформаційну та кібербезпеку розглядають як стратегічну проблему. Транскордонний характер загроз змушує країни світу тісно взаємодіяти між собою. Актори міжнародних відносин дійшли згоди, що лише спільними зусиллями та на основі міжнародного права можливо вирішити проблеми у політичній, економічній, безпековій та інших сферах життєдіяльності суспільства.

Особливою ефективністю вирізняється співпраця в рамках міжнародних організацій, які відзначаються більшим потенціалом для боротьби з загрозами в інформаційній сфері. Міжнародна спільнота в рамках міжнародних організацій та завдяки механізмам міжнародних організацій демонструє прагнення до масштабного співробітництва, об'єднання зусиль, взаємодії, спільної участі, відкритості та прозорості, відповідальності та інноваційності у вирішенні спільної проблеми безпечного світу. Стаття присвячена розгляду міжнародного співробітництва в галузі забезпечення інформаційної безпеки в рамках Організації Об'єднаних націй, Організації Північноатлантичного Договору та Європейського Союзу.

Ключові слова: інформаційна безпека; кібербезпека; міжнародне співробітництво; ООН; НАТО; ЄС.

Інформаційна безпека в загальній системі міжнародної безпеки посідає надважливе місце, оскільки нові виклики сучасного інформаційного світу спричинили появу нових способів ведення війни та новітніх загроз для світового порядку. Реалізація цих загроз спроможна завдати серйозної шкоди національній і міжнародній безпеці.

Сучасні виклики та загрози системі глобальної інформаційної безпеки зумовили переосмислення концептуальних і практичних засад міжнародного співробітництва у сфері інформаційної безпеки. Задля збереження безпеки та стабільності у сучасному світі необхідні єдині правила, принципи та норми

© Фролова Оксана, 2019

відповідальності. Вразливість, взаємопов'язаність, доступність та незахищеність суб'єктів міжнародних відносин притаманні системній кризі міжнародної інформаційної безпеки. Нагальним та актуальним є питання вироблення дієвих механізмів забезпечення міжнародної інформаційної безпеки [1].

Міжнародне співробітництво у сфері інформаційної безпеки зумовлює необхідність пошуку спільних рішень у межах міжнародних організацій щодо протидії інформаційним та кіберзагрозам, вироблення спільної стратегії інформаційної безпеки для протидії кібервійнам, інформаційному тероризму та інформаційній злочинності [2].

Міжнародне співтовариство дійшло згоди, що лише спільними зусиллями та на основі міжнародного права можливо вирішити проблеми у політичній, економічній, безпековій та інших сферах життєдіяльності суспільства.

Протягом минулого десятиліття зусилля у боротьбі з загрозою кіберзлочинності розглядали на міжнародному рівні, зокрема в рамках Шанхайської організації співробітництва, Організації американських держав, Форуму азійсько-тихоокеанського економічного співробітництва, Регіонального форуму Асоціації держав Південно-Східної Азії, Економічного співтовариства західно-африканських держав, Африканського союзу, Європейського Союзу, Організації з безпеки і співробітництва в Європі, Ради Європи, Організації Північноатлантичного договору, а також у формі двостороннього співробітництва держав [3].

Але першочергової уваги в галузі забезпечення міжнародної інформаційної безпеки заслуговує Організація Об'єднаних Націй, оскільки саме її діяльність поклала початок боротьбі з новітніми загрозами та звернула увагу світової громадськості на формування міжнародно-правової бази та організаційних механізмів для протидії міжнародним інформаційним загрозам. ООН була першою міжнародною організацією, яка розпочала боротьбу з очевидними негативними наслідками та загрозами розбудови інформаційного суспільства, такими як протиправне використання науково-технологічного прогресу терористичними угрупованнями. ООН завжди закликає світову громадськість до дво- та багатостороннього співробітництва та об'єднання зусиль, підтримки урядів країн, співпраці правоохоронних органів у спільній боротьбі для забезпечення міжнародної безпеки в інформаційній сфері. Ця діяльність у рамках ООН розпочата ще наприкінці XX століття, 1996 року.

Протягом наступних років ГА ООН прийняла низку Резолюцій в яких міститься заклик до держав-членів ООН сприяти розгляду на міжнародному рівні існуючих та потенційних угод у сфері інформаційної безпеки, розробити міжнародні принципи, спрямовані на укріплення глобальних інформаційних і телекомунікаційних систем та на боротьбу з інформаційним тероризмом і криміналом, використовувати науково-технічний прогрес на користь усього людства, щоб сприяти стійкому економічному і соціальному розвитку всіх держав і гарантувати міжнародну безпеку [4; 5; 6; 7].

ООН спонукала держави до висловлення своєї позиції та звітування щодо загальної оцінки міжнародної інформаційної безпеки та зусиль, які докладають

держави. Вже стало доброю традицією представляти офіційні позиції урядів держав у доповідях Генерального секретаря на сесіях ГА ООН. Мета таких звітів полягає у зміцненні міжнародної безпеки, в обміні досвідом та у сприянні міжнародному співробітництву. Питання кібербезпеки вийшли на рівень дипломатичних відомств і вищих керівників держав.

