УДК 342.951

ПОЛЯКОВ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org /0000-0002-8984-1476.

АКТИВІЗАЦІЯ МІЖНАРОДНОЇ СПІВПРАЦІ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ШЛЯХИ УДОСКОНАЛЕННЯ В РЕАЛІЯХ СЬОГОДЕННЯ

Анотація. *Визначено стратегічні основи міжнародного співробітництва України у сфері кібербезпеки. Узагальнено завдання міжнародної взаємодії у сфері кібербезпеки. Проаналізовано міжнародні ініціативи, які впроваджуються з метою посилення захисту кіберпростору. Деталізовано напрямки здійснення модернізації політики інформаційної безпеки на рівні ООН. Окреслено ключові пріоритети міжнародного співробітництва у сфері забезпечення кібербезпеки між Україною та НАТО. Розглянуто перспективи діяльності в Україні Трастового фонду з кібербезпеки НАТО. Обґрунтовані сучасні світові тенденції, які впливають на безпекову політику НАТО і вимагають вжиття відповідних заходів реагування. На підставі узагальнення визначено шляхи удосконалення міжнародної співпраці у сфері забезпечення кібербезпеки.*

Ключові слова: *гібридна загроза, міжнародне співробітництво, сектор безпеки і оборони, інформаційна безпека, кібербезпека, кіберзагроза, кібератака, кіберзахист, кіберпростір, державна зовнішня політика, інформаційно-комунікаційні технології, НАТО, ООН.*

Summary. *The strategic bases of Ukraine's international cooperation in the field of cybersecurity have been identified. The tasks of international cooperation in the field of cybersecurity are generalized. The international initiatives implemented to strengthen the protection of cyberspace are analyzed. The directions of information security policy modernization at the UN level are detailed. The key priorities of international cooperation in the field of cybersecurity between Ukraine and NATO are outlined. Prospective activities of the NATO Cyber Security Trust Fund in Ukraine are considered. Modern world trends that affect NATO's security policy and require appropriate response measures are substantiated. On the basis of generalization, the directions to improve international cooperation in the field of cybersecurity have been identified.*

Keywords: *hybrid threat, international cooperation, security and defense sector, information security, cybersecurity, cyberthreat, cyberattack, cyberdefense, cyberspace, state foreign policy, information and communication technologies, NATO, UN.*

Аннотация. *Определены стратегические основы международного сотрудничества Украины в сфере обеспечения кибербезопасности. Обобщены задачи международного взаимодействия в сфере кибербезопасности. Проанализированы международные инициативы, которые внедряются с целью усиления защиты киберпространства. Детализированы направления осуществления модернизации политики информационной безопасности на уровне ООН. Очерчены ключевые приоритеты международного сотрудничества в сфере обеспечения кибербезопасности между Украиной и НАТО. Рассмотрены перспективы деятельности в Украине Трастового фонда по кибербезопасности НАТО. Обоснованы современные мировые тенденции, которые влияют на политику безопасности НАТО и требуют осуществления соответствующих мер реагирования. На основании обобщения определены направления усовершенствования международного сотрудничества в сфере кибербезопасности.*

Ключевые слова: *гибридная угроза, международное сотрудничество, сектор безопасности и обороны, информационная безопасность, кибербезопасность, киберугроза, кибератака, киберзащита, киберпространство, государственная внешняя политика, информационно-коммуникационные технологии, НАТО, ООН.*

Постановка проблеми. Активне впровадження сучасних цифрових технологій в економіці, соціальній сфері, управлінні, кредитно-банківській діяльності, безпеці та обороні, стрімкий розвиток інформаційно-телекомунікаційних технологій (далі – ІКТ) на основі використання глобальної інформаційної мережі Інтернет і спрощення доступу до неї широкого кола користувачів, зумовили зростання чисельних ризиків та загроз саме для кібербезпеки та її складових. Тобто ІКТ є важливою складовою майже усіх сфер існування людини й громадянина та провокують потребу комплексного міжгалузевого врегулювання їх захисту. В умовах тотальної глобалізації та стрімкого розвитку ІКТ жодна держава світу самостійно не здатна забезпечити надійного захисту свого цифрового простору та гарантувати кібербезпеку. Однак процес формування моделі міжнародної системи забезпечення кібербезпеки триває досить повільно та має непередбачуваний характер, що значно підвищує значимість розвитку двостороннього та багатостороннього співробітництва у питаннях вироблення єдиного стратегічного курсу з метою спільного запобігання сучасним кіберзагрозам гібридного характеру. Часом перевірено та доведено, що позитивний ефект міжнародного співробітництва полягає у підвищенні рівня кібербезпеки, при цьому цілеспрямовані спільні дії двох або більше держав, державних об'єднань (альянсів) у питаннях протидії кіберзагрозам дають змогу значно обмежити конфліктогенний потенціал агресивно налаштованих у кіберпросторі держав (РФ, КНР, Північна Корея), значно знизити їх деструктивний вплив на глобальну світову систему та її регіональні підсистеми. На цьому фоні важливим напрямом зовнішньої безпекової політики будь-якої держави світу виступає саме міжнародне співробітництво та перспективи його розвитку й удосконалення.

