

## **ІНФОРМАЦІЙНІ ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ**

Для успішного проведення аналізу впливу кіберзброї на національну безпеку, а також для формування загальних уявлень про практичні можливості такого впливу, доцільно дослідити трактування деяких термінів в інформаційній сфері.

В Україні засади кібербезпеки ґрунтуються на основах національної безпеки. У законодавчому полі, на нашу думку, питанню забезпечення кібербезпеки приділено достатньо уваги. Тут можна говорити про Закон України «Про національну безпеку», який безпосередньо закріплює саму Стратегію кібербезпеки України (документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави) [1]. Варто згадати про Закон України «Про основні засади забезпечення кібербезпеки України», норми якого визначають правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [2]. Також Законом [2] визначено ряд таких термінів як «кібербезпека», «кіберзагроза», «кіберпростір», «кіберзахист», «кібератака» та інші.

Кібербезпека, безпека кіберпростору (cybersecurity, cyberspace security) – збереження цілісності, конфіденційності та доступності інформації, що циркулює в кіберсистемі (тобто інформації, що надходить в кіберсистему, накопичується та зберігається в ній для подальшої обробки), з метою забезпечення стійкості і безперервності реалізації кіберсистемою управлінських функцій щодо відповідних об'єктів управління [3, с. 12]. Під кіберзагрозами розуміються наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [4, с. 350]. Можна навести декілька дефініцій поняття «кіберзброя»: сукупність інформаційно-телекомунікаційних технологій, які деструктивно впливають на стани масової свідомості, політичну й економічну ситуацію в локальному (окремі країни) та глобальному масштабах; безліч спеціалізованих методів і засобів, які забезпечують тимчасове або безповоротне пошкодження інформаційної інфраструктури супротивника в цілому або окремих її елементів. До різновидів кіберзброї відносять засоби розвідки, отримання інформації з інформаційних і телекомунікаційних систем; політично мотивовані атаки на веб-сайти та сервери електронної пошти; створення вірусних програм; вербальна (семантична) інформація, яка

здійснює вплив на психіку людини; засоби несанкціонованого збору інформації [5, с. 227].

Як видно, багато з вищезазначених понять формують уявлення про те, які протистояння можуть відбуватися у кіберпросторі. При цьому спричинити шкоду національним інтересам держави за допомогою кіберзброї можна у досить короткий проміжок часу. Вжиті для підриву комп'ютерні технології надають можливість застосовувати кібератаки тихо, на великій відстані та з метою порушення нормального функціонування системи національної безпеки. Таке кібервтручання однозначно визнається навмисною діяльністю і дуже часто для її розпізнавання необхідні спеціальні знання. У дійсності, розрахувати реальні наслідки від кіберзагроз надзвичайно складно. Ніхто до кінця не зможе оцінити в повній мірі ефект непередбачуваності щодо втручання у життя суспільства, маніпулювання людською свідомістю, дестабілізації суспільно-політичної ситуації тощо. І як результат, усе це створює реальні перешкоди, загрози для національної безпеки країни.

Саме тому, побудова в Україні інформаційного суспільства та забезпечення належного рівня кібербезпеки є одним із ключових завдань держави задля життєдіяльності національних правових відносин й подальшого соціального розвитку.

#### ЛІТЕРАТУРА:

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради*. 2018. № 31. Ст. 241.
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
3. Архипов О. Є., Бровко В. Д. Кібербезпека – виникнення, формування, розуміння. *Інформаційна безпека людини, суспільства, держави*. 2017. № 2 (22). С. 6-14.
4. Шеломенцев В. П. Основні напрями і суб'єкти забезпечення кібернетичної безпеки України. 2013. № 1 (29). С. 348-355. URL: [irbis-nbuv.gov.ua > cgi-bin > irbis\\_nbuv > cgiirbis\\_64 > boz\\_2013\\_1\\_42](http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64?boz_2013_1_42).
5. Куцепал С. В. Інформація як засіб здійснення гібридної війни. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. 2015. № 3 (26). С. 226-228.