5. Lukianets-Shakhova, V., Ganus, L., Bryl, K., Nehoda, Y., & Rega, I. (2023). The Gender Policy of Ukraine: Considering the EU Experience. *Revista De Gestão Social E Ambiental*, 17(4), e03403. https://doi.org/10.24857/rgsa.v17n4-030.

6. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами–членами, з іншої сторони від 21.03.2014 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.

7. Справа Абдулазіз, Кабалес і Балкандалі: рішення Ради Європи та Європейського суду з прав людини від 28.05.1985 № 9214/80; 9473/81; 9474/81. Практика Європейського суду з прав людини. Рішення. Коментарі 2004. № 3 URL: https://ips.ligazakon.net/document/SO1181.

8. Рішення у справі «Unal Tekeli v. Turkey» № 29865/96 від 16.11.2004. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-67482.

9. Рішення у справі «Gozum v. Turkey» № 4789/10 від 15.01.2015. *European Court of Human Righ*ts. URL: http://hudoc.echr.coe.int/eng?i=001-150800.

10. Рішення усправі «Price v. The United Kingdom» № 33394/96 від 10.07.2001. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-59565.

Олійник Юрій Ярославович,
доцент кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Інформаційна безпека є одним із ключових елементів національної безпеки України в умовах воєнного стану. Світові тенденції зміни структури злочинності переконливо свідчать про зростання ролі інформаційно-телекомунікаційних технологій, які спричиняють появу принципово нових видів кримінальних правопорушень та активне вдосконалення «традиційної» злочинної діяльності [5, с. 313]. Комп'ютерні мережі, комунікаційні системи стали інструментом злочинців, унаслідок чого криміналізувалася сфера використання інформаційно-телекомунікаційних технологій. Одним із видів злочинної діяльності, що швидко прогресує разом з розвитком комунікаційних комп'ютерних систем, є злочинне використання мережі Інтернет шляхом розміщення в ній протиправного контенту [3; 4]. Інтернет наповнюється протиправним контентом і використовується з метою протиправної діяльності [5,

с. 313]. Масштабні кібератаки, інформаційні диверсії та кампанії дезінформації суттєво впливають на стійкість держави, її військову спроможність та моральний стан населення.

Особливої уваги потребує захист критичної інфраструктури: енергетичних мереж, банківських систем, державних реєстрів та комунікаційних каналів. В умовах гібридної війни інформаційні атаки можуть мати не менш руйнівний вплив, ніж фізичні бойові дії [7].

Серед пріоритетів удосконалення системи інформаційної безпеки слід виділити:

– створення системи оперативного моніторингу та реагування на кібератаки із застосуванням технологій штучного інтелекту;

– розвиток кіберполіції та спеціалізованих підрозділів у Збройних Силах України;

– адаптацію українського законодавства до міжнародних стандартів у сфері кіберзахисту;

– розширення співпраці з НАТО та ЄС щодо обміну даними і спільного реагування на загрози.

Інформаційна безпека в сучасному світі є однією з ключових складових національної безпеки. Особливого значення вона набуває в умовах воєнного стану, коли інформація перетворюється не лише на інструмент комунікації, а й на потужну зброю. Сучасні війни ведуться не лише на полі бою, а й у кіберпросторі та медійному середовищі, де боротьба точиться за свідомість людей, довіру громадян до держави та здатність суспільства протистояти паніці й дезінформації.

Правове регулювання інформаційної безпеки грунтується на ряду нормативно-правових актах [2]. Так, в Україні законодавчі основи інформаційної безпеки закріплені у низці нормативно-правових актів:

– Закон України «Про національну безпеку України» (2018 р.) визначає інформаційну безпеку як один із ключових напрямів захисту держави;

– Закон України «Про інформацію» (1992 р., із подальшими змінами) встановлює права громадян на доступ до достовірної інформації та регламентує відповідальність за поширення недостовірних відомостей;

– Кіберстратегія України (2021 р.) передбачає комплекс заходів для розвитку системи кіберзахисту, зокрема в умовах гібридної війни;

– Укази Президента та рішення РНБО вводять у дію санкції проти інформаційних ресурсів, які загрожують національній безпеці, зокрема проти пропагандистських телеканалів та онлайн-платформ.

Міжнародний досвід також має значення: рекомендації НАТО та ЄС у сфері кіберзахисту та протидії дезінформації стають орієнтирами для формування української політики інформаційної безпеки [6].