Україна є повноцінним членом глобальної системи безпеки, пріоритетами для якої залишаються розвиток міжнародного партнерства й співробітництва у сфері забезпечення кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглиблення тісної співпраці України з НАТО з метою підвищення спроможностей України у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри в кіберпросторі тощо. Україна відповідно до укладених нею міжнародних договорів проводить виважену державну політику у сфері вдосконалення співробітництва у сфері кібербезпеки. Враховуючи глобальну цифровізацію, зростання обсягів транснаціональної кіберзлочинності, загрозливі тенденції динамічного поширення кіберзагроз у світовому масштабі для України актуальним вбачається уточнення напрямків подальшого міжнародного співробітництва щодо посилення спроможностей України у сфері забезпечення кібербезпеки.

Результати аналізу наукових публікацій. Проблемні питання щодо пошуку оптимальної моделі розвитку та посилення міжнародного співробітництва у сфері забезпечення кібербезпеки перебували у фокусі уваги таких науковців: М. Гребенюка [1], С. Демедюка [2], В. Маркова [3], А. Марущака [4], Р. Лук'янчука [5], Є. Скулиша [6], В. Шемчука [7]. Аналіз опублікованих наукових праць вказаних фахівців переконливо засвідчує, що в сучасних умовах саме кібербезпека та її забезпечення для України мають стати одним з ключових пріоритетів міжнародної діяльності, посилюючи для цього потенціал зовнішньополітичних структур та загальний кіберпотенціал держави. Науковцями узагальнено, а експертами підтверджено, що з цією метою Україна розвиває мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва. Проте, розгляд засад міжнародної співпраці у сфері забезпечення кібербезпеки в умовах ескалації протиборства у кіберпросторі та поширення сучасних глобальних гібридних загроз жоден із вказаних авторів не здійснював. За таких умов висвітлення здобутків України та визначення шляхів

удосконалення міжнародної співпраці у сфері забезпечення кібербезпеки з метою їх деталізації є актуальним, своєчасним й таким, що відповідає засадам розвитку сучасної державної кібербезпекової політики.

Метою статті є деталізація шляхів удосконалення подальшого міжнародного співробітництва щодо посилення спроможностей сектору безпеки і оборони України у сфері забезпечення кібербезпеки.

Виклад основного матеріалу. Стаття 14 Закону України "Про основні засади забезпечення кібербезпеки України" [8] регламентує, що міжнародне співробітництво у сфері кібербезпеки наша держава здійснює на виконання укладених міжнародних договорів з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з транснаціональною кіберзлочинністю. Відповідно до чинного законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі. Розуміючи актуалізацію доцільності підвищення рівня кібербезпеки, у тому числі й завдяки міжнародній співпраці, Указом Президента України від 20 грудня 2019 року було уведено в дію рішення Ради Національної безпеки і оборони України від 7 грудня 2019 року "Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки" [9].

Виходячи із доктринальних засад чинного законодавства, Україна, відповідно до укладених нею міжнародних договорів, здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, насамперед держав-членів НАТО та ЄС, а також з міжнародними організаціями. Інформація з питань, пов'язаних із забезпеченням кібербезпеки, боротьбою з міжнародною кіберзлочинністю та кібертероризмом, подається іноземній державі на підставі укладених Україною міжнародних договорів. Такий формат охоплює широке коло питань нормотворчого, методологічного, практичного, наукового і навчально-виховного спрямувань, що передбачає проведення тематичних міжнародних семінарів та конференцій, надання іноземним партнерам методичної та практичної допомоги, організацію робочих контактів з провідними експертами в галузі кібербезпеки, що має позитивні результати вивчення та впровадження кращих практик кіберзахисту на вітчизняних теренах.

