

5. Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. № 389-VIII. Дата оновлення: 24 травня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text>

6. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо призупинення діяльності окремих політичних партій» : Указ Президента України від 19 березня 2022 р №153/2022. URL: <https://www.president.gov.ua/documents/1532022-41765>

*Гусар О.А., к.ю.н., доц., завідувачка кафедри конституційного і адміністративного права Національного авіаційного університету*

### **Інформаційна безпека людини в умовах воєнного стану**

Негативний інформаційно-психологічний вплив закладає підґрунтя для подальших операцій, що спрямовані проти інтересів України на всіх рівнях – особи, суспільства і держави. Так, починаючи з 2014 року Російська Федерація здійснювала політичний і військовий вплив на регіони Сходу та Півдня України, що спровокувало збільшення кількості проявів сепаратизму серед його населення та створило сприятливі умови для воєнного вторгнення Росії на територію України і проведення повномасштабних бойових дій в 2022 році.

З вторгненням Росії на територію України розпочалася ще одна інформаційна війна. Масштабний наратив російської пропаганди політичної еліти, нагнітання чуток, застосування симулякрів, якщо більш точно, то робота цілої «фабрики фейків», яку умовно називають «Kremlinwood», інтерв'ю російських пропагандистів та журналістів здійснюють інформаційну атаку в жорсткій інформвійні проти незалежності України та її територіальної цілісності. В Законі України «Про оборону України» (ст.4) [1], «Про правовий режим воєнного стану» (ст.1) [2] саме небезпека незалежності України та її територіальної цілісності є умовою (підставою) за якою вводиться в Україні воєнний стан. Учасниками бойових дій під час війни є збройні сили, терористи, ополченці, спецпідрозділи, найманці, партизани, а в наш час, з наявною сукупністю воєнних дій та інформаційного фронту, до них додаються ще і цивільні особи з телебачення, ЗМІ, які борються за розум і душі людей з використанням різних форм і засобів впливу.

Звернемо увагу на зміст категорії «безпека», котра у житті людини відіграє роль орієнтиру, навколо якого групуються цінності людського існування. Це поняття багатопланове, з цього приводу в науці існує багато думок. У буквальному розумінні безпека означає відсутність небезпеки. Потреба безпеки належить до числа базових мотиваційних механізмів у життєдіяльності людини. Крім того, безпека становить безсумнівну цінність, що має універсальний характер, оскільки визнається всіма людьми незалежно від їхньої расової, національної чи соціальної належності.

Питання інформаційної безпеки є важливим компонентом усієї системи національної безпеки країни [3, с. 65]. Зважаючи на те, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки, питання її забезпечення має загальнонаціональне і загальнодержавне значення. Водночас, інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки [4]. Відсутність системи забезпечення інформаційної безпеки

унеможлиблює надійне забезпечення не лише інформаційної, а й національної безпеки [5].

Безпека є складним, багаторівневим та системним явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники. Найважливішими є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітичні обставини в державі [6].

Ст. 3 Закону України «Про основи національної безпеки України» [7] визначає, що об'єктами забезпечення національної безпеки є: людина і громадянин – їхні конституційні права і свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

В наступній ст. 4 визначається, що суб'єктами забезпечення національної безпеки є: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; Національне антикорупційне бюро України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України; органи і підрозділи цивільного захисту; громадяни України, об'єднання громадян.

Звернемо увагу, що термін «національна безпека» застосовується у широкому значенні та є станом захищеності держави та її громадян від усіх можливих загроз сучасності.

Закріплення в Конституції[8] України інформаційних прав, а також проголошення забезпечення інформаційної безпеки України оголошено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» (ст. 17).

Таким чином, інформаційна безпека з вузькоспеціалізованого кола вжитку фахівців прикладного характеру була піднесена до правового закріплення на рівні Основного Закону. В різні періоди історичного розвитку людської цивілізації інтенсивність застосування інформаційного впливу, як і досконалість його організації, дуже різнилися.

Інформація, яку отримує людина, впливає на її свідомість та підсвідомість. На рівні підсвідомості інформація впливає на поведінку людини – як і в бік корегування, так і в бік повної зміни. Сама по собі неповна, невчасна, невірогідна або упереджена інформація, що використовується, у більшості випадків не завдає такої шкоди людині, що можна говорити про її небезпеку. Людина постійно стикається з такою інформацією у повсякденному житті та, вважає, що ця інформація є повною, своєчасною та вірогідною. Через деякий час можна оцінити міру її повноти, своєчасності та вірогідності чи взагалі не оцінити.

В той же час, неповна, невчасна, невірогідна або упереджена інформація впливає на свідомість або підсвідомість людини. Наслідками може бути порушення/зміни стану її здоров'я, психічного стану, поведінки та ін., в такому випадку можна й треба говорити про інформаційну небезпеку для людини, а коли це

стосується не однієї людини, а групі людей, їх психічного стану, поведінки та ін., то можна й треба говорити про інформаційну небезпеку для суспільства.

Сьогодні основною загрозою людині й суспільству залишається насильство однієї соціальної групи на іншою, з метою набуття чи збереження політичного, економічного та культурного панування, що супроводжується потужним інформаційно-психологічним впливом, деморалізацією або введення в оману противника через ЗМІ, меседжери, Інтернет, що призводить до дискримінації людини або соціальної групи, обмеження їх прав і свобод. Нажаль, інформаційні мережі створюють усі можливості для доставки ворожого культурного та/або інформаційного контенту, здійснюючи свою нищівну дію на свідомість людини.

