7. Молокова А.Р., Бухтіярова І.Г. Особливості діяльності патрульної поліції в період воєнного стану. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 6. С. 632-637. URL: https://app-journal.in.ua/wp-content/uploads/2024/12/105.pdf

Лось Дар'я Ігорівна,
студент факультету фінансів Київського національного економічного університету імені Вадима Гетьмана

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПОВОЄННИЙ ПЕРІОД

Інформаційна безпека у сучасному світі є ключовою складовою національної безпеки, особливо в умовах збройного конфлікту. З початком повномасштабної агресії рф проти України у 2022 році, питання захисту інформаційного простору стало життєво важливим [5, с. 52–58]. Війна XXI століття ведеться не лише на полі бою, але й у кіберпросторі, на телебаченні, в соціальних мережах, у месенджерах. Саме тому ефективне забезпечення інформаційної безпеки у період воєнного стану та в післявоєнній відбудові є пріоритетом державної політики [6, с. 18-24].

Воєнний стан в Україні запроваджується згідно із Законом України «Про правовий режим воєнного стану» [1]. Цей правовий режим передбачає тимчасове обмеження низки прав і свобод, включаючи свободу слова, з метою захисту інтересів держави. Відповідно до ст. 22 Закону, в умовах воєнного стану можуть запроваджуватися: цензура інформації; обмеження роботи ЗМІ; заборона на поширення певної інформації, що може завдати шкоди обороноздатності [1].

Серед ключових загроз можна виділити: дезінформацію та фейки, кіберзагрози, психологічні операції (PSYOPS), витік конфіденційної інформації [7, с. 44-49]. Для протидії цим загрозам Україна активізувала діяльність Центру протидії дезінформації при РНБО [4], Служби безпеки України, а також волонтерських ініціатив.

Інформаційна політика в період війни має подвійне завдання: захист державної таємниці і національних інтересів, а також забезпечення прозорості, інформування громадян і формування стійкості суспільства [6, с. 18-24]. Успішною практикою є щоденні брифінги, робота офіційних каналів, оперативна реакція на фейки.

Після завершення активної фази війни Україна зіткнеться з такими викликами: реінтеграція деокупованих територій, поствоєнна реабілітація суспільства, відновлення національного медіапростору, протидія гібридним впливам. Особливої уваги потребуватимуть: медіаграмотність, удосконалення законодавства, розвиток аналітичної інфраструктури.

Інформаційна безпека в умовах війни та після неї є фундаментом для стійкості, виживання та відновлення держави. Ефективне законодавче

регулювання, стратегічна комунікація, розвиток інформаційної культури та технологічної інфраструктури мають бути основою державної політики [3].

Додатково варто наголосити на важливості співпраці з міжнародними партнерами у сфері інформаційної безпеки. Україна активно інтегрується в європейський інформаційний простір, бере участь у спільних ініціативах з ЄС та НАТО щодо кіберзахисту, обміну розвідувальною інформацією та протидії дезінформації [5, с. 52-58].

Окрему увагу слід приділити ролі освіти, зокрема розвитку медіаосвітніх програм у школах, університетах, а також для дорослого населення. Формування критичного мислення та навичок розпізнавання інформаційних впливів є запорукою стійкості суспільства до пропаганди.

Не менш важливим є удосконалення національного законодавства в частині кібербезпеки, захисту персональних даних, регулювання діяльності соціальних мереж та платформ онлайн-комунікації. Потрібно забезпечити баланс між безпекою та свободою слова, не допустивши зловживання владними повноваженнями [2]. Пропонуємо внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», доповнивши його обов'язковими галузевими стандартами та національною сертифікацією критичних інформаційних систем, жорсткими строками повідомлення про інциденти, ризик-орієнтованим підходом та державним резервом експертів; водночас оновити Закон України «Про захист персональних даних», запровадивши право переносу, видалення й обмеження обробки даних, закріпивши принцип захисту даних «з проєктування» й «за замовчуванням», наділивши контролюючий орган правом планових і позапланових перевірок із значними санкціями та публічним реєстром витоків і строком інформування до 72 годин; а в частині онлайн-платформ доповнити Закон України «Про інформацію» та Закон України «Про електронні комунікації» визначенням категорій великих сервісів за розміром аудиторії, вимогами до модерації й звітності, прозорістю алгоритмів та незалежними аудитами, забороною реклами для користувачів до 16 років, чіткими строками реагування на скарги й судовим контролем доступу до даних, координуючи все через спеціальну міжвідомчу раду з урахуванням міжнародного досвіду та обов'язкових навчальних програм для фахівців.

У повоєнний період держава повинна підтримувати розвиток незалежних медіа, які дотримуються журналістських стандартів, та сприяти зміцненню громадянського суспільства як активного учасника інформаційного захисту країни.

Висновок. Інформаційна безпека в умовах воєнного стану та у повоєнний період є не лише елементом національної безпеки, а й інструментом збереження державності, суверенітету та суспільної єдності. Успішна протидія ворожим інформаційним впливам потребує поєднання правових, технологічних, освітніх і комунікаційних заходів [5, 6].

Забезпечення інформаційної безпеки суспільства в умовах війни та в повоєнний час вимагає комплексного підходу, який поєднує правове регулювання, технологічні рішення й культивування медіаграмотності громадян. По-перше, необхідно адаптувати законодавчі норми до реалій воєнного стану –

передбачити пріоритетність захисту критичної інфраструктури, оперативний обмін розвідувальною інформацією та чіткі механізми протидії дезінформації. По-друге, у повоєнний період варто закріпити набуті зусилля через довгострокові програми модернізації систем кібербезпеки, підвищення кваліфікації державних службовців і фахівців ІТ-галузі та формування в суспільстві критичного сприйняття джерел інформації. Лише синергія жорстких норм, інноваційних технологій і просвітницьких ініціатив може створити стійку систему інформаційної безпеки, здатну захистити державу й громадян як під час загрози, так і на етапі відновлення.

Список використаних джерел

1. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. URL:https://zakon.rada.gov.ua/laws/show/389-19#Text\.
2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#Text.
3. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 14.02.2017 р. № 47/2017 URL:https://zakon.rada.gov.ua/laws/show/47/2017#Text
4. Центр протидії дезінформації при РНБО України – Офіційний сайт, URL:https://cpd.gov.ua/
5. Ситник І.І. Інформаційна безпека в умовах гібридної війни: національний і міжнародний виміри. *Вісник НАДУ при Президентові України*. 2022. № 1. С. 52–58.
6. Костюченко О.В. Інформаційна політика держави в умовах воєнного стану. *Національна безпека і оборона*. 2023. № 2(158). С. 18–24.
7. StopFake.org. Платформа протидії дезінформації: URL:https://www.stopfake.org/.

Майсук Романа Романівна,
студент навчально-наукового інституту права та психології Національної академії внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ВОЄННОГО СТАНУ: ПРАВОВІ ВИКЛИКИ ТА ПРАВОЗАСТОСУВАННЯ

В наш час, в умовах воєнного стану, ще більш актуального значення набуває безпека, особливо коли відбувається не лише фізична, але й інформаційна агресія. Забезпечення інформаційної безпеки набуває критичної важливості та запобігає спробам посіяти паніку серед населення. Широке використання цифрових технологій зумовлює появу нових форм загроз, таких як кібератаки, дезінформація та маніпулювання інформацією. Однією з основних правових проблем є необхідність розробки нормативно-правових актів, які б ефективно регулювали захист від кібератак, забезпечували прозорість у використанні