

П. С. Іваніцький

аспірант кафедри теорії права та прав людини
юридичний факультет

Чернівецького національного університету ім. Юрія Федьковича

ІНТЕРНЕТ-ШАХРАЙСТВО: ЗАГРОЗИ ПРАВАМ ЛЮДИНИ ТА МЕХАНІЗМИ ЇХНЬОГО ЗАХИСТУ

Стаття присвячена аналізу інтернет-шахрайства як зростаючої загрози правам людини в умовах цифрового простору та використання Інтернет-технологій. Зі стрімким розвитком інформаційних технологій та поширенням доступу до глобальної мережі такі кіберзлочини як шахрайство стають однією із ключових проблем у адаптації до проблем пов'язаних із сучасними технологіями. Такі види злочинів не лише завдають фінансових та економічних збитків громадянам та державам, але й прямо порушують фундаментальні права людини, такі як право на захист персональних даних, право на приватність чи свободу вираження поглядів. У статті досліджують основні форми Інтернет-шахрайства, їхній вплив на права людини а також національні та міжнародні інструменти та засоби правового та комплексного захисту, що протидіють таким загрозам. Особливу увагу приділено правовим, технічним та соціальним механізмам, які можуть мінімізувати ризики та забезпечити ефективний захист прав людини у контексті цифрового простору. На основі вивченої наукової літератури та міжнародного та національного законодавства сформовано перелік основних перспектив розвитку механізмів захисту прав людини від Інтернет-шахрайства та основні види такого шахрайства. Стверджується, що лише міжнародна співпраця, гармонізація національного законодавства до міжнародних рекомендацій та комплексний підхід у тому числі правовий, соціальний, технологічний та освітній, до забезпечення прав людини в контексті їхнього порушення за допомогою шахрайських схем в мережі зможуть мінімізувати ризики таких злочинів.

Ключові слова: права людини, Інтернет, шахрайство, обмеження прав людини, цифрові технології, засоби захисту прав людини, право на захист персональних даних.

Постановка проблеми. Стрімкий розвиток інформаційних технологій і масовість такого явища як глобальна мережа спричинила низку викликів, пов'язаних зі злочинами в мережі, зокрема Інтернет-шахрайством. Цей вид злочинної діяльності охоплює вкрай широкий спектр протиправних дій, таких як фішинг, крадіжка персональних даних, шахрайство у сфері електронної комерції, тощо, які завдають суттєвого збитку як користувачам мережі так і державам і суспільству загалом. Проблема полягає в тому, що сучасні механізми захисту прав людини, передбачені нормами міжнародного та національного законодавства не завжди встигають адаптуватись до появи нових загроз пов'язаних з розвитком сучасних та швидкості змін технологій та Інтернет-мережі

зокрема. Для забезпечення ефективного захисту прав людини умовах зростання інтернет-шахрайства, враховуючи його транскордонний характер, швидкість розвитку та вразливість окремих груп суспільства потрібно дослідити основні форми інтернет-шахрайства, оцінити їхній вплив на права людини та проаналізувати чинні міжнародні та національні механізми захисту, щоб потім зможти запропонувати чіткі перспективи розвитку комплексного підходу до протидії кіберзлочинам, зокрема Інтернет-шахрайству.

Метою дослідження є комплексний аналіз Інтернет-шахрайства як загрози правам людини в цифровому просторі, виявлення основних форм такого шахрайства та оцінку його впливу на фундаментальні права людини.

Ступінь наукової розробки проблематики. Проблема Інтернет-шахрайства є доволі новою, зважаючи на те, що Інтернет є новим технологічним механізмом у суспільстві. Так, проблема впливу інтернет-шахрайства на фундаментальні права людини досліджували такі вітчизняні та іноземні науковці як: Ковальчук А. А., Материнська О., Петренко С. М., Джонсон М., Браун Т., Балагур Ю. А., Шапочка С. В., Руденко Я. П., та іншими. Водночас питання впливу Інтернет шахрайства на права людини та механізми їхнього захисту в контексті використання глобальної мережі є актуальним та досі залишається недостатньо дослідженим.

