

Кримінальне право

УДК 343:004.738.5:004.056.5

DOI <https://doi.org/10.5281/zenodo.13963487>

Інтеграція кримінального права в стратегії розвитку кібербезпеки соціальних мереж: аналітичний погляд

Кундеус Владислав Геннадійович,

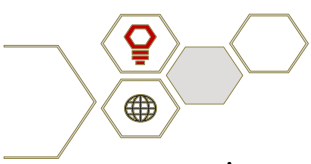
кандидат юридичних наук, доцент кафедри кримінального права та
кримінології, Харківський національний університет внутрішніх справ,
61080, м. Харків, просп. Льва Ландау 27, Україна,
<https://orcid.org/0000-0002-2430-5437>

Татаркіна Юлія Ігорівна,

кандидат юридичних наук, доцент кафедри кримінального права та
кримінології, Харківський національний університет внутрішніх справ,
61080, м. Харків, просп. Льва Ландау 27, Україна,
<https://orcid.org/0000-0002-5975-7636>

Прийнято: 28.09.2024 | Опубліковано: 21.10.2024

Анотація: Упродовж останніх років кількість користувачів соціальних мереж значно збільшилася, що призвело до поширення нових видів кіберзлочинності, таких як: фішинг, вішинг, скимінг (викрадення реквізитів платіжних карток); кардінг (незаконні фінансові операції з використанням платіжних карток або їх реквізитів); онлайн-шахрайство (заволодіння коштами через фіктивні інтернет-магазини); піратство (незаконне розповсюдження програмних продуктів через комп'ютерні мережі) тощо. Мета статті полягає в

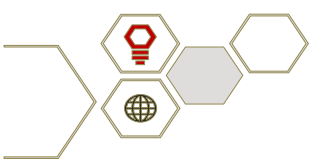


дослідженні особливостей і механізмів державного регулювання та впровадження кримінального права в стратегії розвитку кібербезпеки соціальних мереж в Україні. Основна увага зосереджена на аналізуванні національного та міжнародного законодавства, зокрема Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року та українських нормативно-правових актів, таких як: Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року №96/2016, Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про основні засади забезпечення кібербезпеки України», положення Кримінального кодексу України, що спрямовані на правове забезпечення охорони кібербезпеки в протидії кіберзлочинам, вчиненим через соціальні мережі.

У статті виявлені та проаналізовані прогалини у правовому регулюванні, зокрема відсутність міжнародних механізмів співпраці, відсталість від сучасних технологій та складність у відстеженні анонімності вчинення таких злочинів. Підкреслюється важливість інтеграції кримінального права як найбільш ефективного засобу в системі протидії кіберзлочинності в стратегії розвитку кібербезпеки в системі національної безпеки України. Наголошується на необхідності розробки інноваційних підходів у розслідуванні кіберзлочинів, включно з використанням новітніх технологій і методів аналізу даних, а також підвищенням обізнаності про ризики, пов'язані з використанням соціальних мереж. Важливість цього дослідження полягає в тому, що його метою є встановлення правових меж кримінальної відповідальності за кіберзлочини, вчинені через сайти соціальних мереж, і визначення рівня кримінально-правового забезпечення охорони кібербезпеки.

Ключові слова: соціальні мережі, комп'ютерне шахрайство, кіберзлочини, безпека, кримінальна відповідальність.

Integration of Criminal Law in the Development Strategy of Cybersecurity in Social Networks: An Analytical View



Vladyslav Kundeus,

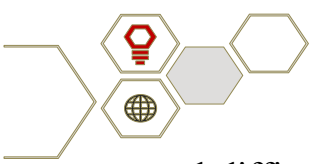
Candidate of Legal Sciences, Associate Professor, Department of Criminal
Law and Criminology, Kharkiv National University of Internal Affairs,
61080, Kharkiv, Ave. L. Landau 27, Ukraine,
<https://orcid.org/0000-0002-2430-5437>

Yuliia Tatarkina,

Candidate of Legal Sciences, Associate Professor, Department of Criminal
Law and Criminology, Kharkiv National University of Internal Affairs,
61080, Kharkiv, Ave. L. Landau 27, Ukraine,
<https://orcid.org/0000-0002-5975-7636>

Abstract: In recent years, the number of social media users has increased significantly, which has led to the spread of new types of cybercrime, such as: phishing, vishing, skimming (theft of payment card details); carding (illegal financial transactions using payment cards or their details); online fraud (misappropriation of funds through fictitious online stores); piracy (illegal distribution of software products via computer networks), etc. The purpose of the article is to study the peculiarities and mechanisms of state regulation and implementation of criminal law in the strategy of development of cybersecurity of social networks in Ukraine. The main focus is on the analysis of national and international legislation, in particular, the Council of Europe Convention on Cybercrime of 23.11.2001 and Ukrainian regulations, such as: The Cybersecurity Strategy of Ukraine approved by the Decree of the President of Ukraine No. 96/2016 dated March 15, 2016, the Law of Ukraine “On Protection of Information in Information and Communication Systems”, the Law of Ukraine “On Basic Principles of Cybersecurity of Ukraine”, and the provisions of the Criminal Code of Ukraine aimed at legal support of cybersecurity protection in countering cybercrime committed through social networks.