Багато країн зміцнило свою стратегію щодо захисту від новітніх кібернетичних, медійних або психологічних загроз. За останні декілька років чимало країн опублікувало або ж оновило свої стратегії щодо захисту від інформаційних загроз. Вони опублікували правила і закони, заснували спеціальні агентства, вдосконалили робочі механізми, запустили просвітницькі та освітні ініціативи в галузі інтернет-безпеки, сприяли поширенню культури безпеки в Інтернеті, наростили свій потенціал і зміцнили міжнародне співробітництво. Зокрема, для України забезпечення інформаційної безпеки належить до пріоритетних напрямів державної політики, що доводить прийняття РНБО України 2016 року Доктрини інформаційної безпеки України. Доктрина визначає національні інтереси в інформаційній сфері, цілі, завдання, принципи, напрями, пріоритети та механізми формування і реалізації державної інформаційної політики. Крім того, 2016 року прийнята Стратегія кібербезпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

На останній, 73-й сесії ГА ООН 5 грудня 2018 року прийнята Резолюція A/RES/73/27 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки». Основна мета – запуск широкої транспарентної політичної дискусії щодо протидії злочинності в інформаційній сфері, захист інтересів усіх країн у цифровій сфері, незалежно від того, на якому рівні технологічного розвитку вони знаходяться, пошук і формулювання відповіді на один з актуальних викликів сучасності. Резолюція спрямована на досягнення глобального консенсусу та вироблення конкретних практичних рішень у сфері боротьби з кіберзлочинністю в умовах відсутності дієвих міжнародно-правових інструментів. В ООН вперше створена робоча група з міжнародної інформаційної безпеки відкритого складу. В роботі групи зможуть брати участь всі, без винятку, держави-члени ООН. Підвищується статус дискусії з міжнародної інформаційної безпеки в ООН. На відміну від традиційної групи урядових експертів ООН, робоча група – це повноцінний орган Генасамблеї ООН, який може виробляти і рекомендувати державам-членам будь-які документи, навіть проекти міжнародних договорів. Положення резолюції викликали суперечності у довірі між державами та протистояння між поглядами на сучасну систему інформаційної безпеки держав-членів ООН, про що говорять результати голосування: за – 119, проти – 46, утрималось – 14 [8].

Окрім значних позитивних зрушень у нормативно-правовому та організаційному забезпеченні, ООН стала ініціатором проведення міжнародних конференцій, семінарів та зустрічей на вищому рівні. Яскравий приклад та важливий етап для розгляду питання міжнародної інформаційної безпеки – Всесвітня зустріч на вищому рівні з питань інформаційного суспільства (перший

етап – 2003 р., Швейцарія; другий етап – 2005 р., Туніс) та Всесвітня зустріч на вищому рівні з питань інформаційного суспільства ВСІС+10 (2015) під егідою ООН. Конференція запропонувала світовій спільноті розглянути існуючі та потенційні загрози для безпеки інформаційних і комунікаційних мереж, об'єднати зусилля держав-членів ООН, спрямовані на оцінку стану інформаційної безпеки, а також на перспективну розробку міжнародної конвенції з інформаційної безпеки. Підґрунтям для такого рішення стали відповідні положення підсумкових документів регіональних конференцій з підготовки Всесвітньої зустрічі, а саме – загальноєвропейської, азіатсько-тихоокеанської, африканської, західно-азійської та латиноамериканської, в яких закладено основу для подальшого обговорення проблематики міжнародної інформаційної безпеки на рівні ООН.

Проблематика міжнародної інформаційної безпеки увійшла до підсумкових документів женевської зустрічі ВСІС – Декларації принципів «Побудова інформаційного суспільства – глобальне завдання нового тисячоліття» та Плану дій. Зокрема, у Декларації принципів (розділ «Зміцнення довіри і безпеки при використанні ІКТ») зазначено, що міжнародна інформаційна безпека і безпека інформаційної інфраструктури є необхідною передумовою становлення глобального інформаційного суспільства та подолання асиметрії інформаційного розвитку. Зазначимо, що підвищення довіри і безпеки при використанні інформаційно-комунікаційних технологій, враховуючи їхню подвійну природу, визначається у документі як стратегія глобальної культури кібербезпеки, що має забезпечуватися за допомогою міжнародного співробітництва усіма зацікавленими сторонами і компетентними міжнародними організаціями. Такі зусилля, на думку міжнародних експертів з проблем інформаційної безпеки, повинні спиратися на широке представництво у розробленні міжнародно-правового документа інформаційно розвинених та інформаційно бідних країн для забезпечення рівності, суверенності та доступу до глобальних інформаційних ресурсів, що зумовлює захист приватного життя і прав людини, транскордонного співробітництва у сфері економіки, торгівлі, культурних обмінів та соціальних гарантій. Політичним підсумком обговорення проблеми міжнародної інформаційної безпеки на форумі ВСІС стало визнання принципів загального і недискримінаційного доступу до високих технологій для всіх націй, підтримка діяльності ООН, спрямованої на забезпечення міжнародного миру і стабільності, запобігання застосуванню інформаційних озброєнь, здатних негативно вплинути на територіальну цілісність, інфраструктуру та масову свідомість будь-якої держави [9].

