УДК 351.865
DOI https://doi.org/10.32782/2524-0374/2022-10/121

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

INTERNATIONAL COOPERATION IN THE SPHERE OF ENSURING CYBER SECURITY OF UKRAINE

Сливка М.М., к.ю.н., доцент,
доцент кафедри адміністративного та інформаційного права
Навчально-науковий інститут права, психології та інноваційної освіти
Національного університету «Львівська політехніка»

Стаття присвячена дослідженню міжнародного співробітництва у сфері забезпечення кібербезпеки України.

Зазначено, що українським фахівцям з кіберзахисту дедалі частіше доводиться шукати шляхів співробітництва з аналогічними організаціями світового співтовариства, адже у своїй роботі вони зіштовхуються з численними труднощами та не мають можливості самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному та кіберпросторі.

Вказано, що вагому роль у виробленні єдиних підходів щодо забезпечення кібербезпеки як складової національної безпеки країн відіграє Організація Північноатлантичного договору (НАТО), партнерство з якою для України є пріоритетним у сфері зовнішньополітичної діяльності.

Зазначено, що співробітництво України з іншими державами світу у сфері забезпечення кібербезпеки може здійснюватись шляхом: 1) взаємодії на міжнародному рівні при протидії кіберзагрозам та кібератакам; 2) обміну досвідом побудови та функціонування національних систем кібербезпеки; 3) вироблення стандартів кібербезпеки.

Підкреслено, що найбільш досконала система кіберзахисту критично важливої інфраструктури функціонує у США, де розроблені стандарти з безпеки (NIST Cybersecurity Framework), які сьогодні активно застосовуються багатьма приватними організаціями в усьому світі, оскільки дають змогу виявляти, реагувати та навіть запобігати кіберінцидентам.

Наголошено, що базовим нормативним актом, у якому визначаються стратегічні напрями державної політики Франції у сфері забезпечення безпеки, є Біла книга оборони та національної безпеки від 2013 р. та Національна стратегія цифрової безпеки 2015 р. Стратегія покликана супроводжувати цифровий перехід французького суспільства і відповідає новим викликам, викликаним зміною використання цифрових технологій і пов'язаних із ними загроз із п'ятьма цілями: 1) гарантувати національний суверенітет; 2) забезпечити сильну відповідь на акти кіберзлочинності; 3) інформувати громадськість в цілому; 4) забезпечити цифрову безпеку, адже це є конкурентною перевагою для французьких підприємств; 5) посилити позиції Франції на міжнародній арені.

Ключові слова: міжнародне співробітництво, кібербезпека, кіберзагроза, кіберпростір, кіберзахист, НАТО, Європейський Союз.

The article is devoted to the study of international cooperation in the sphere of ensuring cyber security of Ukraine.

It is noted that Ukrainian cyber security specialists increasingly have to look for ways of cooperation with similar organizations of the world community, because in their work they face numerous difficulties and do not have the opportunity to deal with all manifestations of internal and external threats to the national security of Ukraine in information and cyberspace on their own.

It is indicated that the North Atlantic Treaty Organization (NATO), a partnership with which is a priority for Ukraine in the field of foreign policy, plays an important role in the development of unified approaches to ensuring cyber security as a component of the national security of countries.

It is noted that Ukraine's cooperation with other countries of the world in the field of cyber security can be implemented through: 1) cooperation at the international level in countering cyber threats and cyber attacks; 2) exchange of experience in building and functioning of national cyber security systems; 3) development of cyber security standards.

It is emphasized that the most advanced system of cyber protection of critical infrastructure operates in the USA, where security standards (NIST Cybersecurity Framework) have been developed, which today are actively used by many private organizations around the world, as they enable detection, response and even prevention of cyber incidents.

It is emphasized that the basic regulatory act, which defines the strategic directions of French state policy in the field of security, is the White Paper of Defense and National Security of 2013 and the National Digital Security Strategy of 2015. The strategy is designed to accompany the digital transition of French society and meet new challenges, caused by the changing use of digital technologies and related threats with five goals: 1) to guarantee national sovereignty; 2) ensure a strong response to acts of cybercrime; 3) inform the public as a whole; 4) ensure digital security, because this is a competitive advantage for French enterprises; 5) strengthen the position of France on the international arena.

Key words: international cooperation, cyber security, cyber threat, cyber space, cyber defense, NATO, European Union.

Постановка проблеми. В сучасних умовах забезпечення кібербезпеки України набуває особливої актуальності, що зумовлено проблемами зростання кількості кіберзагроз у кіберпросторі, активним впровадженням інформаційно-комунікаційних технологій в усі сфери життя суспільства, а також повномасштабним вторгненням Росії в Україну.