The article identifies and analyzes the gaps in legal regulation, in particular, the lack of international cooperation mechanisms, backwardness of modern technologies

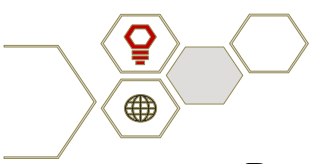


and difficulty in tracking the anonymity of such crimes. The author emphasizes the importance of integrating criminal law as the most effective tool in the system of combating cybercrime into the strategy for the development of cybersecurity in the national security system of Ukraine. The author emphasizes the need to develop innovative approaches to the investigation of cybercrime, including the use of the latest technologies and methods of data analysis, as well as raising awareness of the risks associated with the use of social media. The importance of this study lies in the fact that its purpose is to establish the legal limits of criminal liability for cybercrime committed through social media sites and to determine the level of criminal law support for cybersecurity protection.

Keywords: social networks, computer fraud, cybercrime, security, criminal liability.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. За останні кілька років кількість користувачів соціальних мереж значно збільшилася. У 2020 році кількість користувачів соціальних медіа досягла 2,5 мільярдів осіб у всьому світі. За два роки ця цифра зросла до 3,5 мільярдів. Це еквівалентно збільшенню на 29% і 45% кількості населення світу. Однак багато людей не розуміють значення цих цифр та їх вплив на безпеку й конфіденційність соціальних мереж.

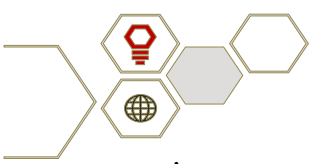
Інтеграція кримінального права в стратегії розвитку кібербезпеки соціальних мереж є ключовим аспектом забезпечення правопорядку в цифровому середовищі. Ключовою ознакою правопорушень, скоєних через соціальні медіа, є їх миттєве та публічне поширення. Одного натискання кнопки достатньо для вчинення протиправних дій у будь-якому куточку світу з доступом до мережі «Інтернет». Злочини, пов'язані з використанням платформ соціальних мереж, здебільшого стосуються або самого вебресурсу, який допускає публікацію незаконного контенту, або дій користувачів, які поширюють цей контент, навіть якщо це заборонено правилами платформи.



Важливим аспектом цієї проблеми є складність ідентифікації справжнього правопорушника через багаторівневу структуру інтернет-послуг. Соціальні мережі стають середовищем та інструментом для вчинення різноманітних правопорушень у кіберпросторі. Проблема виникає у встановленні як юридичних, так фактичних підстав кримінальної відповідальності за такі дії. Це ускладнюється значною кількістю залучених інтернет-суб'єктів, зокрема постачальників доступу до інтернету, хостинг-платформ, постачальників інформаційного контенту та інших послуг, які забезпечують функціонування соціальних мереж.

Крім того, однією з проблем є відсутність чітких законодавчих норм, які б зобов'язували соціальні платформи здійснювати ефективний моніторинг контенту, що дозволяло б протидіяти діям, пов'язаним із порушенням у кіберпросторі. Відповідно, розробка стратегії кібербезпеки в соціальних мережах повинна містити інтеграцію положень норм кримінального права з метою протидії кіберзлочинам, оскільки взаємодія між правоохоронними органами та постачальниками інтернет-послуг може ефективно впливати на забезпечення кібербезпеки.

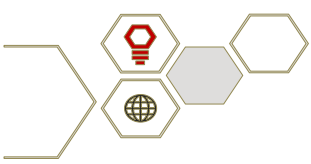
Аналіз останніх досліджень і публікацій. Дослідженням проблем використання соціальних мереж у протидії злочинності займалися вітчизняні та зарубіжні вчені. Зокрема, В. В. Шемчук [1] розкриває сутність кіберзлочинності, підходить до розуміння даного поняття, класифікує кіберзлочини та пропонує можливі способи протидії їм. В. Горлинський, Б. Горлинський [2] у своєму дослідженні розглядають кібербезпеку як невід'ємну складову національної безпеки та наголошують на важливості впровадження кримінальної відповідальності за вчинені злочини в цій сфері. Я. Й. Малик [3] акцентує на тому, що питання правового регулювання кібербезпеки в Україні є однією з ключових сфер, на яку держава має звертати посилену увагу, особливо щодо вразливих категорій населення. О. Бугера [4] вивчає проблеми використання соціальних мереж для запобігання злочинності шляхом здійснення моніторингу кримінологічно значущої інформації та її аналізу. К. А. Автухов [5] зазначає, що