Таким чином, міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, який існує між динамічним розвитком інформаційних технологій та законодавчим реагуванням на сучасні кіберзагрози. Міжнародне співробітництво здійснюється з метою: зміцнення взаємної довіри у сфері кібербезпеки; вироблення спільних підходів до протидії кіберзагрозам; консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних цілях; виконання Україною зобов'язань у рамках укладених міжнародних договорів у контексті співробітництва у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також міжнародними організаціями; оптимізації надання міжнародної технічної допомоги.

В сучасних умовах ситуація, що склалася навколо майбутнього глобального кіберпростору, перебуває на перетині двох рівнозначних трендів. З одного боку, офіційні зусилля світової спільноти спрямовані на демілітаризацію кіберпростору та недопущення його перетворення на нове поле збройного конфлікту, а з іншого – де-факто триває процес полярного протистояння. Міжнародні структури, на кшталт ООН, хоча й роблять спроби впливати на цей процес, однак ці наміри є досить фрагментарними. Незважаючи на цілу низку рішень і резолюцій, ООН так і не запровадила дієвого міжнародно-правового

механізму, який би оптимізував кібербезпекову проблематику. Чимало документів ООН у цій сфері мають суперечливий характер та не сприймаються деякими державами-членами як фундаментальні. Хоча останнім часом ООН демонструє активізацію у сфері нормативного врегулювання світової кібербезпекової тематики. Наприклад, у червні 2015 року за підсумками засідання Групи урядових експертів ООН з міжнародної інформаційної безпеки було визнано, що до сфери використання інформаційно-комунікаційних технологій застосовується міжнародне право, однак у разі необхідності воно може бути доповнене, у тому числі за рахунок прийняття нових норм.

Модернізація політики інформаційної безпеки на рівні ООН зумовлена новими чинниками відповідальної поведінки держав, приватного сектора, наукових кіл й громадянського суспільства у кіберпросторі, яка могла б сприяти підвищенню ефективності міжнародного співробітництва [10, с. 103]. З 2019 року парадигма обговорення та схвалення тематики кібербезпеки в ООН зазнала суттєвих змін, що пов'язано із стрімким поширенням глобальних гібридних загроз міжнародного масштабу у цій площині. Останнім часом активізувалася робота на експертному рівні ООН з метою розробки міжнародних документів щодо вироблення єдиного підходу адекватного реагування на виклики сьогодення, оскільки у світі існує система незбалансованого розподілу та несправедливого управління критично важливими інтернет-ресурсами, що створює певну загрозу безпеці, пов'язану із безперебійним функціонуванням цієї інфраструктури. На цьому фоні держави повинні брати участь в управлінні та розподілі міжнародних інтернет-ресурсів на рівних та паритетних засадах. Адміністратори ключових ресурсів не повинні перебувати під контролем будь-якого уряду. Проте, основним проблемним питанням, актуальним для ООН, є застосування діючого міжнародного права у кіберпросторі.

Так, 28 грудня 2019 року Генеральна Асамблея ООН схвалила Резолюцію щодо боротьби з кіберзлочинністю. "Проти" цієї Резолюції виступили, зокрема, США, Канада, європейські держави та, передусім, Україна. Авторами документа виступили 47 держав, зокрема РФ, Білорусь, Казахстан, Азербайджан, Таджикистан, Вірменія, Китай, Індія, Сирія, Єгипет, КНДР, Іран і Венесуела. Цей документ передбачає створення міжнародного комітету для розробки міжнародної конвенції щодо протидії використанню інформаційно-комунікаційних технологій у злочинних цілях, який мав запрацювати у серпні 2020 року. У США і ЄС вважають, що запропонована ініціатива може призвести до встановлення цензури в Інтернеті та становити реальну загрозу свободі слова в глобальній мережі. Невипадково у представництві США при ООН заявили, що ухвалена резолюція може підірвати міжнародну співпрацю з метою боротьби проти кіберзлочинності. Навіть міжнародна правозахисна організація "Human Rights Watch" наголосила, що авторами Резолюції виступили держави, у першу чергу РФ, які використовують репресивні методи боротьби проти інакомислення. Україна обурена законодавчими ініціативами ООН, оскільки ця міжнародна структура певним чином підігрує державі-агресору, яка власне і запропонувала проект цієї Резолюції з метою поширення свого впливу над кіберпростором, отримання легітимного способу "блокувати інформацію" в Інтернеті та значно обмежити цифрові права громадян. Підставою для таких законодавчих пропозицій для ООН з боку держави-агресора стало набуття чинності з 1 листопада 2019 року в РФ федерального Закону про "суверенний Рунет", головним концептом якого визначено створення інфраструктури, яка дозволить Кремлю ізолювати російський сегмент Інтернету та фільтрувати як внутрішній, так і зовнішній Інтернет-трафік.

