5. Anatoliy Yeremenko v. Ukraine (Application no. 22287/08), § 48.
6. Юдківська Г. Ю. Якість закону як елемент принципу юридичної визначеності. *Слово Національної школи суддів України.* 2021. № 5. С. 16-23.
7. Ukrainian Media Group v. Ukraine (Application no. 72713/01), § 49.
8. Kononov v. Latvia (Application no. 36376/04) [GC], § 235.
9. Jecius v. Lithuania (Application no. 34578/97), § 56.

УДК 343.3/.7

**Яцик Т. П.**
*к.ю.н., доцент,*
*професор кафедри кримінальних розслідувань,*
*Державний податковий університет*

## БЕЗПЕКОВЕ СЕРЕДОВИЩЕ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Розвиток інформаційної цивілізації потребує від суспільства суттєвих змін щодо формування інформаційної політики та інформаційної безпеки держави з метою захисту інформаційного простору від несанкціонованих втручань.

Останнім часом у світі зросла потреба в посиленні інформаційної безпеки у зв'язку зі стрімким розвитком цивілізації, новітніх технологій та збільшення рівня впливу на суспільство та його думку інформації, яку в більшості випадків можна порівняти зі зброєю, тому що вона здатна завдавати не менш руйнівних наслідків ніж військові дії. Тому важливо сформувати ефективний механізм протидії інформаційній складовій гібридної війни.

Гібридна війна та її стратегія поняття не нові. Багато практичних працівників стверджують, що дані поняття виникли ще з появою традиційної війни. Тим не менш, останніми роками вони набули значної популярності та актуальності, оскільки держави для ведення гібридної війни мають можливість використовувати як державні, так і недержавні ресурси та суб'єкти, інформаційні технології, щоб приборкати своїх супротивників під час прямого збройного конфлікту, а часто і без його наявності, тоді присутній лише один з елементів гібридної війни – інформаційна війна.

Науковці чітко не розділяють поняття «гібридної війни» та «війни», тому що перша – це просто один із видів війни, який виник із-за стрімкого розвитку суспільства в цілому та інформаційних систем зокрема.

Для того, щоб зрозуміти, що мається на увазі під терміном «гібридна війна», необхідно проаналізувати війну з точки зору її ієрархічних рівнів.

На рівні стратегії кожна війна є гібридною. Будь-яка держава та її влада використовують всі наявні інструменти та методи (включаючи невійськові) для досягнення своїх політичних та інших цілей.

Після рівня стратегії слідує рівень виконання цієї стратегії. Більшість науковців, які досліджують поняття та суть гібридної війни посилаються саме

на цей рівень, який дає можливість виділити характерні риси гібридної війни. На цьому рівні (тактичному) гібридну війну можна відрізнити від звичайної за рахунок застосування під час такої війни нових збройних (військових) систем і технологій та застосування їх регулярними, нерегулярними і недержавними силами. Це в свою чергу надає не тільки тактичні можливості, але також сприяє появі нових загроз. Гібридна війна на тактичному рівні означає, що системи озброєнь тепер здатні досягати непропорційно високих стратегічних наслідків [1, с. 32].

Інформатизація суспільства – це всеохоплюючий і неминучий процес у розвитку людської цивілізації в цілому та кожної особи зокрема. За інформатизацією стоїть майбутнє, але це і виклик, який постав перед людством щодо приборкання такої потужної рушійної сили. Інформатизація суспільства передбачає використання більш ширшого кола інформаційних технологій у всіх сферах держави і суспільства з метою підвищення їх розвитку. Проте така діяльність, в свою чергу, породжує не тільки позитивні моменти, але і негативні. Оскільки останні десятиліття супроводжувалися стрімким розвитком інформаційних технологій, обмін інформацією значно пришвидшився. У зв'язку з розбудовою мережі Інтернет з'явилися нові можливості поширення інформації [2, с. 119].

Гібридна війна досить розповсюджений вид війти в XXI столітті, тому що за допомогою неї можна досягти масштабних наслідків, використовуючи скромні засоби. Такий вид війни передбачає взаємодію або злиття звичайних і нетрадиційних інструментів влади та тактик ведення війни. Ці інструменти та тактики поєднуються синхронізовано, щоб використовувати вразливі місця противника та досягати синергічного ефекту.

Мета поєднання різних інструментів та тактик полягає в тому, щоб завдати шкоди воюючій державі оптимальним чином. Крім того, є дві відмінні характеристики гібридної війни. По-перше, межа між воєнним і мирним часом стає розмитою. Це означає, що важко ідентифікувати або розрізнити вид війни і навіть інколи взагалі складно стверджувати, що ведеться війна, тому що вона стає невловимою. Потрібно звернути ще увагу на те, що гібридна війна за порогом війни або прямого відкритого насильства приносить досить ґрунтовні і швидкі «дивіденди», тому що стратегія її ведення простіша, процес втілення стратегії дешевший та менш ризикований ніж відкритий збройний конфлікт.