Проблема інформаційної безпеки в контексті формування глобального інформаційного суспільства стала актуальною для діяльності спеціалізованих установ ООН, зокрема, ЮНЕСКО та МСЕ, враховуючи гуманітарні та технічні програми та проекти організацій. Наприклад, ефективним та інформативним є щорічний Глобальний індекс кібербезпеки (GCI), який є ініціативою Міжнародного союзу електрозв'язку. Оскільки кіберзлочинність – глобальна проблема, яка не обмежується національними кордонами, а боротьба з

кіберзлочинністю вимагає багатостороннього підходу із залученням усіх учасників, включаючи двосторонні та багатосторонні угоди, участь у міжнародних форумах, то одним із п'яти базових складових Глобального індексу кібербезпеки є міжнародне співробітництво. Співробітництво може сприяти розвитку значно сильніших можливостей забезпечення кібербезпеки, що допомагає стримувати небезпечні онлайн-загрози. Виходячи із показників індексу 2018 року, у топ 5 увійшли Великобританія, США, Франція, Литва, Естонія та Сінгапур. Україна посіла 54 місце із 175 [10].

ООН активно включилася у процес сприяння глобальному розвитку та побудові безпечного світового суспільства. Тема міжнародної співпраці в питаннях забезпечення міжнародної безпеки взагалі та інформаційної безпеки зокрема стала гострою та актуальною у сучасному світі. Міжнародна спільнота у рамках ООН та завдяки механізмам ООН демонструє прагнення до масштабного співробітництва, об'єднання зусиль, взаємодії, спільної участі, відкритості та прозорості, відповідальності та інноваційності у вирішенні спільної проблеми безпечного світу [1].

Організація Північноатлантичного договору (НАТО) створена з метою захисту свободи і безпеки країн-членів політичними та військовими засобами на основі статті 51 Статуту ООН. НАТО підтримує невід'ємне право незалежних держав на індивідуальну або колективну оборону.

Вперше питання інформаційної та кібербезпеки в рамках НАТО піднімали на Празькому саміті 2002 р., згодом – на Ризькому саміті 2006 р., коли лідери країн Альянсу визнали необхідність захисту інформаційних систем в умовах стрімкого прогресу інформаційно-комунікаційних технологій та вдосконалення політики щодо кібербезпеки. Фактично визнали, що розробка та використання руйнівних кіберінструментів, які можуть загрожувати національній та євроатлантичній безпеці, потребують стратегічних змін щодо нової політики інформаційної безпеки у трансатлантичному вимірі.

У форматі НАТО розроблено основні заходи щодо кібербезпеки, які передбачали:

1. Координацію та надання рекомендацій щодо кібербезпеки: тобто, політика кібербезпеки здійснюється політичними, військовими та технічними департаментами НАТО, а також окремими країнами-членами. Основним аспектом такої політики є формування департаменту управління кібернетичною безпекою, який відповідатиме виключно за узгодження діяльності у сфері кібербезпеки в межах організації і яким керує Комісія, що відповідає за кібербезпеку. Комісія є основним консультативним інститутом Північноатлантичної ради з кібербезпеки та надає рекомендації країнам-членам організації з усіх аспектів кібербезпеки та входить до складу управління нових викликів для безпеки при штаб-квартирі НАТО.

2. Надання допомоги окремим країнам-членам НАТО. Унаслідок атак, спрямованих проти державних органів та здійснених за допомогою мережі Інтернет, увагу НАТО розширено на питання кібербезпеки окремих країн-членів і розроблено механізми надання допомоги для захисту комунікаційних систем

союзникам, включаючи групи швидкого реагування на протидію кіберзагрозам. Проте основна роль у захисті та безпеці комунікаційних систем країн-членів НАТО відводиться союзним державам, тому НАТО співпрацює з національними інститутами щодо розробки принципів і критеріїв забезпечення кібербезпеки там, де національні мережі та мережі НАТО взаємозв'язані.

3. Наукові дослідження та підготовка. Передовий центр НАТО з кібербезпеки (Таллінн, Естонія) з 2008 р. здійснює наукові дослідження та підготовку з проведення операцій у віртуальному просторі. Полігон створено на базі центру кібербезпеки сил оборони Естонії, на якому вже проводили міжнародні навчання, які передбачали відпрацювання як індивідуальних, так і командних навичок у віртуальному кіберсередовищі. На базі центру здійснюють підготовку експертів і провадять різні тренування у сфері безпеки інформаційних систем.

