

комплексної модернізації. Одним з напрямків таких перетворень, на думку автора, має стати формування управлінської культури нової якості, максимально адаптивної до потенційних змін і викликів сучасності. Для вітчизняної системи національної безпеки надзвичайно важливим уявляється також завдання збалансування її внутрішнього і зовнішнього вимірів, адже без створення сприятливого психологічного клімату в суспільстві неможливі успішні перетворення політичного, економічного, соціокультурного та безпекового характеру. Однією з провідних цілей модернізації системи національної безпеки має стати, на наше переконання, створення умов для формування екзистенційно комфортної (а значить і безпечної!) атмосфери в українському суспільстві.

### **Список використаних джерел**

1. Власюк О. С. Національна безпека України : еволюція проблеми внутрішньої політики : Вибрані наукові праці / О. С. Власюк. – К. : НІСД, 2016. – 528 с.

2. Особливості інформаційного забезпечення національного консенсусу в сучасній Україні : монографія / [В. Попик (кер. проекту), О. Онищенко, В. Горовий та ін.] ; НАН України, Національна бібліотека України ім. В. І. Вернадського. – К. : НБУ ім. В. І. Вернадського, 2016. – 220 с.

3. Особливості суспільно-політичної модернізації країн пострадянського простору : Монографія / За ред. А. Г. Бульвінського, ДУ «Інститут всесвітньої історії НАН України». – К. : ДУ «Інститут всесвітньої історії НАН України», 2017. – 288 с.

4. Hiatt, J. (2006). ADKAR : a model for change in Business, Government, and our community, Prosci, 146 pgs. 5. Семенець-Орлова І. Державне управління освітніми змінами в Україні : теоретичні засади : монографія / І. А. Семенець-Орлова. – К. : ЮСТОН, 2018. – 420 с.

**Васильківська І. П.**

к.ю.н., доцент

ДВНЗ “Київський національний економічний  
університет імені Вадима Гетьмана”

м. Київ, Україна

### **ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОГО ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

*Ключові слова: гібридні загрози, кримінальне право, злочини проти основ національної безпеки України, пропаганда, кібернетичні атаки.*



*Keywords: hybrid threats, criminal law, crimes against national security of Ukraine, propaganda, cybernetic attacks.*

З часів окупації Криму та військової агресії на Донбасі з боку Росії Україна опинилася в складних умовах, коли їй необхідно протистояти небезпекам, що породжені новим видом війни, так званим гібридним загрозам. Останні пов'язані з найбільш серйозними, найбрутальнішими порушеннями прав людини, можуть дестабілізувати й підірвати життя всього суспільства, спричинити особливо тяжкі наслідки.

Гібридна війна та небезпеки, які вона породжує, вимагають оперативного й ефективного реагування, уживання досить жорстких заходів. Особливу роль у системі подолання гібридних загроз відіграють кримінально-правові засоби. На цьому наголошує й Парламентська асамблея Ради Європи, яка у своїй резолюції, ухваленій 26 квітня 2018 року державами-членами для спільної протидії гібридним загрозам і війні, закріпила правило, відповідно до якого в разі невійськових дій реагування на гібридні загрози має здійснюватися, передусім, у межах національного кримінального права [1].

Дійсно, криміналізуючи найбільш небезпечні посягання, кримінальне право захищає найголовніші цінності від найбільш небезпечних посягань – злочинів. Водночас в умовах, коли тактики гібридної війни постійно розширюються, законодавець не завжди в змозі оперативно реагувати на сучасні виклики.

Цілком очевидно, що законодавство мирного часу не може повною мірою забезпечити регулювання правовідносин в умовах військових дій. Тому з початком російської агресії законодавець України вжив деяких заходів для створення кримінально-правових механізмів протидії небезпекам, що виникли. Насамперед, зміни торкнулися положень Кримінального кодексу України (далі – КК) [2], які встановлюють відповідальність за злочини проти основ національної безпеки України. З часів незалежності України відповідні норми широко не застосовувалися, однак через появу зовнішніх та внутрішніх загроз було посилено відповідальність за посягання, визначені розділом I Особливої частини КК, криміналізовано діяння, пов'язані з перешкоджанням законній діяльності Збройних Сил України та інших військових формувань (ст. 1141 КК), крім того, закріплено новелу щодо незастосування давності в разі вчинення злочинів, передбачених статтями 109-1141 КК [3; 4].