Виклад основного матеріалу. Інтернет-шахрайство є одною з найпоширеніших загроз для прав людини у світі розвитку інформаційних технологій, оскільки таке шахрайство прямо порушує право на приватність, безпеку особи, захист даних в мережі та економічні права людини. У епоху розвитку цифрових технологій шахрайство в глобальній мережі Інтернет набуває всеосяжних форм та видів, що вкрай ускладнює захист прав громадян. Так, до основних видів Інтернет-шахрайства відносять:

1. «Фішинг» – один з найпоширеніших видів шахрайства в Інтернеті, що спрямований на викрадення особистих даних особи, таких як паролі, номери банківських карток чи інші відомості які містять конфіденційну інформацію. Злочинці використовують вебсайти подібні до офіційних, електронні листи чи повідомлення в мережі, що імітують офіційних характер та «ніби то» надіслані з офіційних джерел. Для прикладу: зловмисник може надіслати електронний лист від імені банку, вимагаючи підтвердження паролів чи особистих даних. Це прямо порушує право на захист персональних даних, передбачене Загальним регламентом про захист даних (GDPR) та іншими міжнародними нормативно-правовими актами, зокрема статті 8 Європейської конвенції про захист прав людини та основоположних свобод.

2. Шахрайство зі здійснення онлайн покупок. Насамперед це продаж неіснуючих товарів, підробку сертифікатів якості чи обман із доставкою товарів із засто-

суванням мережевих технологій. Жертви такого шахрайства втрачають кошти, що прямо порушує їхні економічні права, зокрема право на захист споживачів. Згідно з дослідженнями вітчизняних науковців, шахрайство в електронній комерції становить значну часту кіберзлочинів [8, с. 45–52].

3. Соціальна інженерія. Такий вид Інтернет-шахрайства передбачає маніпуляцію жертвами для отримання доступу до їхніх даних або до фінансових ресурсів атакованої особи. Для прикладу: шахрай може видавати себе за технічну підтримку чи представника державної установи задля отримання неправомірної вигоди. Це прямо загрожує праву людини на безпеку та захист від обману, що є складовою права людини на гідність.

4. Криптовалютні афери та фінансові піраміди. У зв'язку зі зростанням популярності криптовалют з'явилося безліч схем для того, щоб обманювати людей, як наприклад шахрайські інвестиційні платформи чи фальшиві спроби купити/продати криптовалюту. Через це зокрема зросла і кількість фінансових пірамід від шахраїв. Такі дії зловмисників порушують право на власність, оскільки жертви втрачають свої фінансові ресурси, якщо потрапляють у такі шахрайські махінації.

5. Кібербулінг та дезінформація. Такі види шахрайства рідко поєднанні з матеріальними втратами, проте становлять значну часту в порушеннях прав людей за допомогою шахрайства. Кібербулінг в глобальній мережі більше зосереджений серед молоді, що прямо порушує право на психологічну недоторканість та свободу вираження поглядів в мережі, що може в подальшому зробити поштовх для людини у деякі шахрайські схеми чи махінації. Дезінформація у свою чергу, наприклад через фейкові новини, можуть маніпулювати думкою суспільства, що несе у собі загрозу як для прав людини так і для свободи в інформаційному просторі.

Згідно з міжнародними та вітчизняними дослідженнями кіберзлочини стають системним викликом для правового регулювання та прав людини загалом, оскільки норми національного законодавства та міжнародного права часто не встигають

адаптуватись до розвитку новітніх технологій. Материнська О. А. та Кучук А. Р. додають з цього приводу: «Провідними загрозами безпеці банківських операцій у Інтернеті є кібератаки, серед яких найнебезпечнішими є фішинг, «зараження» персональних комп'ютерів шкідливим програмним забезпеченням та недостатня безпека мобільних операційних систем.» [9, с. 48–52]. Так, Інтернет-шахрайство має прямий вплив на низку прав людини:

- **Право на приватність.** Викрадення даних через хакерські атаки, фішинг, систематичні порушення права на захист персональної інформації.

- **Право на власність.** Шахрайство в глобальній мережі у вигляді фейкових онлайн-магазинів чи фінансових пірамід обмежують та є серйозною загрозою для економічних прав людини.

- **Право на безпеку.** Соціальні інженерія, кібербулінг, розвиток новітніх технологій створюють неосяжну загрозу для психологічної та фізичної безпеки користувачі мережі.

- **Право на свободу вираження поглядів.** В мережі існує безліч способів дезінформувати особу та обмежити її доступ до достовірної інформації, впливаючи на свободу думки особи.

