6. UNHCR. Ukraine Refugee Situation: Operational Data Portal. URL: https://data.unhcr.org/en/situations/ukraine
7. Керівні принципи ООН щодо внутрішнього переміщення / розроб. Ф. Денг. Нью-Йорк : ООН, 1998. 40 с. (Doc. E/CN.4/1998/53/Add.2).
8. Council Directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons. Official Journal of the European Communities. 2001. L 212. P. 12–23.
9. Іванюта С., Якушенко Л. Пріоритети забезпечення екологічної безпеки України в умовах російської воєнної агресії : аналітична доповідь. Київ : НІСД, 2024. 61 с. URL: https://doi.org/10.53679/NISS-analytrep.2024.11
10. United Nations Environment Programme. Environmental Impact of the Kakhovka Dam Destruction. Nairobi : UNEP, 2023. 48 p.
11. Stop Ecocide International. Independent Expert Panel for the Legal Definition of Ecocide: Commentary and Core Text. 2021. URL: https://www.stopecocide.earth
12. United Nations General Assembly. Resolution 76/300 «The human right to a clean, healthy and sustainable environment». 28 July 2022. Doc. A/RES/76/300.

УДК 340.1

Мазепа С. О.
к.ю.н., доцент, доцент кафедри кримінального права та процесу Західноукраїнського національного університету, міжнародний дослідник Оснабрюцького університету

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВА УМОВА ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В УМОВАХ МІГРАЦІЇ

Міграція є складним соціально-правовим явищем, що супроводжується не лише зміною місця проживання, а й істотною трансформацією звичного середовища людини: мовного, побутового, правового, соціального та цифрового. Мігранти належать до особливо вразливих категорій населення, оскільки в умовах переїзду, невизначеності, стресу та адаптації вони можуть бути менш уважними до питань особистої безпеки, зокрема безпеки у цифровому просторі. Саме тому кібербезпека в контексті міграції має розглядатися не лише як технічне питання, а як важлива передумова забезпечення фундаментальних прав людини.

У сучасних умовах мігранти активно користуються цифровими сервісами для оформлення документів, подання заяв, отримання адміністративних, соціальних, гуманітарних, медичних і правових послуг,

пошуку житла, роботи, комунікації з державними органами, міжнародними організаціями та волонтерськими ініціативами. У процесі такої взаємодії особа часто завантажує копії документів, повідомляє персональні дані, адресу перебування, інформацію про членів сім'ї, дітей, стан здоров'я, правовий статус або підстави міграції. Втрата, незаконне використання або компрометація таких даних може мати для мігранта особливо тяжкі наслідки. У цьому контексті насамперед ідеться про право на приватність і захист персональних даних. Це право набуває особливого значення тоді, коли обробляються чутливі дані осіб, які перебувають у залежному або вразливому становищі. Водночас кібербезпека пов'язана і з іншими правами людини: правом на безпеку, правом на недискримінацію, правом на доступ до інформації та адміністративних послуг, а також правом на ефективний правовий захист. Якщо цифровий профіль особи буде зламано, документи викрадено, а персональні дані використано для шахрайства, це може фактично унеможливити реалізацію її прав у країні перебування.

Особливе місце у захисті мігрантів посідає кібергігієна — сукупність базових практик безпечної поведінки в цифровому середовищі. Європейське агентство з кібербезпеки ENISA визначає кібергігієну як прості практики й кроки, які допомагають захистити персональну інформацію та пристрої від кіберзагроз. ENISA також акцентує на важливості просвітницьких кампаній, спрямованих на формування безпечної поведінки користувачів у цифровому середовищі. До базових правил кібергігієни, які мають особливе значення для мігрантів, належать: використання сильних і унікальних паролів; увімкнення двофакторної автентифікації; регулярне оновлення програмного забезпечення на мобільних телефонах і комп'ютерах; обережне користування публічними або незнайомими Wi-Fi мережами; використання антивірусного захисту; резервне збереження важливих документів як у цифровому, так і в паперовому вигляді. Такі заходи дають змогу зменшити ризик несанкціонованого доступу до електронних кабінетів, зміни або блокування інформації, викрадення документів, фінансового шахрайства чи витоку персональних даних.