підвищення якості кримінальних розслідувань потребує впровадження інноваційних технологій, зокрема введення інновацій у слідчу діяльність за такими напрямками, як розробка та використання нових науково-технічних засобів розкриття злочинів, збирання доказів та їх попереднє дослідження, а також забезпечення сучасними інформаційними технологіями та їх використання в роботі слідчих; створення (розробка) нових прийомів, методів і способів проведення певних слідчих дій та розслідування кримінальних справ загалом. О. В. Косолап [6] розглядає та аналізує інтеграцію кримінального права в стратегії розвитку кібербезпеки соціальних мереж і виокремлює проблеми, які існують на шляху цієї інтеграції. В. А. Мисливий [7] зазначає, що охорона кібернетичної безпеки в умовах глобалізації є важливою сферою, аналізує етапи її становлення та шляхи вдосконалення. Науковці В. Д. Кириченко і Р. В. Бараненко [8] вивчають реформування правової системи України під впливом євроінтеграційних процесів.

Загалом дослідження та публікації у цій сфері пов'язані з розв'язанням питань правового регулювання кібербезпеки в Україні, вивченням проблем кіберзлочинності, кримінально-правової протидії поширення кіберзлочинів, підвищення якості їх кримінальних розслідувань.

Виділення невирішених раніше частин загальної проблеми. З розвитком сучасних інформаційних технологій, удосконаленням і ускладненням технічних засобів передачі інформації правоохоронні органи стикаються з необхідністю використання ресурсів соціальних мереж для виявлення та розкриття злочинів. Перед правоохоронними органами постають нові виклики, які можуть бути подолані лише шляхом удосконалення способів і засобів отримання та використання інформації. Аналіз нормативно-правових актів, що регулюють боротьбу з кіберзлочинністю, виявляє їх недосконалість, що створює труднощі під час їх застосування. У цій статті запропоновано рекомендації щодо



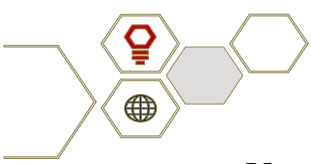
створення ефективних механізмів запобігання кіберзлочинності як на українському, так і міжнародному рівнях.

Формулювання цілей статті (постановка завдання). Мета статті – аналітичний огляд особливостей і механізмів впровадження кримінального права в стратегії розвитку кібербезпеки соціальних мереж в Україні.

Виклад основного матеріалу дослідження з повним обґрунтуванням здобутих наукових результатів. Зі зростанням популярності інтернету неухильно зростає його роль у повсякденному житті людини. Масштабне впровадження швидких і безкоштовних онлайн-сервісів формує основи комунікації значної частини суспільства, надаючи доступ до інформації, актуалізуючи економічні інтереси й політичну позицію громадян.

Інтернет-технології радикально змінили індустрію спілкування та медіа, спосіб споживання і створення новин. Онлайн-платформи, зокрема соціальні мережі, поступово стають домінантним джерелом новин та інформації для сотень людей. Простота створення й поширення новин через мережу «Інтернет», а також неможливість перевірити величезні обсяги інформації, що циркулює у всесвітній мережі, різко посилює поширення дезінформації та фейкових новин.

Сьогодні уряди багатьох країн усвідомлюють, що неконтрольоване використання соціальних мереж становить пряму загрозу національній безпеці та стабільності, і вживають дієвих заходів для забезпечення безпеки інформаційного простору у своїх країнах. Суспільна небезпека, яку становлять деструктивні дії з використанням соціальних мереж, вимагає організації ефективної протидії цим процесам і явищам. З цією метою створено комплексну національну систему кібербезпеки, яка дозволяє оперативно відстежувати зростання соціальної напруги, підбурювання до масових заворушень, протести в соціальних мережах і електоральні настрої проти основних політичних партій, діяльність екстремістських та терористичних угруповань, прояви комп'ютерної злочинності, злочини проти громадського порядку тощо, створено та впроваджено систему моніторингу.

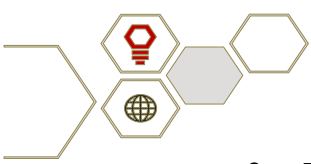


У кримінально-правовій та кримінологічній доктрині дискутуються різні погляди на поняття, види та класифікацію кіберзлочинів. Але, загалом, до таких злочинів відносять злочини, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж. До основних видів цих злочинів належать: створення та поширення шкідливих програмних чи технічних засобів (вірусів), втручання у роботу комп'ютерів, автоматизованих систем та комп'ютерних мереж, крадіжку інформації, поширення протиправної інформації через систему Інтернет, фішинг, фармінг тощо [9, с. 44].