Друга визначальна характеристика гібридної війни стосується неоднозначності та неможливості визначення суб'єкта, який вчиняє атаки. Гібридні атаки зазвичай відрізняються великою нечіткістю та хаотичністю. Така невідомість свідомо створюється та розширюється суб'єктами, які ведуть гібридну війну щоб ускладнити процес їх виявлення, ідентифікації та застосування відповіді на їх дії. Іншими словами, країна, яка є мішенню часто не в змозі виявити вчасно ознаки гібридної атаки або визначити державу, яка може вчиняти або спонсорувати такі дії, а це в свою чергу ускладнює процес розробки державної політики та обрання стратегічних заходів щодо протидії таким негативним явищам [3].

Інформаційна складова гібридної війни – це не тільки вчинення кіберзлочинів, хоча звичайно, вони є її частиною, це також некоректні

маніпуляції з інформацією або її підтасовування, а в деяких випадках і подача завідомо помилкових, неправдивих фактів, внаслідок чого відбувається залякування населення, нав'язування параноїдальних думок [4, с. 55].

Як можна протидіяти гібридній війні в цілому та її інформаційній складовій безпосередньо?

Україна вже зробила вагомі кроки до зміцнення своєї державності, обороноздатності на безпеки в кіберпросторі:

- налагодження комунікації держави (органів державної влади, місцевого самоврядування та їх посадових осіб з громадянами країни та міжнародною спільнотою). З цією метою в Україні у 2021 році створено Центр стратегічних комунікацій та інформаційної безпеки за прикладом Європейського Союзу, який у 2016 році ухвалив резолюцію «Стратегічні комунікації ЄС як протидія пропаганді «третіх сторін», згідно з якою було створено Центри стратегічних комунікацій (StratCom) у Ризі, Польщі, Литві, а також Центр протидії гібридним загрозам.у Фінляндії);
- напрацювання системи національної стійкості (затверджена Указом Президента України від 27 вересня 2021 року № 479/2021) – досвід Естонії;
- законодавчі застереження щодо використання фото- та відео матеріалів із зображенням військових або військової техніки, у тому числі з використанням геолокації (в українському законодавстві такі застереження з'явилися лише у 2022 році).

Підсумовуючи викладене вище, можна констатувати, що інформаційна складова гібридної війни досить потужна рушійна сила та швидко розвивається, а це може призвести до надзвичайних наслідків. Зменшення впливу інформаційної складової гібридної війни можна досягти підвищенням довіри осіб до діяльності держави в цілому та її посадових осіб зокрема, тому що найчастіше мішенню гібридних війн є саме цивільне населення, точніше їхня думка про державу в якій вони проживають чи перебувають. І якщо ворогові вдається за допомогою інформаційної складової гібридної війни вплинути на населення (внести зерно сумніву) щодо довіри до держави, то це в цілому впливає на зниження економічного, політичного, соціального та військового потенціалу держави.

## ЛІТЕРАТУРА:


1. Pikner I., Zilincik S. Military concepts and hybrid war. Forum Scientiae Oeconomia Volume 4 (2016) Special Issue № 1. URL: file:///C:/Users/Home/Desktop/forum-002.pdf.
2. Яцик Т.П., Бодунова О. М. Розповсюдження фейкової інформації як загроза інформаційній безпеці України. Протидія фейкам в Україні як складова інформаційної безпеки держави: Міжвідомчий круглий стіл, 20 травня 2021 року. Київ: ІСТЕ СБУ, 2021. 126 с.
3. Arsalan Bilal. Hybrid Warfare – New Threats, Complexity, and «Trust» as the Antidote. Opinion, analysis and debate on security issues. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.
4. Яцик Т.П. Особливості інформаційного тероризму як одного із способів

інформаційної війни. Науковий вісник Національного університету ДПС України (економіка, право), 2(65), 2014.

УДК 343.3/.7

**Olena Kalhanova**
*Candidate of Juridical Sciences (Ph. D.), Docent,*
*Director of the Educational and Scientific Institute*
*of the Economic Security and Customs Affairs,*
*State Tax University*

**Yevgen Kotukh**
*Doctor of Public Administration,*
*Candidate of Technical Sciences (Ph. D.),*
*Associate Professor of the Department of*
*Computer and Information Technologies and Systems,*
*State Tax University*

## REGULATORY AND LEGAL BASIS FOR ENSURING CYBER SECURITY IN UKRAINE

Legal and organizational foundations for ensuring the protection of the vital interests of a person and citizen, society and the state, national interests of Ukraine in cyberspace, the main goals, directions, and principles of state policy in the field of cyber security, the powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this sphere, the main principles of coordination of their activities to ensure cyber security in our country are determined by the Law of Ukraine «On the Basic Principles of Cyber Security of Ukraine».

According to Clause 5, Part 1, Art. 1 of the above-mentioned Law, cyber security is the protection of the vital interests of a person and citizen, society, and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace [1].

Currently, cyber security issues in Ukraine, in addition to the above-mentioned law, are regulated by:

1. The Cybersecurity Strategy of Ukraine [2], which is a long-term planning document that defines the priorities of Ukraine's national interests in the field of cyber security, existing and potentially possible cyber threats to the vital interests of people and citizens, society and the state in cyberspace, priority areas, conceptual approaches to the formation and implementation of state policy regarding the safe functioning of cyberspace, its use in the interests of the individual, society and the state, increasing the effectiveness of the main subjects of cyber security, primarily subjects of the security and defense sector, regarding the performance of tasks in cyberspace, as well as the need for budgetary funding, sufficient to achieve the defined goals and perform the planned tasks, and the main directions of the use of