Інтернет-шахрайство становить серйозну загрозу правам людини, включаючи такі права як право на приватність, безпеку та власність. Ефективних захист таких прав вимагає комплексного поєднання правових, технологічних та освітніх заходів. Міжнародна співпраця та гармонізація національного законодавства відповідно до міжнародних рекомендацій є критично важливим для протидії усім формам злочинів в мережі Інтернет. [2, с. 23–34]. Таким чином можна виділити основні перспективи для розвитку механізмів захисту прав людини в контексті Інтернет-шахрайства:

- 1. Правові механізми.** Міжнародні нормативно-правові акти, такі як Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), встановлюють чіткі стандарти для того, щоб боротись з Інтернет-шахрайством, в свою чергу рекомендує країнам на національному рівні впроваджувати закони про захист

прав людини в мережі, захист персональних даних [7], тощо. Національні законодавства багатьох країн світу не встигають адаптуватись до швидкості розвитку інформаційних технологій та зокрема шахрайських технологій, тому акцент має бути на гнучкості законодавства та умінні його адаптуватись до будь яких нових викликів.

- 2. Технологічні заходи.** Більшість сучасних технологій, сайтів, соціальних мереж передбачають самозахист від шахрайського впливу такі як двофакторна автентифікація, антивірусне програмне забезпечення яке навчене розпізнавати більшість загроз в мережі та шифрування даних, яке допомагає зменшити ризики для персональних даних осіб. Такі великі корпорації як Google та Microsoft розробляють інструменти для виявлення фішингових та хакерських атак в мережі. Зрозуміло, що нормативно-правове забезпечення таких технологічних заходів повинне відповідати міжнародним стандартам та бути імplementованим у національне законодавство [1, с. 112–125].

- 3. Освітні програми.** Цифрова грамотність та її підвищення є основою для захисту прав людей в мережі Інтернет. Освітні кампанії, які навчають розпізнавати шахрайські схеми та ризики щодо порушення прав громадян значно можуть знизити кількість жертв, які піддалися на протиправний вплив шахраїв [12, с. 67–73].

- 4. Міжнародна співпраця.** Транскордонний характер відносин в мережі Інтернет значно ускладнює захист порушених прав людини. Необхідно нарощувати співпрацю на міжнародному рівні для захисту обміну інформації та переслідуванні злочинців. Такі міжнародні організації як Інтерпол та Європол беруть активну участь у цьому напрямку.

Інтернет-шахрайство є однією з основних загроз для прав людини в мережі Інтернет, зокрема права на захист персональних даних, права на приватність, свободу вираження поглядів чи економічну безпеку людей. Більшість шахрайських схем в мережі призводять до порушення конфіденційності, дискримінації, фінансових втрат та обмеженню доступу до інформації через дезінформацію. Основні форми інтернет-шахрайства (фішинг, крадіжка

особистих даних, злочинні схеми в електронній комерції) створюють низку значних викликів для окремих осіб-користувачів Інтернет-мережі, так і для суспільства та держав загалом.

Висновки. Узагальнюючи, можна сказати, що для ефективного правового захисту прав людини необхідно застосувати комплексний підхід, що включає в себе посилення законодавства (розробку та вдосконалення нормативно-правової бази для боротьби з кіберзлочинністю, а також гармонізація законодавств країн з міжнародними стандартами), технологічні заходи (застосування сучасних систем кібербезпеки, шифрування даних, моніторинг підозрілої активності), освітні кампанії (підвищення цифрової грамотності громадян через навчання безпечного використання Інтернет-мережі, розпізнавання шахрайських схем та самозахисту особистих даних), співпраця на міжнародному рівні (координація зусиль між країнами світу для обміну інформацією, розслідування злочинів, що мають транскордонний характер задля притягнення злочинців до відповідальності), а також підтримка жертв Інтернет-злочинів (створення доступних для громадян засобів та інструментів компенсації завданої шкоди, правової підтримки та психологічної підтримки особам, що постраждали від Інтернет-шахрайства.

Тільки через поєднання правових, соціальних, освітніх та технологічних заходів можливо мінімізувати загрози, які несе в собі Інтернет-шахрайство, щоб забезпечити надійний та всеосяжний захист прав людини в цифровому просторі.