Очкується, що перспективна робота ООН, зокрема групи урядових експертів ООН з питань інформаційної безпеки буде сфокусована на чотирьох ключових аспектах:

1) правила, норми та принципи поведінки держав в інформаційному просторі;

2) заходи, спрямовані на зміцнення довіри у ньому;

3) нарощування цифрового потенціалу;

4) інституціоналізація переговорного механізму з питань міжнародної інформаційної безпеки в ООН.

Враховуючи сучасні виклики та загрози, актуальним для України є забезпечення участі України у роботі міжнародної платформи Програми дій із заохочення відповідальної поведінки держав у кіберпросторі Генеральної Асамблеї ООН та Групи урядових експертів ООН з питань інформаційної безпеки (UNGGE).

Найбільш впливовою та авторитетною міжнародною структурою, яка постійно удосконалює власну безпекову політику, є саме НАТО, яка тлумачить кіберпростір як арену протистояння та середовище інформаційного протиборства, визначаючи при цьому саме кібербезпеку як основний пріоритет своєї діяльності. Союзники підтвердили оборонний мандат НАТО й визнали кіберпростір середовищем операцій, в якому НАТО має ефективно захищатися, як це відбувається в інших фізичних середовищах протиборства. Командування НАТО з питань швидкого реагування на кіберзагрози доручило надавати допомогу союзникам щодо протидії кібератакам. Крім того, для захисту держав-членів НАТО можуть залучатися національні підрозділи кібербезпеки для проведення спеціальних операцій. Зокрема у 2019 році було схвалено рекомендації НАТО, що містять низку інструментів для: перспективного посилення спроможностей адекватного реагування на кібератаки, активізації співпраці з діловими партнерами й бізнес-середовищем у сфері розвитку кіберпромисловості; побудови можливостей використання кіберпростору союзниками на основі рекомендаційних та безпечних норм.

Для України одним із ключових пріоритетів міжнародного співробітництва у сфері забезпечення кібербезпеки залишається стратегічне партнерство з Північноатлантичним Альянсом. При цьому основними завданнями співробітництва між НАТО та державами-партнерами у сфері забезпечення кібернетичного захисту залишаються: підтримання нормальної життєдіяльності об'єктів критичних інформаційно-комунікаційних інфраструктур; розробка дієвих заходів протидії кібератакам; надання допомоги державам-членам у відновленні нормального функціонування відповідної інфраструктури внаслідок проведення зовнішніх кібернетичних атак; функціонування системи оперативного реагування на будь-які загрози в інформаційній сфері держав-членів [5, с. 52].

Головні принципи співробітництва НАТО з державами-партнерами у сфері кібернетичного захисту передбачають, що: Альянс може надавати державам-партнерам, у разі необхідності, свою експертну допомогу та, потенційно, свої спроможності для захисту проти кібернетичних атак; держави-партнери можуть звертатися з пропозицією щодо співпраці у сфері кібернетичного захисту та отримання підтримки з боку НАТО у випадках кібератак національного значення; співпраця між НАТО та державою-партнером має бути взаємовигідною у тому сенсі, що Альянс може надати інформацію та підтримку партнерам, але, у свою чергу, може отримати необхідну інформацію та підтримку від партнерів, зокрема, що стосується обміну досвідом у сфері кібербезпеки; НАТО і партнери повинні уникати дублювання заходів, що вживаються в рамках інших міжнародних організацій, які залучаються до захисту інформаційних систем від кібератак; наявність Угоди про безпеку між НАТО та державою-партнером, в якій визначатимуться обсяги допомоги та інформаційного обміну. Як переконливо доводить світовий досвід, забезпечення національної безпеки неможливо уявити без: удосконалення національної системи забезпечення кібербезпеки, яка б відповідала критеріям членства України в НАТО, підтримки міжнародних ініціатив у сфері кібербезпеки; інтенсифікації співпраці України з

ЄС та НАТО; підвищення спроможностей сектору безпеки і оборони у сфері кібербезпеки; участі у міжнародно-правових заходах щодо зміцнення довіри в кіберпросторі.

