Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Прилуцька Крістіна Вікторівна,
курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Інформаційна безпека є критично важливим аспектом сучасного суспільства, особливо в умовах воєнного стану, коли загрози кібератак, дезінформації та шпигунства набувають стратегічного значення. В Україні, де воєнний стан діє з 24 лютого 2022 року, забезпечення інформаційної безпеки стало одним із пріоритетів національної безпеки.

Доктрина інформаційної безпеки України визначає інформаційну безпеку як важливу самостійну сферу забезпечення національної безпеки [1]. Указом Президента України № 685/2021 від 15.10.2021 р. було схвалено Стратегію інформаційної безпеки [2]. Її метою є регулювання інформаційної безпеки на нормативно-правому рівні, посилення можливостей щодо забезпечення інформаційної безпеки України, інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, охорони суверенітету та цілісності України, демократії, прав та свобод людини і громадянина. Таким чином закладалися основи національної та інформаційної безпеки в інформаційній сфері [3, с. 51].

Інформаційна безпека – це стан, за якого в умовах дії реальних і потенційних загроз забезпечується самозбереження, сталий та прогресивний розвиток інформаційної сфери, в тому числі захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб’єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері [4, с. 77-78; 5, с. 411].

Необхідно погодитись з У. Андрусів, який наголошує на тому, що під час воєнного стану інформація стає не лише ресурсом, а й засобом ведення війни. Посиленими є кібер- та інформаційна активність ворога, збільшуються масовані інформаційні атаки, широко використовуються соціальні мережі, перш за все для дестабілізації громадської думки та ін. За таких умов інформаційна безпека охоплює не лише технічні аспекти, а й стратегічну комунікацію, контрпропаганду, контроль над інформаційними потоками [6, с. 33].

Відповідно до ДСТУ ISO/IEC 29146:2023 «Інформаційні технології. Методи безпеки. Структура керування доступом» [7], методи захисту інформаційних систем включають організаційні, технічні та фізичні заходи, спрямовані на управління ризиками інформаційної безпеки.

У контексті воєнного стану особливу увагу приділяється методам, які дозволяють ефективно реагувати на динамічні загрози. Зокрема серед них доречно виділити:

❖ Правові методи – базуються на законодавстві України, зокрема, Законах України: «Про захист інформації в інформаційно-телекомунікаційних системах» [8], «Про державну таємницю» [9] та «Про захист персональних даних» [10], Закон України «Про основні засади забезпечення кібербезпеки України» [11]. Ці акти формують законодавчу основу, яка визначає правила обігу інформації, права суб'єктів, обов'язки операторів та порядок реагування на кіберінциденти.

❖ Організаційні методи – передбачають створення структур і процедур, спрямованих на управління інформаційною безпекою. Вони включають розробку політик безпеки, навчання та аудит інформаційних систем. У воєнний час до таких методів належать:

- *розробка політики безпеки*. В Україні створюються комплексні системи захисту інформації, які відповідають вимогам законодавства та міжнародним стандартам.
- *навчання та інструктажі*. Проведення тренінгів для працівників щодо кібергігієни, зокрема уникнення фішингових атак, є критично важливим в умовах воєнного стану.
- *аудит і контроль*. Регулярний аудит інформаційних систем дозволяє виявляти порушення та вдосконалювати заходи безпеки [12, с. 56].

❖ Технічні методи – охоплює застосування засобів технічного захисту інформації. Вони включають використання апаратних і програмних засобів для захисту інформації. До таких методів відносять:

- *антивірусний захист*. Використання сучасних антивірусних програм дозволяє виявляти та нейтралізувати шкідливе програмне забезпечення.
- *криптографічний захист* (шифрування даних, електронний цифровий підпис). Зокрема, шифрування є ключовим методом захисту інформації під час її передачі та зберігання. Особливо важливим даний метод є для захисту комунікацій між військовими підрозділами, державними органами.
- *резервне копіювання та відновлення даних*;
- *системи контролю доступу й логування* для обмеження прав доступу та фіксації дій користувачів;
- *багатофакторна аутентифікація* для посиленої перевірки особистості [13].

Розвиток технологій на основі штучного інтелекту і машинного навчання також відкриває нові можливості у виявленні та реагуванні на загрози [14].