Список використаної літератури:

1. Johnson M. Technological Approaches to Combating Phishing Attacks. *IEEE Transactions on Information Security*. 2021. Vol. 15, No. 3. P. 112–125.
2. Smith J., Brown T. Cybersecurity and Human Rights: Challenges in the Digital Age. *Journal of Cybersecurity*. 2022. Vol. 8, No. 1. P. 23–34.
3. Балагур Ю. А. Проблеми безпеки електронної комерції в мережі Інтернет : тези доп. IV наук.-практ. конф. (м. Одеса, 7–8 червня 2018 р.). Одеса, 2018. С. 118–120.
4. Бенедек В., Кетteman М. Свобода вираження поглядів та Інтернет. Видавництво Ради Європи F-67075 Strasbourg Cedex. 2013. URL: <https://rm.coe.int/168059936a>
5. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал*. 2021. № 10. С. 58–61. doi: <https://doi.org/10.32782/2524-0374/2021-10/12>
6. Володовська В. Заборони та свободи в Інтернеті: як виглядатиме Декларація цифрових прав людини. 2019. URL: https://zmina.info/articles/zaboroni_ta_svobodi_v_interneti_jiak_vigljadatime_deklaracijia_cifrovih_prav_ljudini/
7. Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. С. 481.
8. Ковальчук А. А. Кіберзлочинність у сфері електронної комерції: сучасні виклики та протидія. *Юридичний вісник України*. 2023. № 2. С. 45–52.
9. Материнська О., Кучук А. Безпека банківських операцій у мережі інтернет. *Реалії та перспективи розбудови правової держави в Україні та світі* : Матеріали VII Міжнар. науково-практ. конф., м. Суми, 31 трав. – 1 черв. 2024 р. С. 48–52.
10. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.
11. Мусієнко О.Л. Теоретичні засади розслідування шахрайства в сучасних умовах : автореф. дис. ... канд. юрид. наук : 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність»; Нац. юрид. акад. України ім. Ярослава Мудрого.
12. Петренко С. М. Цифрова грамотність як інструмент протидії кібершахрайству. *Науковий вісник Київського національного університету*. 2024. № 1. С. 67–73.
13. Руденко Я.П. Класифікація сучасних методів Інтернетшахрайств. Матеріали наукової Інтернет-конференції. Ірпінь, 2017. С. 128–129.
14. Фалалєєва Л. Права людини та екстра-територіальна дія права ЄС: еволюція практики застосування юрисдикційних моделей. *Вісник Київського національного університету імені Тараса Шевченка. Міжнародні відносини*. 2017. 1(46). С. 91–97.

15. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 1 (32). С. 145–149.
16. Шапочка С. В. Шахрайство у сфері використання всесвітньої мережі Інтернет. *Спеціальна техніка у правоохоронній діяльності* : тези доп. V Міжн. наук.-практ. конф. (Київ, 25 листоп. 2011 р.). К. : НАВС, 2011 С. 31–35.
-

Ivanitskyi P. Internet Fraud: Threats to Human Rights and Mechanisms for Their Protection

The article is dedicated to the analysis of internet fraud as a growing threat to human rights in the context of the digital environment and the use of internet technologies. With the rapid development of information technologies and the widespread access to the global network, cybercrimes such as fraud have become one of the key challenges in adapting to issues related to modern technologies. These types of crimes not only cause financial and economic losses to individuals and states but also directly violate fundamental human rights, such as the right to protection of personal data, the right to privacy, and the freedom of expression. The article examines the main forms of internet fraud, their impact on human rights, as well as national and international instruments and mechanisms for legal and comprehensive protection to counter such threats.

Special attention is given to legal, technical, and social mechanisms that can minimize risks and ensure effective protection of human rights in the digital space. Based on the reviewed scientific literature and international and national legislation, a list of key prospects for the development of mechanisms to protect human rights from internet fraud and the primary types of such fraud is formulated. It is argued that only through international cooperation, harmonization of national legislation with international recommendations, and a comprehensive approach – including legal, social, technological, and educational measures – to ensuring human rights in the context of their violation through fraudulent schemes online can the risks of such crimes be minimized.

Key words: human rights, internet, fraud, restriction of human rights, digital technologies, mechanisms for human rights protection, right to protection of personal data.