Стан дослідження. Питання міжнародного співробітництва у сфері забезпечення кібербезпеки перебували в центрі уваги таких науковців: М. Гребенюка, С. Демедюка, Р. Лук'янчука, А. Марущака, О. Полякова, Т. Станіславського, В. Шемчука та ін. Незважаючи на наявність наукових праць із зазначеної проблематики, чимало питань все ще є нерозкритими або вирішеними фрагментарно.

Метою статті є дослідження міжнародного співробітництва у сфері забезпечення кібербезпеки України.

Виклад основного матеріалу. Українським фахівцям з кіберзахисту дедалі частіше доводиться шукати шляхів співробітництва з аналогічними організаціями світового співтовариства, адже у своїй роботі вони зіштовхуються з численними труднощами та не мають можливості самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному та кіберпросторі.

Як зазначає О. М. Поляков, 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 [1, с. 131].

За своєю сутністю кіберзлочини є транскордонними і тому міжнародні організації закликають держави до співпраці з іншими зацікавленими сторонами розробляти дієві механізми адміністративно-правового регулювання у сфері кібербезпеки, що передбачає не лише розроблення та прийняття необхідного законодавства, а й проведення спільних розслідувань, зазначених діянь з використанням існуючого міжнародного права й, зокрема, Конвенції Ради Європи з кіберзлочинності [2, с. 144].

Серед органів, які здійснюють регулювання кіберпростору, варто зазначити такі: у Європейському Союзі функціонує Агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), у Сполучених Штатах Америки кібербезпекою займається Агентство Національної Безпеки, у НАТО створений Комітет з кібернетичної оборони (The Cyber Defence Committee), а також Спільний центр з кібернетичної оборони (Cooperative Cyber Defence Centreof Excellence), Спеціалізований центр з оборони в сфері кібербезпеки НАТО (CCDCOE), Міжнародний альянс із забезпечення кібербезпеки (ICSPA), Інтерпол (INTERPOL), Міжнародне багатостороннє товариство проти кіберзагроз (IMPACT) та ін. [3, с. 655].

Вагому роль у виробленні єдиних підходів щодо забезпечення кібербезпеки, як складової національної безпеки країн, відіграє Організація Північноатлантичного договору (НАТО), партнерство з якою для України є пріоритетним у сфері зовнішньополітичної діяльності.

У 2008 р. в рамках Спільної робочої групи Україна-НАТО з питань воєнної реформи за ініціативи Служби безпеки України було започатковано створення Робочої підгрупи з питань кібернетичного захисту, що стало поштовхом для розробки концептуальних засад взаємодії між Україною та Північноатлантичним Альянсом у вказаній сфері, запровадження механізму консультацій та оперативного обміну інформацією в разі скоєння кібернетичних атак національного масштабу, розробки критеріїв оцінки кібернетичних загроз [4, с. 52].

Найвищим органом, який ухвалює рішення стосовно розвитку відносин Україна – НАТО та спрямовує заходи в плані практичного співробітництва, є Комісія Україна – НАТО (КУН) [5]. Це співробітництво охоплює операції з підтримання миру, реформування структур безпеки і оборони, безпосереднє військове співробітництво, оборонні технології та ін.

У ст. 14 Закону України «Про основні засади забезпечення кібербезпеки України» [6] регламентовано, що Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

Співробітництво України з іншими державами світу у сфері забезпечення кібербезпеки може здійснюватись шляхом:

1) взаємодії на міжнародному рівні при протидії кіберзагрозам та кібератакам;

2) обміну досвідом побудови та функціонування національних систем кібербезпеки;

3) вироблення стандартів кібербезпеки [7, с. 16].

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.

Досвід США, Великої Британії, Ізраїлю, Німеччини свідчить про створення системи кібербезпеки з єдиним координуючим органом, який здатен за короткий проміжок часу акумулювати сили та засоби різних державних і недержавних органів для протидії та нейтралізації кібератак. Ці системи підпорядковуються главі виконавчої влади та, як правило, містять такі складові:

1) військову;

2) захисту критичної інфраструктури;

3) правоохоронну;

4) дорадчо-консультативну [8, с. 92].

Варто підкреслити, що найбільш досконала система кіберзахисту критично важливої інфраструктури функціонує у США, де розроблені стандарти з безпеки (NIST Cybersecurity Framework), які сьогодні активно застосовуються багатьма приватними організаціями в усьому світі, оскільки дають змогу виявляти, реагувати та навіть запобігати кіберінцидентам.

