УДК 004.056.53:341.238
DOI: 10.31733/15-03-2024/2/389-390

Владислава УСТИМЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Юлія СИНИЦІНА
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО В ГАЛУЗІ КІБЕРБЕЗПЕКИ

Тема міжнародного співробітництва в галузі кібербезпеки є дуже актуальною в сучасному світі, оскільки кіберзагрози стають все більш складними і виразними, а їх вплив може мати серйозні наслідки для держав, підприємств та громадян. Існуючі кіберзлочини та кібератаки, такі як крадіжки даних, кібершпигунство, вплив на вибори та інфраструктуру, створюють загрози для національної безпеки та економічного розвитку країн. В умовах глобалізації та інтерконектованості мереж, ефективне міжнародне співробітництво важливо для обміну інформацією, розробки спільних стратегій та стандартів, а також для координації дій у відповідь на кіберзагрози. Без ефективного співробітництва між державами, міжнародними організаціями та приватним сектором складно забезпечити ефективний захист від кіберзагроз і збереження кібербезпеки в цілому.

Сьогодні дуже важливою є необхідність усвідомлення владою, політичною елітою, наукою, що забезпечення національної безпеки і всіх її складових, законотворча робота, прогнозування, перспективне і поточне планування, розробка стратегій, концепцій, доктрин, програм і проектів, напрямків сталого розвитку, державне управління, міжнародне співробітництво починається з інформаційного рівня. Інформаційна складова пронизує всі сфери життєдіяльності людини, соціальних систем. На цьому етапі формуються основи як кібербезпеки, так і національної безпеки в цілому. Інформаційними перш за все заходами та засобами здійснюється керівництво з питань реалізації державної політики у цій сфері діяльності [1, с. 178].

Нинішня актуалізація гібридних викликів і загроз, пов’язана з агресією Росії проти України, надає додаткового поштовху поглибленню взаємодії двох організацій. Зокрема, в лютому 2016 року перед схваленням Спільної заяви ЄС-НАТО, обидві організації підписали Технічну угоду про співпрацю в галузі кібероборони, що стимулює обмін інформацією, тренування та дослідження. На даний момент співпраця між Групою реагування на комп’ютерні надзвичайні ситуації ЄС та Центром можливостей з реагування на комп’ютерні інциденти НАТО розвивається, що відображено у їхніх офіційних документах. Крім того, розширена співпраця між ЄС та НАТО відзначається усіма аспектами, включаючи кібербезпеку, а також спільність дій у рамках Розширеної співпраці з кібербезпеки з участю третіх країн, таких як Молдова, Туніс та Боснія і Герцеговина. Україна має багато кваліфікованих експертів у кіберсфері. Проте їм все ще не вистачає міжвідомчої координації та співпраці з міжнародними партнерами. Наприклад, Консультативна місія ЄС в Україні співпрацює з Кіберполіцією України, Службою безпеки України та Національним центром координації кібербезпеки при РНБО України. Настільки необхідна взаємодія підтримується низкою ініціатив і зусиль, однак в Україні ще є проблеми з міжвідомчою координацією та співпрацею з міжнародними партнерами, що ускладнює ефективний захист кіберпростору.

Наразі Україна взаємодіє з ЄС та НАТО у сфері кібербезпеки незалежно одна від одної, хоча інколи відбувається узгодження дій на практичному рівні. Проте для досягнення ефективного співробітництва, важливо, щоб ця двостороння підтримка була координована відповідно до принципів співпраці ЄС-НАТО у кібербезпеці.

Розвиток співпраці України з НАТО надає пріоритетне значення кібербезпеці. Українські експерти, які взяли участь у міжнародному круглому столі «Україна-НАТО:

Невійськова співпраця як спільна відповідь на гібридні загрози», відзначили важливість кібербезпеки серед пріоритетних напрямів співпраці Україна-НАТО для протидії гібридним загрозам.

