2. Скочиляс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка».* Серія: Юридичні науки. 2024. № 2(42). С. 151–158.
3. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#top (дата звернення: 31.03.2026).
4. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 31.03.2026).
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 31.03.2026).
6. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 31.03.2026).
7. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 31.03.2026).
8. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 17.09.2021 № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/473/2021#Text (дата звернення: 31.03.2026).
9. Про контррозвідувальну діяльність: Закон України від 26.12.2002 № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text (дата звернення: 31.03.2026).
10. Data Protection Act 2018. *legislation.gov.uk* URL: https://www.legislation.gov.uk/ukpga/2018/12/contents (дата звернення: 31.03.2026).
11. Computer Misuse Act 1990. *legislation.gov.uk* URL: https://www.legislation.gov.uk/ukpga/1990/18/contents (дата звернення: 31.03.2026).
12. Official Secrets Act 1989. *legislation.gov.uk* URL: https://www.legislation.gov.uk/ukpga/1989/6/contents (дата звернення: 31.03.2026).
13. Investigatory Powers Act 2016. *legislation.gov.uk* URL: https://www.legislation.gov.uk/ukpga/2016/25/contents (дата звернення: 31.03.2026).
14. National Security and Investment Act 2021. *legislation.gov.uk* URL: https://www.legislation.gov.uk/ukpga/2021/25/contents (дата звернення: 31.03.2026).

ФІВКІН ПЕТРО МИКОЛАЙОВИЧ
начальник кафедри права національної безпеки та правової роботи Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

КОВТУНЕНКО СТАНІСЛАВ РОМАНОВИЧ
студент 2 курсу 1 групи кафедри підготовки офіцерів запасу Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

ПРОБЛЕМАТИКА РЕГУЛЮВАННЯ НАПРЯМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З початку війни росії проти України забезпечення державної безпеки стало основою для належного функціонування держави. Серед основних загроз, що постали в той час, стала інформаційна безпека та протидія дезінформації. При цьому правові механізми, що були розроблені для захисту країни, потребують подальшого удосконалення.

За час гібридної війни Україна зазнала значну кількість атак, спрямованих на підрив інформаційної безпеки держави. До них входять кібератака на об'єкти енергетики у грудні 2015 року, наслідком чого стало знеструмлення кількох областей, наприклад, кампанія з розповсюдження вірусу Petya, що спричинив масові збої в роботі державних установ, банків та інших організацій [2, с. 273-274]. Крім цього, у січні 2022 року несанкціонованого втручання зазнала і державна система «Дія», що порушило доступ до електронних послуг її користувачів [1, с. 366].

Під час повномасштабної агресії поширеним явищем стало розповсюдження дезінформації шляхом використання месенджерів. Зокрема, у березні 2023 в «Telegram», фіксували зростання кількості повідомлень, що містили фейкову інформацію про втрати Збройних Сил України [1, с. 366].

Протидію таким дестабілізуючим проявам було розроблено на рівні законів та підзаконних нормативно-правових актів, але їх система є досить розгалуженою. Проте, кожен з них містить окремі неточності, на які вказують науковці та правозастосовники, тому варто розглянути їх окремо:

- Закон України «Про основні засади забезпечення кібербезпеки України» [5] – регламентує захист критичної інфраструктури, проте не містить врегулювання штучного інтелекту (ШІ) чи блокчейну, які широко використовуються в кібератаках. Через цю проблему виникають ситуації, коли використовується ШІ для фішингових атак, проте їх неможливо належним чином зафіксувати через відсутність нормативного закріплення у законодавстві [1, с. 367];
- Закон України «Про інформацію» [3] - містить загальні принципи доступу, збирання і поширення інформації, права, обов'язки суб'єктів інформаційних відносин [6, с. 116], але між цим та попереднім нормативно-правовим актом існують колізії, що ускладнюють практику правозастосування [1, с. 367];
- Закон України «Про національну безпеку України» [4] – регламентує інформаційну безпеку як один із основних напрямків для забезпечення національної безпеки, що полягає у протидії дезінформації, пропаганді та кіберзагрозам [6, с. 116];
- Указ Президента України від 19 березня 2021 року № 106/2021 «Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації» [8] - створив нову інституцію – Центр протидії дезінформації (ЦПД) при Раді національної безпеки та оборони. Мета його діяльності полягає у виявленні та протидії дезінформаційним кампаніям, координації органів у цьому напрямі та співпраці з міжнародними партнерами [6, с. 116];
- Указ Президента України від 14 березня 2020 року № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» [7] – Стратегія національної безпеки України вперше на такому рівні (стратегічному) затвердила завдання інформаційної політики у сфері гібридної війни [6, с. 116] та інші.