Законодавець також визначив кримінально-правові заходи протидії сепаратизму. Необхідність цього виникла у зв'язку зі штучним поширенням сепаратистських ідей в Україні, унаслідок чого відбулося силове протистояння в Донецькій та Луганській областях. У зв'язку з цим КК було доповнено статтею 1102, яка встановила кримінальну відповідальність за фінансування дій, вчинених з метою насильницької



зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України [5].

Водночас реалії гібридної війни, у яких опинилася Україна, зумовили потребу сформувати систему протидії новим загрозам засобами кримінального права, які не вирішені до цього часу. Зокрема, сьогодні, коли Україна перебуває в умовах агресивного інформаційного впливу Російської Федерації (а гібридна війна якраз і є комбінацією військових та невійськових дій, насамперед інформаційних), немає необхідного кримінально-правового механізму протидії пропаганді РФ. І це при тому, що боротьба з дезінформацією та деструктивною пропагандою з боку цієї країни називається одним із пріоритетів державної політики в інформаційній сфері [6].

Уважаємо, що мають бути криміналізовані найшкідливіші пропагандистські впливи, насамперед пропаганда, спрямована на насильницьку зміну чи повалення конституційного ладу або порушення суверенітету й територіальної цілісності України, і вважати це посягання потрібно злочином проти основ національної безпеки України. Це необхідно зробити, зважаючи на високий ступінь суспільної небезпечності відповідних дій та родовий об'єкт – суспільні відносини, які забезпечують державну безпеку, конституційний лад, суверенітет, територіальну цілісність і недоторканність нашої держави.

Україна стикається сьогодні ще з однією гібридною загрозою – кібернетичними атаками. Зокрема, наймасштабніша хакерська атака відбулася 27 червня 2017 року і здійснювалася за допомогою вірусної програми Petya.A. Тоді кібератака порушила роботу багатьох українських фінансових установ, енергетичних підприємств, засобів масової інформації, об'єктів транспорту та інфраструктури, телекомунікаційних мереж та інших організацій [7].

Особливу небезпечність становлять кібератаки проти інформаційних систем державних органів й об'єктів критичної інфраструктури України. До останніх належать підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами і наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства й безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [8].

Зважаючи на значну загрозу, яку створюють кібератаки такого роду національній безпеці України, правам та свободам людини і громадянина, варто відокремити їх від злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку й вважати злочинами проти основ національної безпеки України, включивши до об'єктивної сторони диверсії (ст. 113 КК).



Як бачимо, з початком гібридної війни розпочалася трансформація законодавства України про кримінальну відповідальність, що було зумовлено необхідністю відвернути безпосередню загрозу суверенітетові й територіальній цілісності нашої держави, правам та свободам людини і громадянина. Водночас постійне розширення тактик гібридної війни висуває на перший план завдання криміналізації найбільш суспільно небезпечних з них. Перспективними тут будуть дослідження досвіду інших країн щодо створення адекватних кримінально-правових механізмів протидії гібридним війнам та гібридним загрозам і визначення на цій основі шляхів удосконалення вітчизняних кримінально-правових норм.

### Список використаних джерел

1. Parliamentary Assembly. Resolution 2217 (2018). Legal challenges related to hybrid war and human rights obligations [Електронний ресурс]. – Режим доступу: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762&lang=en>

2. Кримінальний кодекс України від 05.04.2001 р. // Офіційний вісник України. – 2001. – № 21. – Ст. 920.

3. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо невідворотності покарання за окремі злочини проти основ національної безпеки, громадської безпеки та корупційні злочини: Закон України від 07.10.2014 р. // Відомості Верховної Ради України. – 2014. – № 46. – Ст. 2046.

4. Про внесення змін до Кримінального кодексу України: Закон України від 08.04.2014 р. // Відомості Верховної Ради України. – 2014. – № 23. – Ст. 867.

5. Про внесення зміни до Кримінального кодексу України щодо кримінальної відповідальності за фінансування сепаратизму: Закон України від 19.06.2014 р. // Відомості Верховної Ради України. – 2014. – № 32. – Ст. 1125.

6. Доктрина інформаційної безпеки України: Затверджена Указом Президента України від 25 лютого 2017 р. № 47/2017 // Офіційний вісник України. – 2017. – № 20. – Ст. 554.

7. Це війна: Україну потрясла найбільша в історії кібератака [Електронний ресурс]. – Режим доступу: <https://www.epravda.com.ua/publications/2017/06/27/626518/>

8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. // Офіційний вісник України. – 2017. – № 91. – Ст. 2765.