На підставі аналізу наукового доробку з обраної проблематики вважаємо за можливе виокремити і такі види кіберзлочинів, що вчиняються в соціальних мережах:

1. Азартні ігри в соціальних мережах, що часто організовують з метою отримання незаконного доходу. Онлайн-азартні ігри можуть сприйматися як ігрові додатки або вебсайти, які пропонують користувачам можливість виграти гроші або інші цінності. Такі азартні ігри часто працюють без необхідних ліцензій і не завжди виплачують виграші. Як наслідок, користувачі втрачають великі суми грошей, а організатори отримують незаконні прибутки [10, с. 274]. Кримінальне законодавство багатьох країн передбачає покарання за організацію або участь в нелегальних азартних іграх.

2. Інтернет-шахрайство. Є одним із найпоширеніших злочинів, що вчиняються в соціальних мережах. Відомим на сьогодні є фішинг, коли шахраї надсилають фальшиві повідомлення або посилання, які мають вигляд офіційних, і викрадають особисту інформацію, таку як логіни, паролі та дані кредитних карток, шахрайство під виглядом продажу товарів або послуг, шахраї використовують соціальні мережі як платформу для продажу неіснуючих товарів або послуг. Вони створюють фейкові сторінки або акаунти, пропонуючи товари за привабливими цінами, і зникають після отримання оплати та фейковий благодійний збір коштів. Злочинці використовують соціальні мережі для збору коштів нібито на благодійні цілі, але насправді можуть використовувати їх для особистого збагачення [10, с. 275].



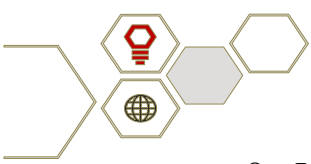
3. Торгівля наркотиками. Соціальні мережі та месенджери стають корисними інструментами для організації продажу та розповсюдження наркотиків. Продавці створюють закриті групи або сторінки та контактують із покупцями за допомогою особистих повідомлень. Така діяльність є особливо небезпечною, оскільки приваблює молодь та становить серйозну загрозу громадській безпеці [10, с. 275].

4. Продаж підроблених документів. У соціальних мережах часто рекламують послуги зі створення підроблених документів, таких як паспорти, водійські права та свідоцтва про освіту. Така діяльність не лише призводить до шахрайства, а й сприяє розвитку інших видів злочинної діяльності, таких як нелегальна імміграція та відмивання грошей [11].

5. Інвестиційне шахрайство та шахрайство з криптовалютами. У соціальних мережах часто можна побачити пропозиції щодо високоприбуткових інвестиційних проєктів і купівлі криптовалюти. Шахраї створюють фейкові інвестиційні платформи або штучно розкручують маловідомі криптовалюти, а згодом використовують техніку «накачування і скидання», коли вартість різко падає, а інвестори втрачають кошти.

6. Романтичні афери. Шахраї створюють фейкові профілі в соціальних мережах і на сайтах знайомств, щоби організувати довіру з потенційними жертвами. Як тільки довіра встановлена, вони придумують різноманітні вигадані історії (наприклад, про раптову хворобу або фінансові проблеми) і вимагають гроші. Ці дії спрямовані на емоційне маніпулювання жертвою та отримання фінансової вигоди [12].

7. Вимагання та примус. У соціальних мережах злочинці можуть вимагати гроші, погрожуючи розкрити особисту інформацію жертви. Наприклад, зламавши акаунт, вони мають змогу отримати доступ до особистих фотографій або повідомлень і вимагати гроші за нерозголошення цієї інформації. Це також стосується так званих «сексуальних пасток», коли жертву заманюють в небезпечні ситуації та шантажують. [12].



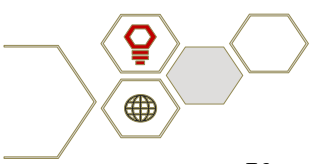
8. Крадіжка особистих даних з метою отримання фінансової вигоди. Злочинці використовують соціальні мережі для збирання особистої інформації (наприклад, імена, адреси, дні народження), яку потім використовують для доступу до банківських рахунків, створення фальшивих кредитних карток та проведення інших фінансових операцій [10, с. 275].

Аналіз нормативно-правових актів, що регулюють кібербезпеку соціальних мереж у контексті кримінального права, містить дослідження міжнародних, національних і спеціальних законів про захист даних, боротьбу з кіберзлочинністю та регулювання поведінки користувачів в інтернеті.

Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року є першим міжнародним документом, що встановлює основні принципи запобігання та боротьби з кіберзлочинністю, зокрема зі злочинами, які можуть бути вчинені через соціальні мережі. Конвенція встановлює норми для криміналізації таких дій, як несанкціонований доступ до інформаційних систем, втручання в роботу комп'ютерних мереж і поширення шкідливого програмного забезпечення [13].

Загальний регламент про захист даних (GDPR), що регулює обробку персональних даних в ЄС, зобов'язує компанії, і навіть соціальні медіаплатформи, забезпечувати захист даних користувачів. Порухення вимог щодо обробки даних може призвести до кримінальної або адміністративної відповідальності [14].