Окрему загрозу становлять фішингові та таргетовані фішингові атаки. Мігранти можуть отримувати шахрайські повідомлення, які імітують офіційні листи від державних органів, банків, служб доставки, міграційних установ, гуманітарних організацій або платформ з пошуку житла та роботи. З розвитком штучного інтелекту такі повідомлення можуть бути граматично правильними, персоналізованими й переконливими. Перехід за небезпечним посиланням або введення персональних даних на підробленому ресурсі може призвести до компрометації облікового запису, втрати доступу до документів, викрадення даних або їх незаконного поширення. Тому важливим напрямом захисту прав мігрантів є не лише технічний захист цифрових сервісів, а й системна просвітницька робота. Мігранти повинні мати доступ до зрозумілої

інформації про актуальні кіберзагрози, ознаки фішингових повідомлень, правила безпечної роботи з документами, алгоритми реагування на кіберінциденти та порядок звернення до компетентних органів. Особливе значення має інформування доступною мовою, з урахуванням рівня цифрової грамотності, правового статусу та життєвих обставин особи.

Справжнім викликом для сучасної системи захисту прав людини є також використання штучного інтелекту в цифрових сервісах, пов'язаних із міграцією. ШІ може застосовуватися для обробки заяв, перевірки документів, ідентифікації особи, аналізу ризиків, класифікації звернень або автоматизації адміністративних процедур. Такі технології можуть спрощувати доступ до послуг, однак водночас створюють ризики неправомірної обробки персональних даних, автоматизованого профілювання, дискримінації, помилкових рішень, витоку або компрометації інформації.

У разі успішної кібератаки важливим є не лише запобігання інциденту, а й здатність цифрової системи швидко виявити атаку, локалізувати її, зупинити подальше поширення та мінімізувати шкоду для особи. Саме тому сучасне розуміння кібербезпеки охоплює не лише індивідуальну кібергігієну користувача, а й кіберстійкість цифрової інфраструктури, в межах якої обробляються дані мігрантів.

У цьому аспекті особливе значення мають європейські стандарти та нормативні акти. Зокрема, Директива NIS2 спрямована на забезпечення високого спільного рівня кібербезпеки в Європейському Союзі, посилює вимоги до управління ризиками та повідомлення про значні інциденти. Важливим є також Cyber Resilience Act, який встановлює горизонтальні вимоги кібербезпеки до продуктів із цифровими елементами, зокрема програмного й апаратного забезпечення. У контексті використання штучного інтелекту релевантним є AI Act, який закріплює ризик-орієнтований підхід до регулювання систем ШІ.

Отже, кібербезпека є важливою умовою реального, а не лише формального забезпечення прав людини в умовах міграції. Вона охоплює захист персональних даних, безпечний доступ до цифрових сервісів, протидію шахрайству, фішингу та кіберзлочинності, а також належне регулювання технологій штучного інтелекту. Ефективний захист мігрантів у цифровому середовищі має ґрунтуватися на поєднанні трьох елементів: підвищення рівня кібергігієни самих користувачів; відповідальності державних і приватних цифрових сервісів за безпечну обробку даних; впровадження європейських стандартів кіберстійкості, управління ризиками, реагування на інциденти та безпечного використання штучного інтелекту.

ЛІТЕРАТУРА:

1. Cyber Hygiene / European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/topics/cyber-hygiene (дата звернення: 03.04.2026).

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). Official Journal of the European Union. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 03.04.2026).
3. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (дата звернення: 03.04.2026).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act). Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 03.04.2026).

УДК 340.1

Семенова О. Г.
адвокат, член комітету НААУ
з питань сімейного права,
аспірантка відділу цивільно-правових наук
Інституту держави і права імені В. М. Корецького
НАН України

ПЕРЕМІЩЕННЯ ГРОМАДЯН В УМОВАХ ВІЙНИ ТА ЗАБЕЗПЕЧЕННЯ ПРАВА НА УТРИМАННЯ ОДНОГО З ПОДРУЖЖЯ ТА ДІТЕЙ

Переміщення громадян України в умовах воєнного стану відбувається не лише в межах країни, а і за її межі в інші держави. І якщо в межах України для внутрішньо переміщених осіб забезпечення права на утримання може в мінімальному розмірі забезпечуватися державою, в якості підтримки вразливих категорій населення, то для тих громадян, хто виїхав за кордон, не передбачено жодних виплат Україною в якості підтримки.

На національному законодавчому рівні право на утримання (аліменти) другого з подружжя та дітей регулюються нормами Сімейного кодексу України, Закону України «Про забезпечення прав і свобод внутрішню переміщених осіб» та низькою постанов Кабінету Міністрів України, які постійно оновлюється.

На міжнародному рівні обов’язок на утримання закріплений,