4. Співпрацю з партнерами. НАТО розвиває практичне співробітництво з кібербезпеки відповідно до «Рекомендацій щодо співпраці з кібербезпеки з партнерами та міжнародними організаціями», ухвалених 2008 р. та «Рамок співпраці з кібербезпеки між НАТО та країнами-партнерами», ухвалених 2009 р. та за підтримки Комітету з планування використання цивільних систем зв'язку, Передового центру з кібербезпеки (Естонія), Передового центру по боротьбі з тероризмом (Туреччина), а також програми НАТО «Наука заради миру та безпеки». Передовий центр НАТО з кібербезпеки провів експертні переговори, виявляв факти, проводив навчальні семінари та обміни інформацією з зацікавленими партнерами та міжнародними організаціями, зокрема з Європейським Союзом та Організацією з безпеки та співробітництва в Європі [11].

На Лісабонському саміті НАТО 2010 р. вирішено розробити нову політику НАТО з кібербезпеки, а також розробити конкретний план дій, який набув чинності з червня 2011 р. У Стратегічній концепції та декларації Лісабонського саміту чітко зазначено, що швидкий розвиток та постійне ускладнення кібератак зумовлюють нагальний захист інформаційно-комунікаційних систем країн-членів НАТО, від якого водночас залежить безпека організації. Альянс не виключає необхідності швидкого реагування на кібератаки шляхом надсилання групи експертів до будь-якої країни-члена, що постраждала від кіберагресії, або до країни, яка відчуває загрозу вторгнення в її інформаційне середовище. У зв'язку з ухваленням в Лісабоні нової Стратегічної концепції НАТО, яка стосується місії Альянсу в кіберпросторі, 10–11 жовтня 2011 р. в Кембриджі (Велика Британія) проведено семінар за участю 40 експертів з країн-членів і партнерів НАТО, на якому обговорювали: нові загрози для безпеки в кіберпросторі; командування і управління в кіберпросторі; порушення безпеки Інтернету; кіберризики і готовність приватного сектора; убезпечення нового покоління Інтернету; урядування в кіберпросторі – право і міжнародну співпрацю. Більшість аналітиків у сфері безпеки визнали важливість кібербезпеки і розглядають безпеку інформаційного середовища на одному рівні з традиційними проблемами НАТО. Оскільки кібератаки здійснюють анонімно і

їх легко заперечувати, зазначено у дискусіях, вони мають надзвичайно сприятливе співвідношення витрат і вигод, порівняно зі звичайними військовими операціями.

У комюніке за результатами Варшавського саміту, виданого главами держав і урядів, що брали участь у засіданні Північноатлантичного альянсу у Варшаві у липні 2016 року, один із найбільших пунктів присвячено кібербезпеці. Кібернапади є значним викликом безпеці Альянсу і можуть бути настільки ж шкідливими, як і звичайні напади. Кіберзахист є частиною основного завдання НАТО щодо колективної оборони. Наріжним каменем саміту у Варшаві стало визнання кіберпростору сферою діяльності, в якій Альянс повинен захищатися так само ефективно, як у повітрі, на суші і на морі. Останнім часом кібератаки стали інформаційною складовою гібридної війни, тому НАТО і його союзники для виконання основних завдань Альянсу – колективної оборони, кризового управління і безпеки – мають бути готовими захищати свої мережі та операції від зростаючих кіберзагроз і атак. НАТО підписала Технічну угоду про співпрацю з кібероборони з ЄС, зокрема щодо обміну інформацією, підготовки кадрів, наукових досліджень і тренувань. Оновлену стратегію з протидії гібридним загрозам ухвалили і міністри закордонних справ на рівні НАТО. Як повідомив на спільній прес-конференції з високим представником ЄС з питань зовнішньої політики і політики безпеки Ф. Могеріні Генеральний секретар Альянсу Є. Столтенберг, Організація Північноатлантичного договору підтримала рішення щодо посилення співпраці між ЄС і НАТО, визначила параметри гібридної війни та її загрози для європейської безпеки, звернула увагу на кризу в Україні і на подальші відносини з Росією [12].

Центр реагування на комп'ютерні інциденти НАТО (NCIRC), що базується в Бельгії, захищає власні мережі НАТО, забезпечуючи централізовану та цілодобову підтримку кібербезпеки різним сайтам НАТО. Очікують, що цей потенціал розвиватиметься на постійній основі, щоб підтримувати безпеку серед зростаючих загроз та технологічних інновацій.