У Стратегії кібербезпеки України, затвердженій Указом Президента України Указом Президента України від 15 березня 2016 року №96/2016 [15], особливе значення приділено загрозам кібербезпеки та безпеці інформаційних ресурсів, серед яких названо уразливість соціальних мереж та інших цифрових платформ до кібератак. Крім того, Урядом України було прийнято низку законів і правок до інтеграції кримінального права до Стратегії кіберзахисту соціальних мереж. До них належать Кримінальний кодекс України, Закон «Про захист інформації» та Закон України «Про основні засади забезпечення кібербезпеки України».



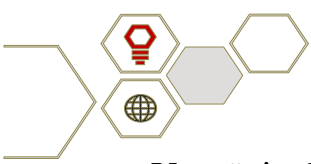
Кримінальний кодекс України (далі – КК) містить низку статей у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що передбачені Розділом XVI КК України і встановлюють відповідальність, зокрема, за кіберзлочини в соціальних мережах [16]:

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК). Ця стаття передбачає покарання за незаконне втручання, що призводить до порушення роботи системи, включно з блокуванням доступу та порушенням цілісності даних. Вона охоплює випадки, коли злочинці отримують доступ до соціальних мереж без дозволу, втручаються в роботу серверів або змінюють інформацію. Оскільки соціальні мережі є платформами, що містять величезну кількість персональних даних, захист цих даних від несанкціонованого доступу є пріоритетом у кібербезпеці. Передбачено кримінальне переслідування осіб, які отримали доступ до облікових записів користувачів соціальних мереж з метою розповсюдження неправдивої інформації або шантажу.

Проте в цій статті нечітко визначено термін «несанкціоноване втручання», що ускладнює правозастосування, призводить до неоднозначного трактування та створює можливості до зловживання з боку правоохоронних органів. Це також зумовлює ускладнення для розслідування та доведення вини й може спричинити ситуації, коли дії не завдають шкоди, але підпадають під цю статтю.

Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів (ст. 361-1 КК). Відповідальність настає, якщо особа створює або продає шкідливе програмне забезпечення, яке може бути використане для атак на користувачів соціальних мереж, викрадення даних або пошкодження інформаційних систем.

Проте положення цієї норми щодо обсягу суспільно-небезпечних дії може бути застосоване до широкого кола дій, що призводить до небезпеки неправомірного переслідування розробників програмного забезпечення, які не мають злого наміру. Це може негативно вплинути на розвиток ІТ-індустрії в



Україні. Не завжди зрозуміло, що конкретно є «шкідливим програмним забезпеченням», оскільки багато програм можуть бути використані як з позитивними, так і негативними намірами. Це може ускладнити правозастосування.

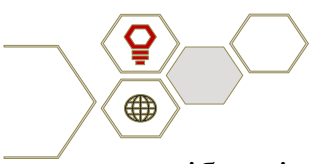
Шахрайські дії щодо інформації, яка обробляється в комп'ютерних мережах (ст. 362 КК). Встановлює покарання за несанкціонований доступ до інформації, її модифікацію, видалення або блокування. Це особливо актуально для соціальних мереж, де злочинці можуть отримувати доступ до персональних даних користувачів, змінювати їх і зловживати ними.

Проте в статті нечітко розрізняються різні форми інтернет-шахрайства, які можуть бути вчинені в комп'ютерних мережах. Це призводить до ситуацій, коли не всі випадки шахрайства можуть бути правомірно кваліфіковані.

В умовах сучасних загроз, таких як інформаційні війни, дезінформація через соціальні мережі, Стратегія національної безпеки України «Безпека людини – безпека країни», затверджена Указом Президента України від 14 вересня 2020 року [17] передбачає заходи проти поширення фейкових новин, маніпуляцій та дезінформації, зокрема під час виборів і збройних конфліктів. Українське кримінальне право передбачає низку норм, які можуть бути застосовані для боротьби з дезінформацією [16]:

Завідомо неправдиве повідомлення про загрозу безпеці громадян (ст. 259 КК) передбачає відповідальність за завідомо неправдиві повідомлення про загрозу безпеці людей, що може містити поширення фейкових новин, які викликають паніку або дестабілізують ситуацію; розслідування випадків поширення через соціальні мережі неправдивої інформації про загрози терактів або масштабні катастрофи, що призводило до паніки серед населення.

Публічні заклики до насильницької зміни чи повалення конституційного ладу (ст. 109 КК). Поширення дезінформації з метою підбурювання до повалення влади або насильницької зміни державного устрою також підпадає під кримінальну відповідальність. Передбачено притягнення до відповідальності



осіб, які через соціальні мережі поширювали фейкові новини та заклики до насильницького повалення влади, підриваючи державну безпеку.

Пропаганда війни (ст. 436 КК) – стосується поширення інформації, що містить заклики до війни або розпалювання національної, расової чи релігійної ворожнечі. У соціальних мережах часто поширюються фейкові новини, спрямовані на підбурювання конфліктів і ненависті. Передбачає відповідальність за поширення через соціальні мережі фейкових новин про етнічні конфлікти, що сприяли розпалюванню ворожнечі між різними групами населення.