У липні 2019 року Польща та НАТО підписали першу угоду про співпрацю у сфері кібербезпеки. Комплексна взаємодія передбачає формат створення цілодобових пунктів швидкого реагування на кіберінциденти з використанням потужностей НАТО, спрямованих на ліквідацію будь-яких загроз у кіберпросторі. Ця угода стала правовим підгрунтям щодо можливого використання Альянсом команд швидкого реагування в разі поширення загроз в кіберпросторі. Завдяки угоді Польща братиме участь у розробці систем раннього попередження про загрози в кіберпросторі, також може розраховувати на поради експертів НАТО та плідну співпрацю з оборонною промисловістю. На цьому фоні ефективність міжнародного співробітництва між Україною та НАТО у кібербезпекових питаннях є очевидною.

Одним із базових аспектів безпекової політики для України залишається розвиток конструктивного партнерства з НАТО, в основі якого міститься критерій протидії сучасним викликам та загрозам, досягнення Україною провідних стандартів у сфері обороноздатності. У рамках розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки для України особливе партнерство з НАТО є невід'ємною складовою євроінтеграційного курсу, оскільки доповнює процес внутрішньодержавних перетворень необхідними реформами оборонного та безпекового секторів. Практика, що склалася в цьому форматі, передбачає щорічне схвалення на державному рівні Національної програми співробітництва Україна – НАТО.

Указом Президента України [11] було затверджено порядок розроблення, моніторингу та оцінювання результатів виконання річної національної програми під егідою Комісії Україна-НАТО. Аналіз цього програмного документа засвідчує, що взаємодія з НАТО не обмежується лише проведенням реформ у сфері безпеки. Річна національна програма під егідою Комісії Україна – НАТО являє собою ключовий інструмент досягнення Україною необхідних критеріїв членства в НАТО. Це системний документ, який містить опис реформ, визначає їхню стратегічну мету, зміст, завдання і заходи в наступних напрямках: політичні та економічні питання, оборонні і військові питання, питання ресурсів, питання безпеки, правові питання. Зокрема, Уряду доручено щорічно затверджувати перелік заходів щодо виконання річної національної програми та показників ефективності її виконання; здійснювати координацію діяльності центральних органів виконавчої влади та інших державних органів з моніторингу та оцінки результатів виконання Річної національної програми; регулярно інформувати громадськість про хід та результати виконання річної національної програми.

В сучасних умовах саме через систему діяльності Трастового фонду з кібербезпеки держави-члени НАТО надаватимуть підтримку Україні з метою розвитку її оборонних можливостей у галузі забезпечення кібернетичної безпеки, що передбачає постачання устаткування та обладнання, програмного забезпечення, надання технічної допомоги, консультативних послуг та проведення навчальних тренінгів. Додатковими контриб'юторами цього Трастового фонду виступили такі держави: Албанія, Італія, Туреччина та США. З огляду на можливості та потенціал Трастового фонду НАТО до основних заходів, реалізація яких дасть змогу посилити кібербезпеку в нашій державі, відносяться: проведення консультацій експертів з питань кіберзахисту, активізація діяльності фонду в напрямі формування базових концептів національної системи кібербезпеки.

Керівництвом НАТО Румунію як державу-члена ЄС було визнано провідною державою цього Трастового фонду, а його координаторами – Румунську спецслужбу та

Державну румунську компанію "RASIROM RA", яка спеціалізується на інтеграції та інжинірингу систем кібербезпеки. Перспективний розвиток оборонного технічного потенціалу України у сфері кібербезпеки досягається шляхом: впровадження на об'єктах критичної інфраструктури передових технічних рішень, які забезпечуватимуть належний рівень кібербезпеки; створення центральної та мережевої лабораторій комп'ютерно-технічних експертиз із фіксованими та мобільними компонентами; проведення тренінгів для персоналу, у тому числі для групи реагування на інциденти кібербезпеки (CERT) щодо експлуатації, ремонту й управління створеними інформаційними системами. Виходячи з цього, найбільш актуальним та важливим завданням діяльності Трастового фонду з питань кібербезпеки є надання допомоги Україні щодо розвитку технологічних можливостей протистояння сучасним кіберзагрозам.

