2. Рябчун Ю. «Реалізація прав і свобод особи в умовах воєнного стану». Право і громадянське суспільство. URL:https://plr.nlu.edu.ua/article/view/287927/285662

3. Закон України «Про захист персональних даних» URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

4. Державний центр кіберзахисту / Держспецзв'язку. Рекомендації та правила обміну інформацією про кіберінциденти. URL: https://scpc.gov.ua/uk/recommendations

5. Правова допомога переселенцям - співпраця Міністерства/БФ і мережі БПД. - Безоплатна правнича допомога. URL: https://legalaid.gov.ua/novyny/pravova-dopomoga-pereselenczyam-u-spivpraczi-z-bf-pravo-na-zahyst/

6. Інформація для ВПО - приклади місцевих практик (інформаційні сторінки громад щодо медичної допомоги та соціальних послуг). URL: https://kozlivska-gromada.gov.ua/informaciya-dlya-vpo-15-17-05-28-02-2025/

Демедюк Марина Сергіївна
здобувачка ступеня вищої освіти
бакалавра ННЕКІ
Національної академії внутрішніх справ
Славна Оксана Володимирівна
професор кафедри
конституційного права та прав людини
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент

ПРАВА ЛЮДИНИ У КІБЕРПРОСТОРІ: НОВІ ЗАГРОЗИ ТА ЮРИДИЧНІ МЕХАНІЗМИ ЗАХИСТУ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

За сучасних геополітичних викликів кібербезпека розглядається держави як складова їх національної безпеки. Для України дослідження прав людини у кіберпросторі, їх загроз та захисту є надто актуальним у зв'язку із дією в державі воєнного стану, який запроваджено у 2018 р. відповідно до Закону України «Про правовий режим воєнного стану» (від 12.05.2015 р. №389-VIII) [3] та продовжено внаслідок повномасштабної агресії проти України з боку рф 24.02.2022 р. (Указ Президента України «Про введення воєнного стану в Україні» від 24.02.2022 р. №64/2022) [5].

У контексті збройних конфліктів права людини в інформаційній та кіберпросторовій сферах зазнають систематичних порушень, що становить загрозу для фундаментальних гарантій свободи вираження та доступу до даних. У науковій літературі ці права класифікують на інформаційні та цифрові; інформаційні, закріплені в статті 34 Конституції України, охоплюють свободу думки і слова, право на вільне вираження поглядів і переконань, а також на збір, зберігання, використання та поширення інформації в усній, письмовій або

іншій формі за власним вибором. [1]. Щодо цифрових прав людини, їх визначення відсутнє, проте, на нашу думку, до таких прав слід віднести свободу вираження поглядів та особисту безпеку онлайн, право на приватність і захист персональних даних, на цифрове самовизначення та на відключення від онлайну тощо.

Загалом, під кіберпростором розуміють середовище для можливих злочинних дій у вигляді кібератак [9, с.165]. Україна стала об'єктом систематичних кібератак ще за умов гібридної агресії росії, починаючи з 1990-х років. Такі злочинні дії були спрямовані на дестабілізацію критичної інфраструктури, державних інституцій та економічної системи, створення дезінформації для цивільного населення, здійснення кібершпигунства [10, с.114]. Сьогодні війна проти України стала підставою для виникнення нових загроз у сфері прав людини у кіберпросторі. Зокрема це стосується перешкоджань у сфері надання електронних послуг громадянам України, порушення цілісності та конфіденційності їх персональних відомостей, застосування проти цивільного населення інформаційно-психологічних операцій (дезінформативних вкидів, пропаганди тощо). З боку агресора здійснюються фішингові та цільові кібератаки на критичну інфраструктуру держави, посилено кібершпигунство та кібертероризм у воєнній, безпековій та економічній сферах [8, с.93]. Також має місце порушення права на публікування цифрових медіа (зокрема, щодо контенту про російсько-українську війну), закріпленого ст. 19 Загальної декларації прав людини [2].

Слід зазначити, що юридичні механізми захисту права людини у кіберпросторі включають як нормативно-правові, так і організаційно-правові засади. Зокрема, інформаційні та деякі цифрові права людини врегульовано, окрім Загальної декларації прав людини, нормами МППЛ та ЄКПЛ (ст. 8 та 10).