У Фінляндії (Гельсінкі) 2017 р. відкрито Європейський центр з протидії гібридним загрозам. Центр, створений 12 країнами ЄС і НАТО, повинен допомогти країнам у протидії новим загрозам, націленим на дестабілізацію держави. В діяльності центру бере участь 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, Німеччина, Великобританія, Іспанія, Польща, Естонія, Латвія і Литва. Створений у Фінляндії Європейський центр з протидії гібридним загрозам став платформою для співпраці між ЄС і НАТО в галузі забезпечення інформаційної безпеки. Європейський центр передового досвіду для протидії гібридним загрозам є центром практиків і експертів, які розбудовують можливості держав-членів і посилюють співпрацю між ЄС і НАТО у протидії гібридним загрозам. Згодом до центру приєдналися Канада, Австрія, Чехія, Данія, Італія, Нідерланди, Румунія. Можливо, в майбутньому для співпраці приєднаються й інші країни [13].

Кіберзахист інтегрований також в ініціативи інтелектуальної оборони НАТО (NATO’s Smart Defence). Розумна оборона дає змогу країнам-членам

співпрацювати над розвитком і підтримкою можливостей, які вони не можуть дозволити собі розробити або закупити окремо, а також звільнити ресурси для розвитку інших можливостей. Проекти інтелектуальної оборони в кіберзахисті містять платформу для обміну інформацією про зловмисне програмне забезпечення, розробку багатофункціональних можливостей для оборонних засобів та багатонаціональний проект з освіти та навчання. НАТО проводить регулярні навчання, такі як щорічні навчання з кібер-коаліції, і прагне інтегрувати елементи з кіберзахисту на повний спектр навчань Альянсу, зокрема щорічні навчання з управління кризами.

У Таллінні 2017 року створено експертний Центр зі спільної кібероборони Організації Північноатлантичного договору, в якому брала участь 21 держава-член. Центр є акредитованим НАТО навчальним центром, який займається освітою з кіберзахисту, консультаціями, дослідженнями і розробками. Завдання Центру полягає в підтримці країн-членів та НАТО з унікальним міждисциплінарним досвідом у сфері кіберзахисту, сприянні співпраці однодумців, об'єднанні членів НАТО і партнерів за межами Альянсу. Експертний Центр зі спільної кібероборони є акредитованим центром НАТО з кіберзахисту [14].

До прикладів освітніх та навчальних проектів НАТО можна зачислити школу НАТО з комунікаційних та інформаційних систем в Латіні (Італія), яка проводить навчання персоналу країн-членів Альянсу (а також країн, які не є членами НАТО), пов'язаних з функціонуванням та підтримкою інформаційних систем НАТО. Школа НАТО в Обераммергау (Німеччина), здійснює освіту та навчання з кіберзахисту для підтримки операцій, стратегій та політики Альянсу. Оборонний коледж НАТО в Римі (Італія), розвиває стратегічне мислення щодо військово-політичних питань, у тому числі з питань кіберзахисту.

На саміті НАТО в Брюсселі 2018 року активно обговорювали питання інформаційної безпеки. Союзники погодилися створити новий центр операцій у сфері кіберпростору як частину посиленої командної структури НАТО. Вони також погодилися, що НАТО може використовувати національні кібернетичні можливості для своїх місій і операцій. До того ж, НАТО докладає зусиль для забезпечення належного поєднання військового і цивільного потенціалу, щоб бути в змозі реагувати на новітні загрози безпеці, такі як гібридна війна.

Оскільки кіберзагрози кидають виклик державним кордонам, НАТО взаємодіє з країнами та організаціями з метою зміцнення міжнародної безпеки. Взаємодія з країнами-партнерами базується на спільних цінностях та спільних підходах до кіберзахисту. Запити про співпрацю з Альянсом обробляють в індивідуальному порядку на основі взаємного інтересу. НАТО також активно співпрацює з Європейським Союзом (ЄС), Організацією Об'єднаних Націй (ООН) та Організацією з безпеки і співробітництва в Європі (ОБСЄ). НАТО і ЄС обмінюються інформацією та передовим досвідом між групами реагування на кібер-загрози. Також розширюється співпраця в галузі навчання, досліджень і освіти [15].

Кіберзахист є однією зі сфер посиленої співпраці між НАТО і Європейським Союзом, як частина координованих зусиль організацій щодо протидії гібридним загрозам. НАТО та ЄС активно обмінюються інформацією та досвідом з метою протидії загрозам в інформаційній сфері.

Реалізація спільної політики безпеки та оборони ЄС вимагає постійних потужних зусиль для кіберзахисту, щоб підтримувати структури, місії та операції в рамках спільної політики безпеки та оборони ЄС.

Концепція інформаційної безпеки ЄС зумовлює пошук спільних рішень щодо протидії інформаційним та комунікаційним загрозам, визначає пріоритетами діяльності безпекових інституцій вироблення загальної стратегії європейської інформаційної безпеки, протидії кібервійнам, інформаційному тероризму та боротьби з інформаційною злочинністю.