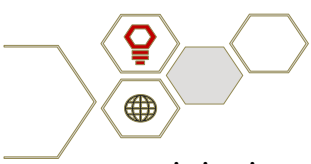
Захист дітей у соціальних мережах є одним із найважливіших аспектів кібербезпеки. В українському кримінальному законодавстві посилено відповідальність за злочини, пов'язані з кібербулінгом, сексуальною експлуатацією та переслідуванням дітей в інтернеті та інтегровані до Стратегії кібербезпеки України [16]:

Ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 300 КК) передбачає кримінальну відповідальність за розповсюдження порнографічних матеріалів, зокрема із зображенням дітей, серед них і через соціальні мережі; розслідування випадків поширення через соціальні мережі матеріалів, що містять дитячу порнографію, та притягнення винних до кримінальної відповідальності.

Крім того, Кримінальний кодекс України містить інші статті, пов'язані з кіберзлочинністю, зокрема відповідальність за незаконне збирання інформації, її поширення та використання з метою отримання матеріальної вигоди.

Закон України «Про захист інформації в інформаційно-комунікаційних системах» встановлює правові основи захисту інформації, яка обробляється в інформаційно-комунікаційних системах, зокрема в соціальних мережах. Основними положеннями закону є [18]:

1. Конфіденційність, цілісність та доступність даних. Закон зобов'язує забезпечувати конфіденційність (захист від несанкціонованого доступу),



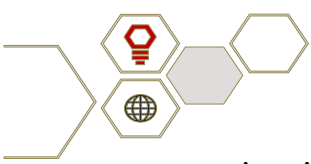
цілісність (захист від модифікації або видалення) та доступність (забезпечення доступу до даних уповноваженим користувачам).

2. **Обов'язки операторів і адміністраторів систем.** Власники інформаційних систем, зокрема адміністратори соціальних мереж, зобов'язані вживати заходів для захисту даних користувачів, і навіть вживати технічні та організаційні заходи задля зменшення ризику несанкціонованого доступу.

3. **Регулювання доступу.** Закон встановлює умови та порядок надання доступу до оброблюваної інформації, зокрема вимоги до аутентифікації користувачів і використання засобів криптографічного захисту інформації.

4. **Відповідальність за порушення.** Порушення законодавства про захист персональних даних, зокрема неправомірне використання даних користувачів соціальних мереж, тягне за собою адміністративну або кримінальну відповідальність.

Закон України «Основні засади забезпечення кібербезпеки України» [19] регулює питання кібербезпеки на національному рівні та визначає заходи для забезпечення кібербезпеки в усіх сферах, включно з соціальними мережами. Закон встановлює основні засади державної політики у сфері кібербезпеки, а також запобігання, виявлення та реагування на кіберзагрози та мінімізацію їх наслідків. Основними суб'єктами, відповідальними за забезпечення кібербезпеки, є адміністративні органи, правоохоронні органи та оператори критичної інфраструктури. Керівники соціальних мереж також повинні співпрацювати з цими суб'єктами для виявлення та запобігання кіберзагрозам. Закон встановлює процедури реагування на кіберінциденти та кібератаки, які можуть вплинути на соціальні мережі. Зокрема, він передбачає створення спеціальної команди реагування на інциденти (CERT) для виявлення, аналізування та ліквідації наслідків кіберінцидентів. Закон наголошує на необхідності підвищення обізнаності користувачів соціальних мереж щодо кіберзагроз, зокрема через проведення інформаційних кампаній, навчання та підготовки фахівців з кібербезпеки. Закон також передбачає участь України в міжнародних ініціативах і співпрацю з іншими країнами та міжнародними



організаціями з метою покращення кібербезпеки, що є важливим у боротьбі з транскордонною кіберзлочинністю в соціальних мережах.

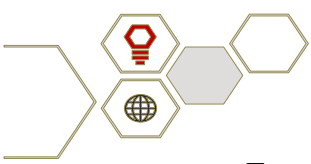
Проте, незважаючи на розроблені та прийняті закони, можна виокремити низку проблем:

Діяльність із протидії кіберзлочинам засобами кримінально-правового впливу ґрунтується на їх криміналізації. Хоча поняття «кіберзлочинність», «кіберзлочини» використовується як у міжнародному, так і в національному законодавстві, Кримінальний кодекс не містить визначення поняття кіберзлочину [9, с. 44].

Законодавство часто не встигає за розвитком нових технологій і тактик кіберзлочинності, що ускладнює розслідування злочинів у соціальних мережах. Технології розвиваються швидше, ніж спроможність законодавців. Наприклад, постійно з'являються нові соціальні медіаплатформи та додатки, кожна з яких може мати певні особливості безпеки та функціонування. Злочинці можуть використовувати ці нові технології для обману користувачів, вчиняючи шахрайство або поширюючи шкідливий контент. Наприклад, технології блокчейн і криптовалюти створюють нові способи вчинення фінансових злочинів, які не обов'язково охоплені чинним законодавством.