Разом із тим, існуюче нормативне регулювання є фрагментарним щодо впровадження конкретних механізмів протидії загрозам інформаційній безпеці, попри наявну системність [6, с. 116].

Що ж стосується органів для протидії цим загрозам, то станом на зараз це: Рада національної безпеки і оборони України, ЦПД при РНБО, Міністерство культури України, Державна служба спеціального зв'язку та захисту інформації України. Проте, ані в рамкових документах, ані в практиці цих відомств належним чином не здійснено координацію чи розподіл повноважень, що призводить до їх дублювання між інституціями [6, с. 117]. Так, у 2023 у ході судового розгляду було виявлено дублювання повноважень між РНБО та Міністерством культури, внаслідок чого відбулась затримка в ухваленні рішень [1, с. 367].

Разом з тим, не вся державна політика з цього напряму є провальною. Так, у 2022 році відбулась співпраця Міністерства цифрової трансформації України з Microsoft. Завдяки цьому скоротились на 25% витрати на кіберзахист, так як відбувався обмін технологіями. Зважаючи на цей позитивний досвід, науковцями запропонована модель юридичної особи, яка б увібрала у себе українські ІТ- компанії, по типу Ajax Systems та в співпраці з міжнародними лідерами – як-

то Google, Microsoft, сфокусувалась би на регіональних потребах, що сприяло б у використанні передових технічних і правових ресурсів [1, с. 368].

Отже, національне законодавство у сфері інформаційної безпеки є великим за обсягом, але доволі недоопрацьованим за змістом. Внаслідок цього воно не регулює належним чином відповідь та протидію загрозам у цій сфері, а також призводить до проблем у практиці правозастосування уповноваженими органами. Досвід, отриманий внаслідок співпраці з закордонними компаніями свідчить про швидший розвиток регулювання цього напряму саме цим шляхом, тому необхідним є поглиблення такої співпраці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горулько В. В. Основні напрями удосконалення законодавства України з інформаційної безпеки в умовах війни. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2025. Вип. 88: частина 2. С. 364–370.
2. Димитрієв В. В. Інформаційна безпека як пріоритет державної політики України. *Держава та регіони*. Серія: Державне управління. 2020. № 2 (70). С. 272–278.
3. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII (з наступ. змін. та доповн.). URL: https://zakon.rada.gov.ua/laws/show/2657-12.
4. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII (з наступ. змін. та доповн.). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
5. Про основні засади забезпечення кібербезпеки в Україні: Закон України від 5 жовтня 2017 року № 2163-VIII (з наступ. змін. та доповн.). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
6. Пашковський В. Ф. Ідентифікація політико-правових механізмів інформаційної безпеки держави в умовах гібридної війни. *Політичне життя*. 2025. № 3. С. 114–120.
7. Стратегія національної безпеки України: затв. Указом Президента України від 14.09.2020 р. № 392/2020 (з наступ. змін. та доповн.). URL: https://zakon.rada.gov.ua/go/392/2020.
8. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: введене в дію Указом Президента України від 19.03.2021 р. № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text.

ХАДЖИНОВ АНДРІЙ ВОЛОДИМИРОВИЧ
Командир 3 відділення 123 навчальної групи факультету забезпечення державної безпеки Київського інституту Національної гвардії України

САХНЕВИЧ БОРИС ВАЛЕРІЙОВИЧ
кандидат економічних наук, заступник начальника кафедри бойового та логістичного забезпечення факультету службово-бойової діяльності НГУ Київського інституту Національної гвардії України

ІННОВАЦІЙНІ ЛОГІСТИЧНІ СИСТЕМИ В УМОВАХ ВІЙНИ

Впровадження інноваційних підходів у логістичну сферу в період воєнного стану перестало бути питанням конкурентної переваги, перетворившись на фундаментальну умову національного виживання. Актуальність дослідження зумовлена безпрецедентним руйнуванням традиційних транспортних вузлів, що потребує негайного переосмислення методів управління потоками. Метою роботи є аналіз практичного застосування новітніх логістичних систем, що інтегрують