❖ Інформаційні методи – спрямовані на протидію дезінформації та інформаційним впливам, які є частиною гібридної війни. До них належать:

- *моніторинг інформаційного простору*. Виявлення дезінформаційних кампаній та їх нейтралізація.
- *проведення інформаційних кампаній*. Зокрема, актуальним є проведення роз'яснення громадянам правил кібергігієни та процедур реагування на кіберзагрози.

❖ Соціальні та психолого-комунікаційні методи. Зокрема, соціальні методи ґрунтуються на розумінні поведінки користувачів у цифровому середовищі [15]. Для забезпечення інформаційної безпеки важливим є врахування людського чинника. Основними заходами є:

- формування навичок цифрової гігієни;
- психологічна діагностика та профілактика внутрішніх загроз.

Ефективне забезпечення ІБ вимагає комплексного підходу, що передбачає взаємодію між усіма методами. Слушною з цього питання є і позиція, яка наголошує на тому, що в умовах воєнного стану інформаційна безпека України має базуватися на синхронізованих діях різних структур держави та громадянського суспільства [3, с. 55]. Доречним, на наш погляд, є використання штучного інтелекту для загроз та автоматизації захисту. Також важливим є обмін досвідом та технологіями з державами-партнерами, міжнародними організаціями.

Підсумовуючи вищевикладене, можна сказати, що забезпечення інформаційної безпеки в умовах воєнного стану є комплексним завданням, яке вимагає поєднання технічних, організаційних, правових та інформаційних методів. Сучасні методи інформаційної безпеки мають адаптуватися до нових викликів, таких як кіберзагрози, гібридні впливи, зростання ролі соціальних мереж. Ключем до успіху є постійне оновлення знань, інтеграція технологій та активна участь усіх суб’єктів інформаційного середовища.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017 URL: https://zakon.rada.gov.ua/laws/show/47/2017#n2
2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7
3. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна*, Серія «Питання політології», 2022. Випуск 42. С. 50-57.
4. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис… д-ра. юрид. наук : 12.00.07. Ужгород. 2019. 487 с.
5. Моргун Н.С., Шевчук О.О., Марчевський С.В. Щодо визначення поняття інформаційної безпеки у діяльності Національній поліції України. *Електронне наукове видання «Аналітично-порівняльне правознавство».* С. 409-415. URL: https://app-journal.in.ua/wp-content/uploads/2024/08/69.pdf
6. Андрусів У. Інформаційна безпека в умовах війни: нові виклики і відповіді. *Інформаційне право України*. 2023. № 1. С. 31–35.
7. Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів: Наказ ДП"УкрНДНЦ" від 17.08.2023 № 210. URL: https://zakon.rada.gov.ua/rada/show/v0210774-23#Text

8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
9. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
10. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
11. 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
12. Бачинська О. А. Організаційні аспекти забезпечення інформаційної безпеки в Україні. *Держава та регіони. Серія: Право*. 2022. № 1. С. 55–59.
13. Інформаційна безпека: що це таке, види та засоби захисту. https://voll.kiev.ua/uk/blog/informacijna-bezpeka-sho-ce-take-vidi-ta-zasobi-zahistu
14. Yakimenko I., Yermakov V. AI and ML in Cybersecurity: Opportunities and Risks. *Cybersecurity Journal*. 2023. Vol. 9№. 2. P. 33–39.
15. Садовська І. Психологічні аспекти інформаційної безпеки. *Психологія і суспільство*. 2021. № 2. С. 78–84.
16. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна,* Серія «Питання політології», 2022, випуск 42. С. 50-57.

Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Трофимчук Дарія Юріївна,
курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

ОБМЕЖЕННЯ СВОБОДИ СЛОВА ТА ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН ПІД ЧАС ВОЄННОГО СТАНУ

Свобода слова та право на інформацію є фундаментальними складовими демократичного суспільства, закріпленими як у національному законодавстві, так і в міжнародно-правових актах. Однак, в умовах війни, держава може обґрунтовано застосовувати обмеження на ці права задля захисту національної безпеки, суспільного порядку та обороноздатності. Такі обмеження мають тимчасовий характер і повинні відповідати принципам пропорційності, необхідності та законності.

Право на свободу вираження поглядів гарантується статтею 34 Конституції України [1], а також статтею 10 Конвенції про захист прав людини і