УДК 327.7:341.1(4-11):005.334
DOI https://doi.org/10.32850/LB2414-4207.2020.12.12

РОЛЬ ОБСЄ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

Дубовик Віктор Борисович,
кандидат юридичних наук

Актуальність теми статті підтверджується тим, що кількість та частота викликів і загроз, що виникають у кіберпросторі, підштовхує кожен національний орган державної влади та кожну міжнародну організацію, яка має завдання уникати та керувати такими подіями, до розробки постійної та стабільної системи захисту.

Наголошено, що особливістю подій у сфері кібербезпеки є їх непередбачуваність, частота та еволюція протягом короткого періоду, здебільшого поширюючись через національні кордони і охоплюючи кілька країн одночасно. Враховуючи це, міжнародне співробітництво відіграє вирішальну роль. У сфері кібербезпеки навіть двостороння угода може бути складним питанням через різні національні інтереси, цінності та цілі. З огляду на це регіональне співробітництво здається все більш проблематичним.

Визначено, що події в кіберпросторі часто залишають місце для неоднозначності та спекуляцій. Такі неоднозначності між державами, які виникають внаслідок діяльності в кіберпросторі, можуть посилитися, що призведе до серйозних наслідків як для громадян, так і для економіки, і, можливо, породить політичну напругу. Ключовим викликом є те, що інформаційно-комунікаційні технології ускладнили правопорушення та порядок їх розслідування. Хоча держави інвестують значні кошти в оборонні кіберможливості, нині не існує технічних засобів, щоб віднести кібердіяльність поза розумним сумнівом.

Зроблено висновок, що для досягнення національних і регіональних цілей у сфері кібербезпеки необхідний розвиток міцної співпраці в регіоні та ефективний і швидкий обмін інформацією. Ефективна участь у боротьбі з загрозами та викликами кібербезпеці робить колективну та спільну роботу країн-членів неминучою. Пріоритетом є запобігання, але значення має також і швидке та ефективне реагування на події та кризи в кібербезпеці, управління кризами та процес відновлення. Надання пріоритету національним інтересам створює перешкоду під час міжнародної співпраці, створюючи більш-менш тривалий застій у роботі для досягнення цілей такої співпраці.

Ключові слова: Організація з безпеки і співробітництва в Європі, європейська система міжнародної безпеки, інформаційна безпека, кібербезпека, безпека в інтернеті, захист персональних даних, виміри діяльності ОБСЄ.

ROLE OF OSCE IN ENSURING CYBER SECURITY

Dubovyk Viktor Borysovych,
Candidate of Juridical Sciences

The relevance of the topic of the article is confirmed by the fact that the number and frequency of challenges and threats that arise in cyberspace, pushes every national authority and every international organization tasked with avoiding and managing such events, to develop a permanent and stable protection system.

It is emphasized that the peculiarity of events in the field of cybersecurity is their unpredictability, frequency and their evolution over a short period, mainly spreading

across more national borders and thus covering several countries simultaneously. With this in mind, international cooperation plays a crucial role. In the field of cybersecurity, even a bilateral agreement can be a complex issue due to different national interests, values and goals, and based on this, regional cooperation seems increasingly problematic.

It is determined that events in cyberspace often leave room for ambiguity and speculation. Such ambiguities between states as a result of cyberspace activities may intensify, with serious consequences for both citizens and the economy and possibly creating political tensions. The key challenge is that information and communication technologies have complicated offenses and the way they are investigated. Although states are investing heavily in cyber defense capabilities, there are currently no technical means to attribute cyber activities beyond a reasonable doubt.

It is concluded that the achievement of national and regional goals in the field of cybersecurity requires the development of strong cooperation in the region and efficient and rapid exchange of information. Effective participation in combating cybersecurity threats and challenges makes collective and collaborative work by member countries inevitable. Prevention is of course a priority, but rapid and effective response to cybersecurity events and crises, crisis management and the recovery process are equally important. Prioritization of national interests creates an obstacle in international cooperation, thus creating a more or less long stagnation in work and achieving the goals for this cooperation.

