

**УДК 681.518.54**

**Доколяса О.С. студент гр. УБіт-14-1**

**Науковий керівник: Ковальова Ю.В., асистент кафедри безпеки інформації та телекомунікацій**

*(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)*

## **КІБЕРБЕЗПЕКА В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРИ УКРАЇНИ**

З'ясовано зміст поняття «кібербезпека». Визначено проблему у необхідності подолання суперечності між наявним станом стрімкого зростання важливості кібербезпекової проблематики та часткової готовності Української держави відповісти на новітні кіберзагрози. Розглянуто проблему забезпечення державою кібербезпеки в інформаційному просторі, через ряд вдало проведених кібератак на інфраструктуру України.

Ключові слова: кіберпростір, кібербезпека, кіберзагроза.

За останні 6–8 років глобальний кіберпростір усе більшою мірою розглядається всіма державами світу як один із найважливіших безпекових пріоритетів, оскільки його функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів. У таких умовах виняткового значення для забезпечення національних інтересів та їх захисту на міжнародному рівні набуває ефективність механізмів забезпечення кібербезпеки держави та вирішення тих проблем, які виникають на шляху їх розбудови. Саме через більш широке використання комп'ютерних і телекомунікаційних технологій у найрізноманітніших сферах життєдіяльності соціуму України, у тому числі інтернет-технологій, разом з великою кількістю переваг принесло також і чималу кількість загроз. Реалізація цих загроз може завдати значної шкоди інфраструктурі України. Усвідомлення можливих втрат призвело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації загроз кіберпростору України і визначення важливості кібербезпеки в сучасному інформаційному просторі в цілому.

Згадки про перше використання терміну «кібербезпека» виникали у середині 1990-х років, коли уряд США став досліджувати цю тему [1].

За Законом України «Про основні засади забезпечення кібербезпеки України» термін «кібербезпека» означає захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2].

З урахуванням того, що проблема кібербезпеки носить глобальний характер, досить цікавою видається позиція міжнародних організацій. Так, Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй рекомендації дає таке визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача [3].

Актуальним питанням сьогодення є вдало здійснені кібератаки на інформаційний простір України. Влітку 2017 року державні установи та українські компанії зазнали масової кібератаки, вірусу Petya. А. Це була одна з найбільш масштабних кібератак в історії України. Атака показала, що держава була абсолютно не готова до кіберзагроз

через несвоєчасне їх виявлення і відповідною реакцією основних суб'єктів національної безпеки України. Основною причиною неготовності полягало у відсутності правового документу, що визначав би основні положення, щодо забезпечення кібербезпеки України.

Для регулювання подібних ситуацій необхідна нормативна база, саме тому в Україні розроблявся Закон «Про основні засади забезпечення кібербезпеки України» понад двох років. 5 жовтня 2017 р. Верховна Рада України ухвалила Закон «Про основні засади забезпечення кібербезпеки України» (Реєстраційний № 2126а), який був підписаний президентом 7 листопада 2017 р. Цей закон є позитивним нормативно-правовим актом, оскільки він визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів української держави в сфері кібербезпеки, забезпечує і надає основні правові повноваження спеціальним службам (державним органам) для забезпечення кібербезпеки. Основними її суб'єктами, тобто ті, на кого ляже відповідальність за гарантування кібербезпеки, мають стати Держспецзв'язок, нацполіція, СБУ, міністерство оборони, генштаб ЗСУ, розвідка та НБУ. Першочергове реагування на кіберзагрози закон покладає на створену ще в 2007 році урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA. Ця структура діє при Державній службі спеціального зв'язку та захисту. Важливим у цьому законі є те, що він впроваджує кримінальну відповідальність, за злочини, вчинені саме в кіберпросторі. А також тлумачить самі поняття "кібербезпека", "кіберзахист" та "кіберзлочинність", які вже понад десяти років використовують у юридичній практиці, у тому числі у зв'язку із вчиненими в мережі злочинами, але які досі не були ніде закріплені в документах.

Таким чином, у контексті вище зазначеного, ми бачимо, що однією з головних проблем забезпечення кібербезпеки в сучасному інформаційному просторі України є брак нормативної бази. Не було зроблено головного - країна і суспільство перейшли у нове сторіччя, у кіберпростір, проте не підготували у свій час відповідних інструкцій та фахівців. Можемо зробити висновок, що Закон «Про основні засади забезпечення кібербезпеки України» має стати першим кроком для подальших значно конкретніших дій у цій сфері. Має бути розроблена низка підзаконних актів, які детальніше регулюватимуть заходи з кібербезпеки.

#### ПЕРЕЛІК ПОСИЛАНЬ

1. Лисичкин В.А, Третья світова інформаційно-психологічна війна. М.: Ваклер, 2009, с. 265.
2. Закон України «Про основні засади забезпечення кібербезпеки України», документ 2163-19, прийняття від 05.10.2017
3. Крутских А., Федоров А. Про міжнародну інформаційну безпеку / Крутских А., Федоров А. // Міжнародне життя. 2000, № 2, С. 43.