Налагоджено кіберспівпрацю між Україною й НАТО, яка щороку прописується в Річних національних програмах під егідою Комісії Україна НАТО (РНП) в окремому розділі «Кібербезпека». Метою цієї співпраці визначено «удосконалення національної системи кібербезпеки як складової системи забезпечення інформаційної безпеки, її правових концептуальних засад та практичних механізмів протидії агресії РФ у кіберпросторі». Згідно з РНП, Україна зміцнює співробітництво державних, у тому числі правоохоронних і спеціальних органів, з приватним ІТ-сектором, що відповідає підходам і ЄС, і НАТО у сфері протидії кіберзагрозам [2, с. 133-134].

Загалом, міжнародне співробітництво у сфері кібербезпеки включає наступні складові:

– розробку нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі кібербезпеки;

– входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на спільне вирішення проблем кібербезпеки;

– участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів [1, с. 166].

Задля успішної реалізації міжнародного співробітництва у сфері забезпечення кібербезпеки України варто, на нашу думку, вивчити досвід зарубіжних країн у згаданій сфері, а також прийняті ними акти та ефективність їх реалізації.

За висновками Артеменко Я.В.: «Співробітництво України з іншими державами світу у сфері забезпечення кібербезпеки може здійснюватись наступними шляхами: взаємодії на міжнародному рівні при протидії кіберзагрозам та кібератакам; обміну досвідом побудови та функціонування національних систем кібербезпеки; вироблення стандартів кібербезпеки [3, с. 16]. Наразі нами запропоновано більш детальне формування основних перспективних напрямів розвитку міжнародного співробітництва в галузі кібербезпеки, а саме: *Створення міжнародних стандартів і нормативів:* Розвиток загальноприйнятих міжнародних стандартів і нормативів щодо кібербезпеки може сприяти збільшенню взаєморозуміння між країнами та покращенню співпраці у боротьбі з кіберзагрозами. *Обмін інформацією і досвідом:* Створення механізмів для обміну інформацією про кіберзагрози, інциденти та кращі практики може допомогти країнам вчасно реагувати на кібератаки та підвищити рівень кібербезпеки.*Спільні навчальні програми та тренування:* Організація спільних навчальних програм, симуляцій та тренувань може допомогти підвищити кваліфікацію фахівців з кібербезпеки та підготувати їх до реагування на складні кіберзагрози.*Створення міжнародних центрів експертизи:* Розвиток міжнародних центрів експертизи з кібербезпеки може сприяти спільному вивченню та аналізу кіберзагроз, а також розробці ефективних стратегій захисту.*Міжнародна дипломатія в галузі кібербезпеки:* Залучення дипломатичних зусиль для вирішення питань кібербезпеки на міжнародному рівні може допомогти укладенню міжнародних угод та договорів, спрямованих на забезпечення стабільності та безпеки в кіберпросторі.

Отже, можемо зробити висновок, що міжнародне співробітництво в галузі кібербезпеки є невід'ємною складовою ефективного захисту від кіберзагроз у сучасному цифровому середовищі. Міжнародне співробітництво в галузі кібербезпеки має включати розробку нормативно-правової бази, створення та підтримку двосторонніх і багатосторонніх структур, а також активну участь у роботі цих структур. Це також передбачає взаємодію на міжнародному рівні, обмін досвідом та розроблення загальних стандартів кібербезпеки. Загалом, співробітництво в цій сфері є критично важливим для забезпечення національної безпеки та стійкості у діджиталізованому світі, і його подальше посилення вимагає спільних зусиль та залучення різних зацікавлених сторін.

1. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ : Видавничий дім «Кондор», 2019. 272 с.

2. Даник Ю.Г., . Воробієнко П.П, Чернега В.М. Основи кібербезпеки та кібероборони: підручник Одеса : ОНАЗ ім. О.С. Попова, 2019. 320 с.

3. Артеменко Я.В. Адміністративно-правове забезпечення функціонування національної системи кібербезпеки України: автореф. дис. …канд. юрид. наук: 12.00.07. Київ, 2020. 21 с.