Key words: Organization for Security and Co-operation in Europe, European system of international security, information security, cybersecurity, internet security, protection of personal data, dimensions of OSCE activity.

Постановка проблеми. Кібербезпека – одна з найважливіших проблем, з якою стикається суспільство у сучасному світі. Кількість та частота викликів і загроз, що виникають у кіберпросторі, підштовхують кожен національний орган державної влади та кожну міжнародну організацію, яка має завдання уникати та керувати такими подіями, до розробки постійної та стабільної системи захисту.

До XX століття безпека була розділена на п'ять секторів: військова, політична, економічна, соціальна та екологічна. Однак, починаючи з 2010-х років, інформаційний сектор все більше розвивався [1]. Особливістю подій у сфері кібербезпеки є їх непередбачуваність, частота та еволюція протягом короткого періоду, здебільшого поширюючись через національні кордони і охоплюючи кілька країн одночасно. Враховуючи це, міжнародне співробітництво відіграє вирішальну роль. У сфері кібербезпеки навіть двостороння угода може бути складним питанням через різні національні інтереси, цінності та цілі. З огляду на це регіональне співробітництво здається все більш проблематичним.

Метою статті є визначення особливої ролі ОБСЄ у забезпеченні кібербезпеки в інформаційному просторі.

Виклад матеріалу дослідження. Протягом останніх 15 років ОБСЄ здійснила переорієнтацію своїх напрямів діяльності з урахуванням необхідності відповідати очікуванням нового середовища безпеки. Організація безпеки та співробітництва в Європі, будучи загальноєвропейською організацією безпеки з багаторічною історією, до якої входять 57 європейських, північноамериканських і середньоазіатських країн і 11 країн-партнерів, має забезпечувати інформаційну безпеку при співробітництві всіх своїх членів. Таке переорієнтування відповідає найвищій меті організації – захисту європейської безпеки та стабільності, ранньому попередженню, управлінню конфліктами та процесами підтримки після конфлікту [2].

ОБСЄ постійно адаптується до очікувань нового середовища безпеки та протистоїть новим видам загроз, таких як тероризм, торгівля людьми та наркотиками, організована злочинність і кіберзлочинність. З метою посилення особистої та колективної участі у підтримці інформаційно-комунікаційних технологій (далі – ІКТ) у складній формі своєю резолюцією № 1039 від 29 квітня 2012 року ОБСЄ створила Неофіційну робочу групу (далі – МРГ). Основним завданням групи було визначено обробку заходів із підвищення довіри з метою підтримання міжнародної співпраці, прозорості, передбачуваності та стабільності, а також для зменшення ризику непорозумінь, ескалації та конфліктів, пов'язаних із використанням ІКТ [1].

Відповідно до Резолюції № 1202 ОБСЄ держави-члени виконують такі завдання:

1) обмін національним досвідом щодо різних аспектів національних і транснаціональних загроз при використанні ІКТ;

2) розвиток співпраці та обмін інформацією між своїми компетентними національними організаціями щодо ІКТ;

3) консультування, щоб зменшити політичні та військові сутички, які виникають через непорозуміння внаслідок використання ІКТ;

4) обмін досвідом щодо забезпечення відкритої, сумісної, безпечної та надійної мережі Інтернет;

5) розгляд ОБСЄ як платформи, здатної підтримувати дискусії, обмін передовою практикою, консультації щодо підвищення потенціалу більш безпечних ІКТ та обмін ефективними відповідями на кожну загрозу;

6) підготовка національних нормативних актів, які забезпечують двостороннє співробітництво між компетентними відомствами, насамперед правоохоронних;

7) обмін національними стратегіями, директивами та програмами з державною та приватною сферою, а також щодо безпеки використання ІКТ;

8) встановлення контактної точки, обмін контактними даними для кожного елемента національної структури, які можуть бути використані у випадку можливого інциденту (ці дані оновлюють щорічно);