У липні 2017 року в Службі безпеки України відбулася офіційна церемонія завершення першого етапу програми Трастового фонду НАТО зі сприяння Україні у зміцненні її спроможності у сфері кіберзахисту. Загальна сума відрахувань до Трастового фонду становила на першому етапі 1 млн. Євро. Крім постачання обладнання та програмного забезпечення, програма передбачала оплату проведення тренінгів та навчань персоналу. Ще у 2018 році в м. Києві відкрили перший ситуаційний центр кібербезпеки, який був створений згідно з угодою про реалізацію Трастового фонду Україна – НАТО. За результатами роботи у 2018 році Трастовий фонд кібербезпеки повністю виконав першу фазу, після чого відбувся перехід до другої фази, яка наразі триває. За таких умов, актуальним напрямом міжнародного співробітництва у сфері забезпечення кібербезпеки залишається конструктивна співпраця з НАТО, що передбачає: проведення консультацій та переговорів з питань кіберзахисту; продовження удосконалення нормативно-правової бази з питань кібербезпеки; забезпечення та сприяння розвитку під егідою Альянсу Трастового фонду з кібербезпеки. Таким чином, держава здійснює діяльність щодо консолідації зусиль, спрямованих на прискорення запровадження стандартів НАТО у сфері приєднання до колективної системи забезпечення кіберзахисту.

Загалом можна констатувати, що Україна реалізує конструктивний діалог з НАТО у сфері забезпечення кібербезпеки. За таких умов, Україна має розвивати міжнародне співробітництво у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України, поглиблюючи діалог України з Організацією з безпеки і співробітництва в Європі щодо зміцнення довіри при використанні кіберпростору, спільного розуміння ландшафту кіберзагроз та вдосконалення механізмів такої співпраці. У майбутньому динамічний розвиток співпраці з НАТО у сфері кібербезпеки матиме результативне продовження, якщо українське політичне керівництво буде підтримувати, у першу чергу, темпи реформ у військовій та оборонній сферах та покращить рівень міжвідомчої координації.

Російська гіперактивність в кіберпросторі є головним викликом та загрозою для України у сфері забезпечення кібербезпеки. РФ використовує кіберпростір як простір нових можливостей для здійснення не тільки розвідувально-підривної діяльності проти України, але й проведення спеціальних операцій з прихованого проникнення в кібер-мережі органів державної влади й управління, встановлення дистанційного контролю над об'єктами критичної інфраструктури з метою отримання переваг та забезпечення своїх інтересів у інформаційній, військово-політичній, фінансово-економічній, енергетичній сферах. Загальновідомо, що в РФ напрацьовані зразки кіберзброї для нейтралізації та виведення з ладу об'єктів критичної інфраструктури супротивника з метою підвищення ефективності наступного першого удару або ж максимального послаблення його спроможностей чинити опір. Адже подібна кіберзброя не може мати ніякого потенціалу стримування.

Також занепокоєння викликає і факт насичення українського ринку засобами мобільного зв'язку китайського виробництва з відповідним програмним забезпеченням. На тлі резонансних розслідувань у Європі та США щодо прихованих можливостей китайських продуктів для збору інформації для України важливою є співпраця з НАТО, спрямована на запобігання можливим негативним наслідкам їх масового використання та недопущення появи подібного обладнання і програмного забезпечення в системі державного та військового управління. Не випадково у січні 2021 року Генеральний секретар Північноатлантичного альянсу Столтенберг закликав членів Військового комітету НАТО продовжувати збільшувати витрати на оборону та інвестувати в сучасні технології через "агресивні дії РФ та підйом Китаю".