Пріоритетного значення ЄС завжди приділяв забезпеченню захисту приватного життя і персональних даних. Ці ініціативи почали набувати своєї актуальності ще з 1995 р. Чимало ініціатив Європейського Союзу спрямовано на створення відповідної правової основи і встановлення інституційних та організаційних механізмів забезпечення інформаційної безпеки (Директиви Європейського парламенту і Європейської ради 95/46/ЕС від 24 жовтня 1995 р. і 2002/58/ЕС від 12 липня 2002 р., Директиви 2002/20/ЄС, 2002/21/ЄС, 2002/22/ЄС від 7 березня 2002 р., Регламент Європейського парламенту і Європейської ради від 18 грудня 2000 р., Рекомендація Європейської ради від 25 червня 2001 р., Резолюція Європейської ради від 18 лютого 2003 р. і т. д.), в яких зафіксовано визначення нових загроз для демократії, прав людини і систем державного управління, оскільки високотехнологічні загрози характеризуються ознаками системно організованих впливів щодо державних та комерційних структур ЄС [11].

У грудні 2000 р. на базі відповідних директив прийняті Правила Європейського парламенту і Європейської ради ЄС про захист персональних даних в умовах автоматизованої обробки та транскордонному їхньому переміщенні органами й установами Європейського Співтовариства (№ 45/2001). Вони орієнтовані на захист фундаментальних прав і свобод фізичних осіб, передусім прав на недоторканність приватного життя, на визначення прав і обов'язків у зв'язку зі збереженням, обробкою і використанням, у тому числі передачею і розкриттям, таких даних, а також передбачають відповідальність за порушення цих зобов'язань.

Одним із останніх досягнень ЄС у галузі захисту даних є прийнятий Європейським парламентом у травні 2018 р. новий регламент GDPR (General Data Protection Regulation). GDPR містить 99 статей і, по суті, є вдосконаленою інтерпретацією Директиви 1995 року. Дія документа не лімітована рамками Євросоюзу, а поширюється на всі організації, що мають справу з даними громадян ЄС. Основна мета GDPR полягає в гарантії захисту персональних даних громадян ЄС без прив'язки до того, на території якої країни вони зберігаються. Також новий регламент покликаний гармонізувати закони про конфіденційність даних по всій Європі. Важливо те, що GDPR не зобов'язує

компанії впроваджувати будь-які конкретні прийоми і методи захисту даних. Організації можуть самостійно обирати систему забезпечення безпеки внутрішніх даних. Головне – кінцевий результат – надійний захист персональних даних. Основна вимога до компаній, які працюють з даними громадян ЄС, – ретельно захищати конфіденційність цих даних [16].

Кібербезпека – один із пріоритетних напрямів, який регламентується та регулюється в рамках ЄС. Європейська Конвенція про кіберзлочинність (2001) прийнята за активної підтримки ЄС, який визнав її базовим документом, спрямованим на розвиток національного законодавства та активізацію європейського права в цій галузі з метою захисту суспільства від кіберзлочинності.

Європейська Рада ЄС у травні 2001 р. прийняла резолюцію «План дій «Електронна Європа»: мережева та інформаційна безпека», а в січні 2002 р. – резолюцію про єдиний підхід і конкретні дії у галузі інформаційної безпеки. Вона закликає держави-члени ЄС активізувати проведення освітніх програм з метою підвищення обізнаності про інформаційну безпеку, проводити обмін досвідом в галузі управління безпекою і зміцнювати діалог ЄС з іншими міжнародними організаціями в цій галузі.

Результатом плідної роботи Європейської Комісії в цьому напрямку стала стратегія щодо зміцнення кібербезпеки (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace), прийнята у лютому 2013 р. Основною метою стратегії кібербезпеки ЄС визначено підвищення стійкості і нарощування потенціалу в сфері кібербезпеки держав-членів ЄС, що передбачало посилення боротьби з кіберзлочинністю, формування ефективної інфраструктури забезпечення безпеки, розробку принципів міжнародної політики у сфері кібербезпеки тощо. Для досягнення цієї мети Комісія передбачала розвивати промислові ресурси і технології у сфері кібербезпеки, а також збільшити фінансування цієї сфери на рівні ЄС. Європейська Комісія також представила проект Директиви ЄС, спрямований на реалізацію стратегії, в якій, зокрема, передбачається, що країни-члени ЄС повинні будуть розробляти і затверджувати національні стратегії мережевої та інформаційної безпеки, створювати національні органи в цій сфері з відповідними фінансовими ресурсами для забезпечення їх роботи [17].

У вересні 2014 р Координаційна група з кібербезпеки, Європейська комісія стандартизації (CEN), Європейський комітет електротехнічної стандартизації (CENELEC), Європейський інститут телекомунікаційних стандартів (ETSI) опублікували рекомендації щодо цифрової безпеки (Recommendations for a Strategy on European Cyber Security Standardisation), розроблені у розвиток Європейської стратегії кібербезпеки. Рекомендації містять пропозиції Координаційної групи з кібербезпеки, систематизовані за трьома критеріями: управління, узгодження і глобальний вимір. При цьому Агентство рекомендує не тільки узгодити використання ключових термінів у сфері кібербезпеки («кібербезпека», «безпека мереж та інформації», «кіберзлочинність» тощо), оскільки це призводить до різної їх інтерпретації в державах-членах ЄС, але й

розробити узгоджене розуміння взаємозалежності та моделей управління в цих трьох сферах.