Пропаганда набуває різних форм в залежності від етапу інформаційної війни та цільової аудиторії, на яку скеровується. Цілеспрямовано направлена інформація впливає на формування світогляду об'єкту впливу у бажаному для організатора пропаганди напрямку та здійснюється відповідна зміна поведінки людей. Так, автори навчального посібника «Гібридна війна і журналістика. Проблеми інформаційної безпеки» звертають увагу, зокрема, на такі напрямки антиукраїнської пропаганди, як безпрецедентне й нищівне втручання в сферу історичної пам'яті (спекуляції на фактах історії, маніпулювання почуттями людей щодо минулих подій і учасників цих подій), мовне питання (істеричні й безпідставні лементациї про «утиски росіян, російськомовних» та «насильницьку українізацію») тощо[9, с. 19]. Одним із напрямів фільтрації інформації про супротивника є приховування його успіхів і приховування втрат власних збройних сил.

Досить тривалий час російська верхівка використовуючи свої експансіоністські амбіції щодо України, намагається підпорядкувати її своєму впливу, примусово домінує та всіляко намагається демонструвати свою перевагу в ієрархії рівня впливу, з таким позиціонуванням, що представники інших груп – «чужі», а тому «вороги». Якщо «вороги» то можна вбивати, нищити?!

Тому одним із важливих «бойових завдань» у протидії інформаційній війни для України є проведення контрпропаганда, яка має виконувати випереджальну та викривальну функцію. Якісно продумана та ефективна діяльність державних та приватних структур, громадських активістів, щодо проведення контрпропаганди являє собою сукупність тих засобів, прийомів і методів, які спрямовані на нейтралізацію та протидію пропаганди ворожої сторони з метою протистояння її негативному впливу на свідомість громадян як то власної держави, ворогуючої держави так і світового співтовариства. У свідомості українців має бути сформована своя чітка позиція, стійкий імунітет до інформаційних впливів російської пропаганди. Держава повинна сприяти психологічній стабільності громадян України та викривати токсичну інформацію, нищити стереотипи та пропагандистські штампи, а також проводити роз'яснювальну роботу населенню щодо фейкової інформації з боку Російської Федерації.

#### Список використаних джерел

1. Про оборону України: Закон України від 6 грудня 1991 року. № 1932-ХІІ. URL: <https://zakon.rada.gov.ua/laws/show/1932-12/ed19911206>.
2. Про правовий режим воєнного стану: Закон України від 12 травня 2015 року. № 389-VIII. Відомості Верховної Ради України. 2015. № 28. Ст. 250
3. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. Вісник НАН України. 2014. № 5. С. 65–69.

4. Доктрина інформаційної безпеки України: Указ Президента України від 29.12.2016 р.№ 47/2017514/2009. URL: <https://www.president.gov.ua/documents/472017-21374?fbclid=IwAR3idC8nwxYZJm>

5. Ліпкан В.А., Максименко Ю.Є., В.М. Желіховський В.М Інформаційна безпека України в умовах євроінтеграції: Навч. посіб. К.: КНТ, 2006. С. 178.

6. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. Віче. 2007. №12. С. 23-25.

7. Про основи національної безпеки України: Закон України : від 19.06.2003 р. № 964-IV. ВВР України. 2003. № 39

8. Конституція України від 28 червня 1996 р. URL: <http://zakon5.rada.gov.ua/laws/show/254к/96-вр>

9. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В.О. Жадька; ред.-упор. О.І. Харитоненко, Ю.С. Полтавець. К., Вид-во НПУ імені М.П. Драгоманова, 2018. с. 319.

*Устинова І.П., к.ю.н., доц., доцентка  
кафедри конституційного і адміністративного права  
Національного авіаційного університету*

### **Правові питання нормативного регулювання електронних грошей в Україні**

Бурхливий розвиток фінансової системи в сучасних трансформаційних умовах потребує зміни процесів публічного адміністрування публічними фінансами. Зокрема, важливою складовою є контроль за адресністю використання виділених коштів з відповідних бюджетів за відповідними державними та місцевими програмами розвитку або інших напрямів фінансування. Сучасні методики фінансового контролю не можуть виконати відстеження стадії використання цих коштів фінальним споживачем без зміни цільового призначення. Електронні кошти є таким сучасним інструментом, який дозволить вирішити питання адміністрування публічних фінансів.

Початок історії виникнення електронних грошей сягає 1900-х рр., коли Федеральний резервний банк США вперше переказав гроші телеграфом. Але найбільш значною подією в історії появи електронних грошей є створення Девідом Чоумом, якого ще називали батьком електронних грошей, компанії "DigiCash", яка розпочала випуск перших електронних грошей міжнародної платіжної системи eCash. Для збереження надійності й анонімності проведених операцій Д. Чоум вигадав так звану систему «сліпого» цифрового підпису, яка полягала в тому, що емітент електронних грошей не бачив серійних номерів електронних банкнот але після здійснення відповідної перевірки ставив на них цифровий підпис, тим самим підтверджував їхню справжність [1]

Міжнародну платіжну систему eCash почали використовувати американські банки, зокрема Mark Twain Bancshares. Також у цей період у Європі була розроблена система PhonePaid, яка дозволяла проводити транзакції за допомогою мобільних телефонів [2, с. 142].

Що стосується України, то електронні гроші не набули такого стрімкого поширення і правового регулювання, як у США та Європі. Основними нормативно