В умовах співпраці з НАТО, стратегічним завданням для України є захист від кібератак, мішенню яких неодноразово ставали об'єкти критичної інфраструктури держави. Україна зацікавлена у залученні до роботи Агентства з питань мережевої та інформаційної безпеки ЄС (далі – ENISA), Європейського центру досліджень та компетенції з кібербезпеки, а також до тренінгів ЄС щодо координації механізмів спільного реагування ЄС та держав-членів на масштабні інциденти та кризові ситуації в галузі кібербезпеки. Посилення кібербезпеки України та поглиблення співпраці у цій сфері відповідає інтересам як ЄС так і України. На цьому тлі актуальним для України є посилення співробітництва з ENISA, зокрема з питань скоординованого розкриття уразливостей та імплементації Директиви ЄС "Про безпеку мережевих та інформаційних систем" (NIS Directive) від 6 липня 2016 року щодо заходів для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, як елементу євроінтеграції України.

У рамках перспективного розвитку співробітництва між Україною та НАТО варто, перш за все, враховувати поточні тенденції такої співпраці. Подальше співробітництво доцільно зосередити на наступних напрямках: використання передового досвіду НАТО у цій площині, поглиблювати державно-приватне партнерство; ініціювати приєднання України до Центру передового досвіду НАТО з кібероборони, що допоможе Україні імплементувати кращі практики і поглибити співпрацю з Альянсом у цій сфері; нарощувати оборонний технічний потенціал України у сфері кібербезпеки за сприяння Трастового фонду НАТО з кібербезпеки та у співпраці із Румунією; розробити механізми розподілення ризиків через використання захищених Хмарних сервісів задля мінімізації можливих втрат у разі кібернападу на інформаційні бази органів державної влади; залучати кращі практики задля посилення міжвідомчого співробітництва з виробленням конкретного дієвого механізму його практичного застосування; спільними зусиллями розробити систему мотивації для фахівців, зайнятих у сфері кібербезпеки тощо.

Міжнародний позитивний досвід у боротьбі із загрозами у сфері кібербезпеки та його здобутки є конче необхідними для України та мають бути враховані під час формування державної безпекової політики та адаптовані під час розбудови власної системи кібербезпеки. На сучасному етапі перед політичним керівництвом України постає важливе та відповідальне завдання: запозичуючи передовий зарубіжний досвід, разом із світовим співтовариством спільними зусиллями активізувати реалізацію дієвих заходів щодо боротьби з міжнародною кіберзлочинністю, що передбачає, передусім: побудову ефективної моделі національної системи кібербезпеки, її поступову інтеграцію до спільноти НАТО; залучення та кооперацію з європейськими інституціями, які опікуються проблематикою забезпечення кібербезпеки; концентрацію зусиль у напрямі розробки міжнародно-правового механізму гарантування кібербезпеки та його впровадження на теренах України; залучення можливостей міжнародної технічної допомоги з метою розбудови національної системи кібербезпеки, грантів міжнародних організацій у рамках

реалізації комплексних міжурядових програм розвитку міжнародної інформаційної безпеки; забезпечення поглиблення співпраці України з НАТО для підвищення стійкості та посилення спроможностей держави у сфері кібербезпеки.

Україна робить важливі поступальні кроки у сфері нарощування потенціалу у сфері кібербезпеки, активізуючи міжнародне співробітництво. Так, останнім часом, Україна та Ізраїль домовилися про поглиблення співпраці у галузі кібербезпеки. На початку 2020 року Україна та Японія визначили сфери майбутньої співпраці у галузі кібербезпеки та висловили готовність до посилення двостороннього співробітництва щодо боротьби з кіберзагрозами. Очікується, що така перспективна двостороння співпраця сприятиме розбудові та визначенню більш чіткого плану подальшого руху у напрямку покращення систем та заходів з реагування на майбутні загрози. На цьому тлі сторони домовилися про взаємодію компетентних органів двох держав щодо побудови відкритого, операційно-сумісного, надійного та безпечного кіберпростору.

На виконання Постанови Верховної Ради України від 4 лютого 2020 року [12] на 15 квітня 2020 року було заплановано проведення парламентських слухань на тему: "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення". Проте у зв'язку із запровадженням локдауну внаслідок поширення масштабів пандемії COVID-19 в Україні вказаний захід так і не відбувся.

Під час офіційного візиту 21 – 23 березня 2021 року Голови Верховної Ради України Д. Разумкова до Бельгії було проголошено, що саме реалізація курсу, спрямованого на прискорення реформування військової та безпекової сфери відповідно до принципів та стандартів НАТО є пріоритетом для України. А тому визнання України стратегічним партнером НАТО з розширеними можливостями є важливим етапом реалізації євроатлантичних прагнень України. Голова Верховної Ради також наголосив, що завданням Альянсу та України є відновлення формату засідань Комісії Україна – НАТО на високому рівні. За таких умов можна впевнено констатувати, що євроатлантична інтеграція залишається пріоритом зовнішньої та безпекової політики України.