До речі, Європейські організації зі стандартизації (CEN, CENELEC та ETSI), створили в 2011 році групу з координації кібербезпеки для надання стратегічних консультацій щодо стандартизації в галузі інформаційної безпеки, мережевої та інформаційної безпеки (NIS) та кібербезпеки (CS). Ще 2016 року групу перетворили у єдину фокус-групу з кібербезпеки CEN-CENELEC. Цього ж року фокус-група розглянула різні способи використання значення слова «кібербезпека» в різних стандартах і завершила роботу над документом «Визначення кібербезпеки», що складається з огляду непорозумінь та прогалин у визначеннях. Це стало суттєвим кроком до єдиного розуміння поняття «кібербезпека» [18].

Оновлена «Стратегія спільної безпеки і оборони ЄС 2015» визначає необхідність вироблення програми європейської інформаційної безпеки, протидії кібервійнам, інформаційному тероризму та кіберзлочинності. За планом дій передбачено здійснення стратегічного планування щодо протидії інформаційним загрозам у співробітництві з Радою Безпеки ООН; встановлення стратегічного партнерства у сфері кібербезпеки з провідними міжнародними акторами; трансформації нормативної бази ЄС з інформаційної безпеки шляхом ухвалення конвенцій, директив, рекомендацій та резолюцій про європейську інформаційну безпеку та конфіденційність електронних комунікацій; визначення та оцінка інформаційних і кіберзагроз для критично важливих сфер життєдіяльності європейського співтовариства загалом і для національних спільнот зокрема; розробка положень європейської та національної політики інформаційної безпеки і зростання ролі ЄС у забезпеченні регіональної інформаційної безпеки. Стратегія ЄС 2015 р. містить положення про необхідність подолання інформаційної асиметрії між країнами ЄС, запобігання конфліктам у Європейському регіоні із застосуванням інформаційних озброєнь, забезпечення основних прав і свобод людини в інформаційному суспільстві, протидії інформаційним впливам, що спрямовані на моральні цінності європейських спільнот [11].

Окрім перелічених організацій важливою структурно-організаційною ланкою з забезпечення кібербезпеки ЄС є Європейське агентство мережевої та інформаційної безпеки (ENISA), засноване 2004 року. Агентство розташоване в Греції та є експертним центром з кібербезпеки в Європі. Основна мета Європейського агентства мережевої та інформаційної безпеки – сприяння розвиткові культури безпеки мереж та інформації в Європейському Союзі, підтримка загальноєвропейського співробітництва, обмін передовим досвідом, підвищення поінформованості і здійснення консультування з питань дослідницької програми Європейської комісії в контексті осмислення ризиків і загроз. ENISA та Європейська комісія організовують міжнародні конференції з питань підготовки стандартизації кібербезпеки і закону про кібербезпеку. В березні 2019 року агентство святкувало 15 річчя плідної та ефективної роботи з укріплення інформаційної безпеки в Європі [19].

Європол спільно з Європейською комісією та державами-членами ЄС заснував 2010 року Оперативну групу з кіберзлочинності Європейського Союзу (EUCTF). До складу EUCTF входять глави національних груп з кіберзлочинності різних країн-членів, а також представники Європолу та Європейської комісії. EUCTF – заснована на довірі мережа, яка збирається двічі рази на рік у Європолі і надає форум для керівників підрозділів з кіберзлочинності країн-членів ЄС разом з EUROPOL, CEPOL, EUROJUST і DG HOME для визначення та обговорення пріоритетних завдань та дій у боротьбі з кіберзлочинністю. EUCTF працює над тим, щоб зробити кіберпростір безпечним місцем для громадян, організацій, підприємств та урядів ЄС. Він також спрямований на надання допомоги Європолу та державам-членам у розробці та погодженні пріоритетів ЄС щодо підходу до боротьби з кіберзлочинністю [20].

Європейський Союз бере участь у Форумі Груп реагування на надзвичайні ситуації в комп'ютерній галузі шляхом функціонування європейської цільової групи сприяння співробітництву між Групами реагування на надзвичайні ситуації в комп'ютерній галузі. ЄС створив постійну групу реагування на комп'ютерні інциденти CERT-EU 2012 року. Команда налічує експертів з інформаційної безпеки з основних інститутів ЄС, тісно співпрацює з іншими CERT командами у державах-членах і за їхніми межами, а також зі спеціалізованими компаніями у сфері інформаційної безпеки.

