

нормативно-правового регулювання, а й подальшого вдосконалення практики кваліфікації таких правопорушень, розвитку цифрової криміналістики та посилення міжвідомчої й міжнародної співпраці в цій сфері.

Список використаних джерел

1. Бабанін С. В. Кіберзлочинність: поняття та основні ознаки. *Вісник кримінального права*. 2019. URL: <https://vakp.nlu.edu.ua/article/view/173523>
2. Галушко О. М. Теоретико-правовий аналіз понять кіберзлочину та кіберзлочинності. *Підприємництво, господарство і право*. 2020. URL: <https://pb.univd.edu.ua/index.php/PB/article/view/131>
3. Русецький С. О. Кіберзлочинність: поняття та соціально-правова природа. 2025. URL: <https://vca.univd.edu.ua/index.php/vca/uk/article/view/516>
4. Аніщук Н. В. Історико-правові аспекти розвитку кіберзлочинності. 2023. URL: <https://journal-app.uzhnu.edu.ua/article/view/277954>
5. Ларченко М. В. Особливості розслідування кіберзлочинів. 2022. URL: <https://journals.lvduvs.lviv.ua/index.php/law/article/view/910>
6. Жевелева І. С. Кримінально-правова кваліфікація правопорушень у сфері використання електронно-обчислювальних машин, автоматизованих систем та комп'ютерних мереж. 2025. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/343949>
7. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III (зі змін. та доп.). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

Шубін Дмитрій Сергійович,
тимчасово виконуючий обов'язки
помічника командира військової
частини з правової роботи
(військова частина 5287,
Збройні Сили України)

ІНФОРМАЦІЙНА СТІЙКІСТЬ ДЕРЖАВИ ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

У XXI столітті інформація перетворилася на ключовий стратегічний ресурс, що визначає рівень національної безпеки держави. В умовах гібридної війни кіберпростір стає повноцінним театром бойових дій, де поряд із традиційними загрозами виникають нові форми впливу – інформаційно-психологічні операції, кібератаки та маніпуляції суспільною свідомістю.

Україна є одним із найбільш показових прикладів держави, яка одночасно здійснює цифрову трансформацію та протидіє масштабним кіберзагрозам. Атаки на енергетичну інфраструктуру, державні реєстри та інформаційні системи підтверджують необхідність формування комплексної системи кіберзахисту.

Сучасна модель забезпечення кібербезпеки має базуватися на принципах міжвідомчої взаємодії, адаптивності та проактивності. Важливим є не лише реагування на інциденти, а і їх попередження через аналітику загроз, упровадження штучного інтелекту та міжнародне співробітництво.

Особливу роль відіграє формування інформаційної стійкості суспільства. Це передбачає розвиток медіаграмотності, критичного мислення та здатності протистояти дезінформації. Людський фактор залишається найуразливішою ланкою у системі безпеки, що зумовлює необхідність системної просвітницької роботи.

Отже, кібербезпека й інформаційна стійкість є взаємопов'язаними елементами національної безпеки, що потребують інтегрованого підходу, поєднання правових, технологічних і соціальних механізмів.

Список використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України».
2. Стратегія кібербезпеки України.
3. Nye J. Soft Power and Cyber Power. Harvard University.
4. Castells M. The Rise of the Network Society.