Для України важливо знати досвід США у сфері кібербезпеки, зокрема, в питаннях створення відповідної нормативно-правової бази. У 2003 році була опублікована Національна стратегія безпеки кіберпростору (National Strategy to Secure Cyberspace) CLUA. Вона стала складовою частиною стратегії національної безпеки. NSSC визначає три стратегічні цілі: захист від кібератак критичних інфраструктур США; зменшення вразливості від кібератак в загальнонаціональному масштабі; мінімізація збитків та часу відновлення від кібератак [9, с. 248].

Стратегія кібербезпеки Канади передбачає три напрями: захист урядових систем (встановлення чітких ролей і відповідальності, посилення безпеки кіберсистем федерального рівня і підвищення інформованості уряду в області кібербезпеки); співпраця з метою захисту ключових кіберсистем, що знаходяться за межами федерального Уряду (ряд партнерських проектів державного рівня із залученням приватного сектора і секторів критичних інфраструктур) та забезпечення безпеки канадських громадян в онлайн-середовищі (боротьба з кіберзлочинністю і захист канадських громадян в онлайн-середовищі. Також порушується проблема персональних даних [10, с. 13].

Однією з ключових цілей Франції є зміцнення стратегічної стабільності і міжнародної безпеки в кіберпросторі. Базовим нормативним актом, у якому визначаються стратегічні напрями державної політики Франції у сфері забезпечення безпеки, є Біла книга оборони та національної безпеки від 2013 р. та Національна стратегія цифрової безпеки 2015 р. Стратегія покликана супроводжувати цифровий перехід французького суспільства і відповідає новим викликам, викликаним зміною використання цифрових технологій і пов'язаних із ними загроз із п'ятьма цілями: 1) гарантувати національний суверенітет; 2) забезпечити сильну відповідь на акти кіберзлочинності; 3) інформувати громадськість у цілому; 4) забезпечити цифрову безпеку, адже це є конкурентною перевагою для французьких підприємств; 5) посилити позиції Франції на міжнародній арені.

Національна стратегія кібербезпеки передбачає, що французька держава працює над забезпеченням безпеки IT-систем у напрямі колективного реагування, цифрової довіри, що є необхідним для стабільності держави, економічного розвитку і захисту громадян [11, с. 79].

У Німеччині механізм адміністративно-правового забезпечення кібербезпеки містить значну кількість нормативно-правових актів, які передбачають відповідальність та суворе покарання за різні правопорушення в кіберпросторі.

Законом ФРН «Про посилення безпеки інформаційних систем» завдання попередження, реагування на інциденти, викликані кібернетичними загрозами, управління й координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема у взаємодії з приватним сектором, покладене на Федеральне відомство безпеки інформаційних систем (BSI) ФРН [12, с. 178].

Зважаючи на значний прогрес і досвід Європейського Союзу у виробленні й удосконаленні механізму забезпечення кібербезпеки європейських країн, Україна повинна стати активним учасником цих безпекових процесів. З одного боку, враховуючи інтеграційні прагнення України, це буде сприяти поліпшенню іміджу держави, а з іншого – впливати на формування організаційно-правової основи забезпечення національної кібербезпеки України [13, с. 34].

Висновки. Міжнародне співробітництво України та набуття досвіду адміністративно-правового забезпечення у сфері кібербезпеки є вкрай важливим та необхідним для вдосконалення законодавства у даній сфері, а також підвищення ефективності функціонування національної системи кібербезпеки України.

ЛІТЕРАТУРА

1. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.
2. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис*. 2015. № 2. С. 144–147.
3. Федченко Д.І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *Молодий вчений*. 2017. Випуск 5 (57). С. 653–658.
4. 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.
5. Офіційний портал НАТО. URL: https://www.nato. int/cps/uk/natohq/topics_37750.htm
6. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017 р. № 2163-VIII. ВВР України. 2017. № 45. Ст.403.
7. Артеменко Я. В. Адміністративно-правове забезпечення функціонування національної системи кібербезпеки України: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2020. 21 с.
8. Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз. *Інформаційна безпека людини, суспільства, держави*. 2012. № 3 (10). С. 91–100.
9. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В.О. Жадька ; ред.-упор. : О.І. Харитоненко, Ю.С. Полтавець. Київ : Вид-во НПУ імені М.П. Драгоманова, 2018. 356 с.
10. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / НАПрН України, НДІІП К.: Видавничий дім «АртЕк». 2017. 107с.
11. Бухарєв В.В. Зарубіжний досвід забезпечення кібербезпеки ат можливості його використання в Україні. *Науковий вісник УжНУ. Серія «Право»*. № 43, Т. 3. С. 76-80.
12. Ліпкан В. А., Діордіца І. В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174–180.
13. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. 2018. № 53. С. 26–37.