Криптовалюти використовуються для фінансування тероризму на окупованих територіях України через кілька ключових механізмів. Ці методи дозволяють уникати традиційних фінансових систем, забезпечуючи анонімність та безпеку фінансових потоків для терористичних організацій.

На окупованих територіях України терористичні організації, підтримувані росією, використовують криптовалютні платформи для збору коштів через онлайн-компанії. Ці компанії часто розміщуються на платформах соціальних медіа, криптовалютних форумах і в темних вебсайтах. Групи, такі як «ДНР» (Донецька Народна Республіка) і «ЛНР» (Луганська Народна Республіка), створюють закриті групи у Telegram, VK та на інших платформах, де публікують адреси криптовалютних гаманців і закликають своїх прихильників та симпатиків надавати фінансову підтримку [20].



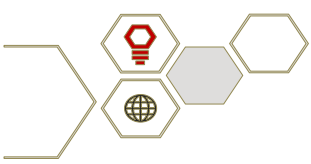
Багато злочинів у соціальних мережах є транскордонними, що ускладнює співпрацю з правоохоронними органами інших країн. Закони, що регулюють кіберзлочинність, відрізняються в різних країнах. Це ускладнює правоохоронну діяльність, оскільки злочини, скоєні в одній країні, можуть не підпадати під юрисдикцію правоохоронних органів іншої країни. Наприклад, якщо злочинець перебуває в одній країні, а жертва – в іншій, стає складно зібрати докази й притягнути до відповідальності.

Важливо створити міжнародні механізми, які сприятимуть швидкому обміну інформацією та спільному розслідуванню кіберзлочинів. Розробити та впровадити платформи обміну інформацією між правоохоронними органами для швидкого обміну даними про кіберзлочини, що відбуваються. Наприклад, Наприклад, У 2010 році Europol спільно з Європейською комісією та державами-членами ЄС створили Робочу групу Європейського Союзу з кіберзлочинності (EUCTF), роль якої полягає у визначенні, обговоренні та визначенні пріоритетів ключових проблем і дій у боротьбі з кіберзлочинністю [10].

Необхідно вдосконалити законодавство для забезпечення ефективнішого захисту персональних даних користувачів соціальних мереж. Україна повинна прийняти законодавство, що відповідало б стандартам GDPR (General Data Protection Regulation), яке встановлює суворіші вимоги до захисту даних і забезпечує відповідальність платформ за витоки даних [14].

Злочини, скоєні в інтернеті, зокрема в соціальних мережах, часто важко розслідувати через анонімність правопорушників і використання методів шифрування. Це ускладнює збирання доказів і доведення вини злочинця в суді. Наприклад, якщо злочинець використовує VPN або проксі-сервери для маскування своєї IP-адреси, правоохоронним органам важко встановити його реальне місцеперебування. Це призводить до затримок у розслідуванні та, у деяких випадках, до відсутності доказів, що ускладнює подальші судові процеси.

Підсумовуючи, зазначимо, що українське законодавство передбачає низку норм, спрямованих на забезпечення кібербезпеки та протидії кіберзлочинності в соціальних мережах. Однак ефективні заходи протидії кіберзагрозам потребують



подальшого вдосконалення нормативно-правової бази, міжнародного співробітництва та розробки механізмів реагування на кіберінциденти.

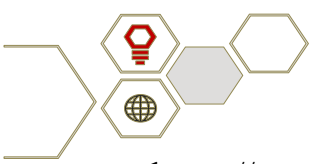
Висновки. З розвитком інформаційних технологій та поширенням соціальних мереж проблема кіберзлочинності в Україні набуває все більшої актуальності. Вчинення злочинів у кіберпросторі, особливо в соціальних мережах, становить серйозну загрозу як для користувачів, так і для безпеки держави. Аналіз нормативно-правових актів, що регулюють протидію кіберзлочинності, виявляє серйозні недоліки, такі як неточна термінологія, відсутність чітких стандартів відповідальності та складнощі зі збиранням доказів. Це свідчить про нагальну потребу в удосконаленні правової бази.

Багато кіберзлочинів, що вчиняються в соціальних мережах мають транснаціональний характер і вимагають активної міжнародної співпраці національних правоохоронних органів. Створення ефективних механізмів обміну інформацією та проведення спільних розслідувань має вирішальне значення для успішної боротьби з кіберзлочинністю. Україні необхідно впроваджувати нові технології та інноваційні підходи до кримінальних розслідувань, такі як створення спеціалізованих груп реагування на кіберінциденти (CERT) та підвищення кваліфікації експертів із кібербезпеки.