Збройна агресія завжди супроводжується масованими інформаційними атаками. Пропаганда, дезінформація, фейкові новини, маніпулятивні повідомлення та ворожі кібероперації спрямовані на підрив морального духу, послаблення довіри до влади, розпалювання внутрішніх конфліктів. В умовах воєнного стану особливо небезпечними стають спроби ворога поширювати паніку, дискредитувати Збройні сили та інші органи державної влади.

Україна, яка перебуває у стані широкомасштабної війни, щоденно стикається з гібридними загрозами [1]. Ворог намагається використати соціальні мережі, телеграм-канали, ботоферми для поширення фейкових повідомлень. Особливу небезпеку становить кіберзлочинність: атаки на критичну інфраструктуру, злам державних реєстрів, спроби паралізувати банківську систему чи енергетичний сектор.

В умовах воєнного стану держава зобов'язана розробляти й реалізовувати комплексні заходи для захисту інформаційного простору. Це включає:

– оперативне спростування фейків та чітке інформування населення;

– розвиток кіберзахисту та цифрової безпеки критичної інфраструктури;

– посилення відповідальності за колабораціонізм та поширення дезінформації;

– налагодження міжнародної співпраці у сфері кібербезпеки та медіаграмотності.

Водночас ефективна інформаційна безпека неможлива без активної участі громадян. Кожен українець має виявляти критичне мислення, перевіряти джерела інформації, не поширювати неперевірені чутки, дотримуватись інформаційної гігієни. Стійкість суспільства до інформаційних атак стає запорукою збереження єдності та здатності протистояти ворогу.

Інформаційна безпека в умовах воєнного стану – це питання виживання держави та суспільства. Вона забезпечується комплексом правових, організаційних, технологічних та просвітницьких заходів. Успішна протидія дезінформації та кіберзагрозам можлива лише за умови співпраці державних органів, громадянського суспільства та міжнародних партнерів.

Сьогодні інформаційна безпека України стала своєрідним «інформаційним щитом», що захищає не лише територію, а й свідомість, ідентичність та майбутнє українського народу.

Список бібліографічних посилань

1. Балюра А. О. Правові та організаційні основи здійснення оперативно-розшукової протидії злочинності оперативними підрозділами Національної поліції України. *Актуальні проблеми оперативно-розшукової протидії злочинам* : матеріали наук.-практ. семінару (м. Дніпро, 24 трав. 2018 р.). Дніпро : ДДУВС, 2018. С. 8–11.

2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI (зі змін. і доп.).

3.Науково-практичний коментар Кримінального кодексу України / [Д. С. Азаров, В. К. Грищук, А. В. Савченко та ін.] ; за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. 2-ге вид., переробл. і доповн. Київ : Юрінком Інтер, 2018. 1104 с.

4.Таран О. В., Вознюк А.А., Тарасенко О. С. та ін. Використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні: *метод. рек*. Київ, НАВС. 2021. 50 с.

5.Тарасенко О. С. Чинники, що сприяють вчиненню кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали VI Міжнар. наук.-практ. конф. (м. Дніпро, 11 бер. 2022 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. С. 308–309.

6. OECD. *Cybersecurity Policy Making at a Turning Point*. Paris: OECD Publishing, 2021. 38 с. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf.

7. European Union Agency for Cybersecurity (ENISA). *Threat Landscape Report*. Brussels, 2022. URL: https://eucyberdirect.eu/atlas/sources/enisa-threat-landscape-2022.

Панченко Наталія Володимирівна,
аспірант Інституту держави і права
імені В. М. Корецького НАН України

ТОЛЕРАНТНІСТЬ ДО НЕВИЗНАЧЕНОСТІ ЗА УМОВ КРИМІНАЛЬНО-ПРАВОВОЇ ПРАВОТВОРЧОСТІ ТА ПРАВОЗАСТОСУВАННЯ

Важливим під принципом верховенства права є правова визначеність, яка фактично є тією цінністю, до якої повинні прагнути розробники кримінального законодавства України. На нашу думку, правова невизначеність, є сутнісним відображенням природи юридичної регламентації кримінально-правових явищ, яка завжди притаманна, як і визначеність, тексту кримінально-правового припису. Визначеність та невизначеність не є антиподами чи парними категоріями. Вони є складовими одного явища, яке утворюється завдяки взаємодії визначеності та невизначеності, їх діалектичній єдності протилежності, що в кінцевому рахунку сприяє розвитку кримінально-правової матерії у бік точності та передбачуваності кримінального законодавства України в цілому.

Роздумуючи про спекулятивне законодавство, австро-британський економіст Фрідріх Август фон Хайєк відзначив, що терміни «незнання», «необізнаність» є занадто вузькими, а в окремих