У контексті національного законодавства кожна держава формулює власне трактування поняття кібербезпеки як фундаментальної складової забезпечення захисту прав і свобод людини в цифровому середовищі. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» від 2017 р., кібербезпека визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору» [4]. Повномасштабне вторгнення, розпочате 24 лютого 2022 р., стало каталізатором подальшого еволюціонування українського правового поля в частині гарантування прав людини в кіберпросторі. Зокрема, у 2023-2024 рр. було схвалено план заходів з реалізації Стратегії кібербезпеки України, який у 2025 р. зазнав суттєвих оновлень та розширень. Крім того, у поточному році ухвалено Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», що, поміж іншого, передбачає формування єдиної системи реагування на кібератаки як інструменту оперативного нейтралізації загроз.

Отже, у контексті воєнного стану, запровадженого Указом Президента № 64/2022, правове регулювання кібербезпеки в Україні, як гарантії захисту інформаційних та цифрових прав людини, демонструє еволюцію від базових

норм Закону "Про кібербезпеку" 2017 р. до розширених заходів 2023–2025 рр., включаючи Стратегію кібербезпеки та Закон про кіберзахист, що передбачає єдину систему реагування на загрози; проте для забезпечення стійкості цифрового середовища необхідне подальше гармонізування з міжнародними стандартами (ЄКПЛ ст. 10, МППЛ), посилення координації суб'єктів (СБУ, РНБО, приватний сектор) та впровадження превентивних індивідуальних механізмів, аби протидіяти гібридним атакам РФ і утвердити права людини як основу національної безпеки в кіберпросторі.

У контексті організаційно-правового механізму забезпечення прав людини в кіберпросторі Україна характеризується багатошаровою системою державних суб'єктів, які реалізують компетенції з кібербезпеки в межах законодавчо визначених повноважень. Зокрема, до ключових акторів належать Кабінет Міністрів України, центральні органи виконавчої влади (Міністерство оборони України, Міністерство внутрішніх справ України через Управління боротьби з кіберзлочинністю, Міністерство закордонних справ України), місцеві державні адміністрації, органи місцевого самоврядування, Уповноважений Верховної Ради України з прав людини, Збройні Сили України, Служба безпеки України, Національна поліція України, Державна служба спеціального зв'язку та захисту інформації України, Національний координаційний центр кібербезпеки (при Раді національної безпеки і оборони України), Національний банк України, а також підприємства, установи та організації, віднесені до об'єктів критичної інформаційної інфраструктури, що забезпечують комплексний підхід до протидії загрозам у цифровому середовищі. Крім того, вищезгаданим Законом України 2025 року передбачено запровадження посадових осіб, відповідальних за кібербезпеку в структурах органів державної влади, а також активне залучення приватного сектору до формування комплексної системи захисту кіберпростору. У контексті воєнного стану механізм гарантування прав людини в цифровому середовищі доповнюється індивідуальними превентивними заходами, такими як забезпечення конфіденційності персональних даних та уникнення потенційно небезпечних мережевих ресурсів. Врешті-решт, для відновлення порушених інформаційних чи цифрових прав громадяни України мають можливість звертатися до судових інстанцій загальної юрисдикції, Конституційного Суду України, Європейського суду з прав людини або до недержавних організацій, які надають спеціалізовану юридичну та правозахисну допомогу в цій сфері. [7, с.53-54]. Отже, комплексне вдосконалення правового регулювання кіберпростору в Україні, з інтеграцією міжнародних стандартів та фокусом на превентивних заходах, є критичним для посилення національної стійкості, гарантування прав людини в цифровому середовищі та запобігання ескалації гібридних загроз у довгостроковій перспективі.

Окремо варто акцентувати увагу на проблематиці правового регулювання застосування штучного інтелекту в кіберпросторі в умовах воєнного стану, що зумовлює суттєве посилення ризиків кібершпигунства в оборонній сфері. На сучасному етапі в міжнародному праві відсутні спеціалізовані норми, які б чітко визначали принципи та межі використання штучного інтелекту в

контексті збройних конфліктів, що створює прогалини в забезпеченні правової визначеності та безпеки.