Необхідно вжити комплексних заходів для забезпечення ефективної боротьби з кіберзлочинністю в Україні, включно із законодавством, зміцненням міжнародної співспівпраці, розробкою механізмів реагування на кіберінциденти та підвищенням обізнаності громадськості про ризики, пов'язані з використанням соціальних мереж.

Список використаних джерел

1. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. 2018. Т. 29 (68). № 6. С. 119–124. URL:



https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf

(дата

звернення: 03.08.2024).

2. Горлинський В., Горлинський Б. Кібербезпека як складова інформаційної безпеки. *Information Technology and Security*. Вип. 1. С. 12–21. DOI: 10.20535/2411-1031.2019.7.2.190559

3. Малик Я. Й. Інформаційна війна і Україна. *Демократичне врядування*. 2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3. (дата звернення: 04.08.2024).

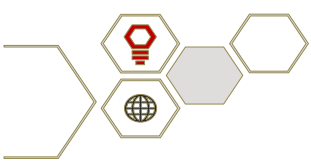
4. Бугера О. Використання соціальних інтернет-мереж для запобігання злочинності. *Підприємництво, господарство і право*. 2018. № 5. С. 238–241. URL: <http://pgp-journal.kiev.ua/archive/2018/5/47.pdf> (дата звернення: 04.08.2024).

5. Автухов К. А. Кримінологічний погляд на соціальні мережі. *Актуальні питання публічного та приватного права*. 2020. Вип. 1. С. 150–153. URL: https://dspace.nlu.edu.ua/bitstream/123456789/1856/1/Avtyxov_150-153.pdf (дата звернення: 03.08.2024).

6. Косолап О. В. Соціальні мережі як об'єкт криміналістичного дослідження. *Вісник кримінального судочинства*. 2016. Вип. 1. С. 126–134. URL: https://vkslaw.knu.ua/images/verstka/1_2016_Kosolap.pdf (дата звернення: 02.08.2024).

7. Мисливий В. А. Кримінально-правова охорона кібернетичної безпеки в умовах глобалізації. *Кримінально-правове забезпечення сталого розвитку України в умовах глобалізації*: матеріали міжнар. наук.-практ. конф., (м. Харків, 12–13 жовт. 2017 р.). Харків, 2017. С. 122–126. URL: <https://elar.naiau.kiev.ua/server/api/core/bitstreams/966ab3ff-05f2-43de-82c6-58a56d78a403/content> (дата звернення: 04.08.2024).

8. Кириченко В. Д., Бараненко Р. В. Характеристика кіберзлочинності. *Реформування правової системи України під впливом євроінтеграційних*



процесів : матеріали III Всеукраїнської науково-практичної конференції. Херсон, 2018. С. 189–191.

9. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора, О.М. Литвака* (м. Харків, 23 квіт. 2020 р.). Харків : ХНУВС, 2020. С. 44–45

10. Горбачова І. М. Кримінальні правопорушення, що вчиняються в інформаційній мережі. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/60324756-f941-4d47-a892-70245ba613f8/content> (дата звернення: 04.08.2024).

11. Cybercrime. *Europol*: вебсайт. URL: <https://www.europol.europa.eu/crime-areas/cybercrime> (date of access: 04.08.2024).

12. Барановська Т. В. Запобігання та протидія кримінальним правопорушенням проти економічної системи: дис...докт. юр. наук: 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Житомир, 2023. URL: https://dduvs.edu.ua/wp-content/uploads/files/Structure/science/rada/new_d0872702/2023/4/4/d4.pdf (дата звернення: 04.08.2024).

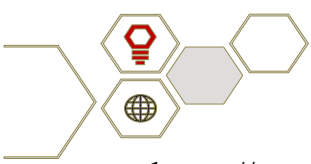
13. Конвенція про кіберзлочинність від 23.11.2001. URL: <https://ips.ligazakon.net/document/MU01209> (дата звернення: 03.10.2024).

14. Загальний регламент про захист даних (GDPR). URL: <https://gdpr-text.com/uk/> (дата звернення: 03.08.2024).

15. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року №96/2016. URL: <https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT> (дата звернення: 04.10.2024).

16. Кримінальний кодекс України від 5 квітня 2001 року. URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 03.08.2024).

17. Стратегія національної безпеки України «Безпека людини – безпека країни», затверджена Указом Президента України від 14 вересня 2020 року. URL:



<https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 04.08.2024).

18. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 03.08.2024).

19. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 03.08.2024).

20. Величко Л., Попов В., Гулька І., Некшуцу М. Як криптовалюти використовуються для фінансування тероризму на окупованих територіях України та Молдови (розслідування). *Text.org.ua: вебсайт*. 2021. URL: <https://texty.org.ua/articles/102844/yak-kryptovalyuty-vykorystovuyutsya-dlya-finansuvannya-teroryzmu-na-okupovanyh-terytoriyah-ukrayiny-ta-moldovy-rozsliduvannya/> (дата звернення: 03.08.2024).