9) щоб уникнути непорозумінь, які виникають через відсутність загальної термінології, проведення підготовки переліку термінів щодо використання та забезпечення безпеки ІКТ;

10) підтримка консультацій, добровільно використовуючи платформи та механізми ОБСЄ, щоб полегшити зв'язок, пов'язаний з управлінням КБ;

11) проведення експертних засідань щонайменше тричі на рік на рівні призначених експертів-членів нації в рамках ІРГ щодо обговорення, реалізації та розвитку МБР;

12) підтримка обміну інформацією та обмін інформацією між країнами-членами шляхом організації семінарів і круглих столів;

13) підтримка спілкування між посадовими особами та експертами захищеними та законними каналами з метою уникнення та зменшення можливих наслідків непорозумінь, конфліктів та ескалації;

14) сприяння співпраці між державною та приватною сферою у досліджуваній сфері;

15) підтримка регіональної співпраці між посадовими особами, відповідальними за безпеку критичної інфраструктури;

16) підтримка обміну інформацією щодо вразливості безпеки та використання ІКТ, оскільки вся така інформація та комунікації підтримують регіональне співробітництво з ОБСЄ [2].

Робоча група працює під керівництвом президента ОБСЄ щорічно на замовлення адміністрації ОБСЄ і має за мету здійснення досліджень шляхом отримання експерт-

них висновків із країн, які добровільно розробляють пропозиції щодо безпечного використання ІКТ [3]. ОБСЄ відіграє унікальну роль у підвищенні безпеки в кіберпросторі, зокрема, зменшуючи ризики конфліктів, які виникають внаслідок використання ІКТ між державами-учасницями. Останніми роками ІКТ додають складнощів у вимірі міждержавних відносин.

Події в кіберпросторі часто залишають місце для неоднозначності та спекуляцій. Такі неоднозначності між державами, що виникають внаслідок діяльності в кіберпросторі, можуть посилитися, що призведе до серйозних наслідків як для громадян, так і для економіки, і, можливо, породить політичну напругу. Ключовим викликом є те, що ІКТ ускладнили правопорушення та порядок їх розслідування. Хоча держави інвестують значні кошти в оборонні кіберможливості, нині не існує технічних засобів, щоб віднести кібердіяльність поза розумним сумнівом [4].

Під егідою ОБСЄ 57 держав-учасниць організації розробили та продовжують працювати над ґрунтовним набором заходів щодо утвердження довіри (КБМ) для зменшення ризиків виникнення конфліктів, пов'язаних із використанням ІКТ. Вони покликані зробити кіберпростір більш передбачуваним і запропонувати конкретні інструменти та механізми для уникнення та усунення можливих непорозумінь [5], зокрема:

1) механізм об'єднання держав для консультацій щодо можливих інцидентів безпеки в кіберпросторі / ІКТ для усунення зростаючої напруги;

2) платформа для обміну думками, національної політики та підходів до кібер / ІКТ, що дозволить державам краще «читати» наміри один одного в кіберпросторі;

3) предмети співпраці, включаючи захист критичної інфраструктури, що підтримує ІКТ, як частину підвищення кіберстійкості в регіоні ОБСЄ на благо всіх [5].

ОБСЄ прийняла два комплекси заходів щодо зміцнення довіри. Перший набір заходів щодо прозорості (2013 рік) створив, серед іншого, офіційні пункти зв'язку та лінії зв'язку для запобігання можливої напруги внаслідок кібердіяльності (див.: www.osce.org/pc/109168). Другий набір (2016 рік) був зосереджений на подальшому вдосконаленні співробітництва між державами-учасницями, включаючи, наприклад, ефективне пом'якшення кібератак на критичну інфраструктуру, що може вплинути на більш ніж одну державу-учасницю (див.: www.osce.org/pc/227281).