Висновки.

У світових масштабах проблема забезпечення кібербезпеки з кожним роком посилюється та постійно актуалізується як перед світовою спільнотою, так і політичним керівництвом України. Таким чином, у міжнародному кіберпросторі, незважаючи на прагнення світової спільноти врегулювати питання його мирного використання та повної демілітаризації, спостерігається конфронтація та протиборство між групами держав (США, РФ, КНР), що бажають довести своє домінуюче становище та лідерство у кіберпросторі, який на сьогодні є ареною протистояння, продемонструвати силу та перевагу. З огляду на викладене, можна констатувати, що міжнародне співробітництво у сфері забезпечення кібербезпеки здійснюється переважно у організаційно-правових формах, типових і для інших сфер міжнародного регулювання – договірній та інституційній.

Україна повинна продовжувати участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації заінтересованих сторін на міжнародних форумах, в яких Україна буде не лише учасником, але й ініціатором та організатором. Враховуючи викладене, Україна повинна займати більш проактивну позицію на міжнародній арені з питань забезпечення кібербезпеки. Держава має розвивати міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України, підтримання ініціатив учасників системи колективної безпеки НАТО.

З цією метою доцільно прискорити вжиття таких заходів, як: динамічний розвиток міжнародного співробітництва у сфері кібербезпеки шляхом підтримки міжнародних ініціатив, які відповідають національним інтересам України, поглиблюючи діалог України з Організацією Північноатлантичного договору та ЄС, особливо у питаннях зміцнення довіри при використанні кіберпростору, спільного розуміння ландшафту кіберзагроз та вдосконалення механізмів такої паритетної співпраці; визначити та затвердити перелік пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України. Іншими словами, актуальним напрямком для України залишається продовження партнерської співпраці з НАТО у кіберсфері. При цьому головним зовнішньополітичним фарватером України у сфері кібербезпеки є: поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками НАТО; вжиття інших узгоджених з іноземними партнерами заходів, спрямованих на посилення кіберстійкості України; розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Використана література

1. Гребенюк М.В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. *Підприємництво, господарство і право.* 2019. № 2. С. 203-207.

2. Демедюк С.В., Демедюк Т.С. Міжнародний досвід протидії кіберзлочинності, *Вісник Харківського національного університету внутрішніх справ*. 2014. № 4. С. 65-75. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2014_4_10 (дата звернення: 31.03.2021).

3. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека.* 2015. № 2 (57). С. 107-113.

4. Марущак А.І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право.* № 3(26)/2018. С. 104-110.

5. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України. Серія: "Державне управління"*. 2015. № 4. С. 50-56. URL: http://nbuv. gov.ua/UJRN/Vnadu_2015_4_10 (дата звернення: 31.03.2021).

6. Скулиш Є.Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право.* № 1(10)/2014. С. 93-100.

7. Шемчук В.В. Основні напрями міжнародного співробітництва у сфері кібербезпеки. *Вчені записки ТНУ імені В.І. Вернадського. Серія: "Юридичні науки"*. 2018. № 2. Т. 29 (68). С. 125-130.

8. Про основні засади забезпечення кібербезпеки в Україні: Закон України від 05.10.17 р. № 163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 31.03.2021).

9. Про рішення Ради національної безпеки і оборони України від 7 грудня 2019 року "Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки": Указ Президента України від 20.12.19 р. № 923/2019 URL: https://zakon.rada.gov.ua/laws/show/923/ 2019#Text (дата звернення: 31.03.2021).

10. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя.* 2020. № 1. С. 102-109.

11. Про затвердження Положення про Річні національні програми під егідою Комісії Україна – НАТО: Указ Президента України від 24.02.21 р. № 72/2021. URL: https://www.president.gov.ua/documents/722021-36825 (дата звернення: 31.03.2021).

12. Про проведення парламентських слухань на тему: "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення": Постанова Верховної Ради України від 04.02.20 р. № 500. URL: https://zakon.rada.gov.ua/laws/ show/500-20#Text (дата звернення 31.03.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~