Хоча, російська агресія щодо України сприяла початку розвитку таких норм. Зокрема, 2020 р. було схвалено Концепцію розвитку штучного інтелекту в Україні. У травні 2023 року Міністерством закордонних справ України спільно з міжнародними партнерами було започатковано новий інструмент співпраці в кіберпросторі (Талліннський механізм), спрямований на допомогу Україні із самообороною в кіберпросторі на тлі протидії російській агресії. А у липні того ж року підписано Спільну декларацію країн - членів Group of 7, яка, зокрема, передбачає підтримку ініціативи з кіберзахисту для протидії гібридним загрозам [11, с.170].

Особливої уваги варте створення в НААУ робочої групи з правового регулювання штучного інтелекту. Дана група займається аналізом важливих юридичних питань розвитку штучного інтелекту щодо визначення меж його використання в різних галузях, захисту персональних даних, формулювання правил щодо збереження та застосування зібраних систем штучного інтелекту тощо [6, с.48]. Для правового регулювання використання штучного інтелекту було б доцільно розглянути питання розробки національного кодексу етики ШІ, що включатиме обов'язкові стандарти захисту персональних даних та обмеження використання технологій у критичних галузях, з метою гармонізації українського законодавства з європейськими нормами (GDPR) та забезпечення національної безпеки в умовах цифрової трансформації.

Отже, на сучасному етапі Україна володіє розвиненою системою механізмів гарантування прав людини в кіберпросторі під час дії воєнного стану, однак національне законодавство потребує подальшої гармонізації з міжнародними стандартами з урахуванням найкращих зарубіжних практик для забезпечення комплексної стійкості та ефективності протидії гібридним загрозам.

У сучасних геополітичних реаліях кібербезпека як невід'ємна складова національної безпеки України набуває стратегічного значення, особливо в умовах воєнного стану, запровадженого Указом Президента № 64/2022 від 24 лютого 2022 р. та продовженого відповідно до Закону № 389-VIII. Дослідження підкреслює, що порушення прав людини у кіберпросторі - від інформаційних (ст. 34 Конституції України) до цифрових (приватність, безпека онлайн) - посилюється гібридними атаками РФ, що включають кібершпигунство, дезінформацію та загрози критичній інфраструктурі, починаючи з 1990-х років. Нормативно-правова база (Закон «Про кібербезпеку» 2017 р., Стратегія кібербезпеки 2023–2025 рр.) та організаційні суб'єкти (СБУ, Нацполіція, РНБО) забезпечують базовий захист, гармонізований з міжнародними стандартами (ЄКПЛ ст. 10, МППЛ), але потребують посилення регулювання ШІ та персональних даних.

Перспективи розвитку охоплюють інтеграцію глобального досвіду, ухвалення Інформаційного кодексу України для уніфікації цифрових прав та розширення міжнародної співпраці (Талліннський механізм, декларація G7 2023 р.). Комплексний підхід - юридичний, інституційний та індивідуальний - є

ключем до запобігання загрозам, відновлення довіри та сталого розвитку кіберпростору.

Список використаних джерел:

1. Конституція України від 28.06.1996 р. № 254к/96-ВР. URL:https://zakon.rada.gov.ua/laws/main/254%D0%BA/96-%D0%B2%D1%80

2. Загальна декларація прав людини від 10.12.1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015

3. Про правовий режим воєнного стану: Закон України від 12.05.2015 р. №389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19/stru

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

5. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 р. №64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022/conv

6. Гульванська Ю.А. Правове регулювання кібербезпеки в Україні: сучасний стан та перспективи розвитку. *Інформація і право*. 2024. № 2(49). С. 45–52.

7. Гусаров С. М. Адміністративно-правове забезпечення інформаційної безпеки в Україні в період дії правового режиму воєнного стану. *Сучасні проблеми правового, економічного та соціального розвитку держави.* МВС України. Нац. акад. прав. Наук. України. Вінниця. ХНУВС. 2024. С. 52-54.

8. Денисенко К.В., Борко І.С., Косов О.М. Реалізація цифрових та інформаційних прав людини в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2023. Випуск 77: частина 1. С.90-94.

9. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства.* 2025. № 2 (42). С.164-171.

10. Марущак А. І. Стратегія кібербезпеки України: правові засади та механізми реалізації. *Вісник Національного університету «Львівська політехніка». Юридичні науки.* 2024. № 2(38). С. 112–119.

11. Шемчук В. В., Костенко О. Л. Кіберпростір як сфера національної безпеки: правові засади забезпечення. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 167–174.