Регіональні організації, такі як ОБСЄ, є ідеальними платформами для утвердження довіри до кіберпростору: їх часто задумували для запобігання конфліктам і пропонують практичну експертизу з МБР та пов'язаними з ними механізмами, які можна застосувати до цієї нової сфери. ОБСЄ є першою регіональною організацією безпеки з таким різноманітним виборчим округом, якій вдалося досягти домовленостей щодо заходів безпеки в сфері ІКТ, зосереджених на кіберзасобах [3].

Відділ транснаціональних загроз Секретаріату ОБСЄ допомагає державам-учасницям у їхніх зусиллях щодо підвищення кібер / ІКТ безпеки. Зокрема, його службовець з питань кібербезпеки допомагає впроваджувати та розробляти нові КБ із питань кібер / ІКТ, пропонуючи рекомендації щодо політики, а також координуючи організаційний результат у цій галузі [4].

Департамент транснаціональних загроз також пропонує конкретні заходи, спрямовані на підвищення потенціалу держав-учасниць у боротьбі з загрозами кібер / ІКТ. Такі заходи варіюються від навчань, що сприяють адекватному національному реагуванню на потенційні кібератаки на критичні інфраструктури, до семінарів із протидії використанню інтернету з терористичною метою та тренувань щодо розслідування та переслідування кіберзлочинів [2].

Зусилля ОБСЄ, пов'язані з безпекою в галузі ІКТ, доповнюють керівництво ООН групи урядових експертів щодо підвищення кіберстабільності між державами, рекомендуючи чотирипроменевий підхід до глобальної кіберстабільності між державами [4]:

1) підвищення прозорості, співпраці та стабільності між державами в кіберпросторі за допомогою заходів з утвердження довіри (ЦБ);

2) розробка прийнятних норм поведінки держави в кіберпросторі та уточнення, як у цій галузі застосовується міжнародне право;

3) поглиблення міжнародної співпраці;

4) нарощування національного / міжнародного потенціалу для вирішення кіберпроблем.

Висновки. Таким чином, для досягнення національних і регіональних цілей у сфері кібербезпеки необхідний розвиток міцної співпраці в регіоні та ефективний і швидкий обмін інформацією.

Ефективна участь у боротьбі з загрозами та викликами кібербезпеки робить колективну та спільну роботу країн-членів неминучою. Пріоритетом є запобігання, але однакове значення має також швидке та ефективне реагування на події та кризи в кібербезпеці, управління кризами та процес відновлення. Надання пріоритету національним інтересам створює перешкоду під час міжнародної співпраці, створюючи більш-менш тривалий застій у роботі та досягнення цілей для такої співпраці [5]. Також у випадку ОБСЄ є приклади зазначених вище причин, які викликають спад у співпраці, але також очевидно, що стосовно теперішнього та майбутнього часу регіональне співробітництво неминуче для вирішення нових, транснаціональних видів безпекових викликів.

Список використаних джерел:

1. Gazdag F., Remek É. A biztonsági tanulmányok alapjai. Dialóg Campus Kiadó, Budapest, 2018.

2. Decision № 1202 OSCE Confidence-building measures toreduce the risks of conflict stemming from the use of information and communication. URL: technologies https://www.osce.org/pc/227281?download=true.

3. V4 connects, Hungarian presidency 2017/2018 of the Visegrad Group. URL: http://v4.gov.hu/a-visegradi-egyuttmukodesrol (accessed on: 2019, febr. 27).

4. Rajnai Z., Fregán B. Új alapokon a magyarországi kibervédelmi stratégia. In: A XXII. Fiatal műszakiak tudományos ülésszak előadásai. Proceedings of the 22th international scientific conference of youngth engineers, Kolozsvár / Cluj, Románia, Műszaki Tudományos Közlemények 7. (2017) 351–354. URL: https://eda.eme.ro/handle/10598/29842.

5. Antal József Tudásközpont, Kutatás-Kutatói. URL: http://www.ajtk.hu/kutatoi-blog/219/a-visegradi-negyek-helyzete-a-kibervedelem-tekinteteben.