ЄС 2010 року запровадив чотирирічну політичну програму для посилення зусиль у боротьбі з серйозною міжнародною та організованою злочинністю (EMPACT). Програма вимагає ефективної співпраці між правоохоронними органами, іншими агентствами та інституціями ЄС. Зокрема, 2017 року вирішено продовжити програму ЄС щодо організованої та міжнародної злочинності на період 2018–2021 рр. Цей багаторічний політичний цикл, спрямований на усунення найважливіших загроз, що створює організована злочинність для ЄС. Серед пріоритетних цілей: припинення злочинної діяльності, пов'язаної з атаками на інформаційні системи, зокрема тих, які слідують бізнес-моделі «Злочин як послуга»; боротьба з сексуальним насильством над дітьми, в тому числі виробництво і розповсюдження матеріалів про жорстоке поводження з дітьми; переслідування злочинців, причетних до шахрайства і підробки негрошових платіжних засобів, включаючи великомасштабне шахрайство з платіжними картами... [21].

Інформаційну та кібербезпеку ЄС розглядають як стратегічну проблему, яка стосується всіх країн-членів зокрема та ЄС загалом.

Транскордонний характер інформаційних загроз змушує країни світу тісно взаємодіяти між собою. Особливою ефективністю вирізняється співпраця у рамках міжнародних організацій, які мають більший потенціал для боротьби з загрозами в інформаційній сфері, систему швидкого реагування на виникаючі загрози, на базі яких можна обмінюватися досвідом та приймати рішення глобального характеру. В умовах швидкого розвитку ІКТ та кіберзагроз, що не обмежуються національними рамками, необхідна міжнародна співпраця за

участю багатьох зацікавлених сторін, щоб бути в курсі поточних подій і постійно мінливих вимог цифрової сфери.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Веб-сайт Європейського агентства мережевої та інформаційної безпеки https://www.enisa.europa.eu/about-enisa.
2. Глобальний індекс кібербезпеки 2018 р. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.
3. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Доклад Генерального секретаря. Добавление. 3 октября 2001 г. [Электронный ресурс]. – Режим доступа : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/561/59/PDF/N0156159.pdf?OpenElement.
4. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Доклад Генерального секретаря ООН. 10 июля 2000 г. [Электронный ресурс]. – Режим доступа : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/535/04/PDF/N0053504.pdf?OpenElement.
5. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция ГА ООН № 53/70 [Электронный ресурс] // Организация Объединенных наций. – Режим доступа : http://daccess-ddsny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement.
6. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция ГА ООН № A/73/27 [Электронный ресурс] // Организация Объединенных наций. – Режим доступа : https://undocs.org/ru/A/RES/73/27.
7. Кіберзахист. https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en.
8. *Макаренко Є. А.* Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст /Актуальні проблеми міжнародних відносин. Випуск 102 (Частина І), 2011.
9. Міжнародна інформаційна безпека: теорія і практика : підручник. – Київ : Центр вільної преси, 2016. – С. 416.
10. Роль науки и техники в контексте международной безопасности и разоружения: Резолюция ГА ООН № 54/50, 1 декабря 1999 г. [Электронный ресурс]. – Режим доступа : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/21/PDF/N9977721.pdf?OpenElement.
11. Стратегічне партнерство в міжнародних відносинах : монографія. – Київ : Вадекс, 2018, С. 541.
12. *Фролова О. М.* Роль ООН в системі міжнародної інформаційної безпеки Електронне видання Інституту міжнародних відносин «Міжнародні відносини. Серія: Політичні науки», № 18 (2018).
13. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
14. European standardization https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx.
15. EU POLICY CYCLE – EMPACT. – https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.
16. European Union CYBERCRIME TASK FORCE https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf.
17. NATO Warsaw Summit Communiqué, 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
18. The European Centre of Excellence for Countering Hybrid Threats https://www.hybridcoe.fi/.
19. The NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/.
20. World Summit on the Information Society (WSIS) [Electronic resource]. – Access mode : http://www.itu.int/net/wsis.

21. 2018 reform of EU data protection rules https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

Стаття надійшла до редколегії 10.04.2019
Прийнята до друку 20.04.2019

INTERNATIONAL COOPERATION IN THE SPHERE OF INTERNATIONAL SECURITY

Oksana Frolova

Institute of International Relations,
Taras Shevchenko National University of Kyiv,
36/1, Y. Illienka Str., Kyiv, Ukraine, 04119, tel.044 481 4437,
e-mail: sancha279@ukr.net

Threats in the field of information security are among the most serious problems of the modern system of world order. Information and cybersecurity are being considered as a strategic issue. The transboundary nature of threats makes the countries of the world closely interact with each other. The actors of international relations agreed that only joint efforts and on the basis of international law can solve problems in the political, economic, security and other spheres of society life.

Especially effective is cooperation within different international organizations that have greater potential to deal with threats in the information sphere. Through the international organizations and through the mechanisms of international organizations, the international community demonstrates a desire for large-scale cooperation, united efforts, collaboration, joint participation, openness and transparency, responsibility and innovation in solving the common problem of a secure world. The article is devoted to consideration of international cooperation in the field of information security within the United Nations, the North Atlantic Treaty Organization and the European Union.

Key words: information security; cybersecurity; international cooperation; the UN; NATO; EU.