ФП 2023-4
ISSN 1995-6134

УДК 343.9:343.98
DOI: http://doi.org/10.5281/zenodo.10512327

І.В. ЗОЗУЛЯ,
професор кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор, м. Харків, Україна; e-mail: journals@meta.ua;
ORCID: https://orcid.org/0000-0002-3507-0012

О.І. ЗОЗУЛЯ,
доцент кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, доцент, м. Харків, Україна; e-mail: oizozulia@gmail.com;
ORCID: https://orcid.org/0000-0002-5428-4622

ШАХРАЙСТВО ЧЕРЕЗ ЕЛЕКТРОННІ КОМУНІКАЦІЇ: ЗАУВАЖЕННЯ ДО ЗАКОНОПРОЄКТУ

I.V. ZOZULIA,
Professor, Chair of Criminalistics, Forensic Expertise and Pre-Medical Training, Kharkiv National University of Internal Affairs, Doctor of Law, Professor, Kharkiv, Ukraine; e-mail: journals@meta.ua;
ORCID: http://orcid.org/0000-0002-3507-0012

O.I. ZOZULIA,
Associate Professor, Chair of Criminal Law and Criminology, Kharkiv National University of Internal Affairs, Doctor of Law, Ass. Professor, Kharkiv, Ukraine; e-mail: oizozulia@gmail.com;
ORCID: https://orcid.org/0000-0002-5428-4622

FRAUD VIA ELECTRONIC COMMUNICATIONS: COMMENTS TO THE BILL

АНОТАЦІЇ (ABSTRACTS), КЛЮЧОВІ СЛОВА (KEYWORDS)

Постановка проблеми. У період активного розвитку цифрових технологій та зростаючої залежності суспільства від електронних комунікацій, питання кібербезпеки та злочинів, пов'язаних із цими технологіями, стають надзвичайно актуальними. І саме кібершахрайство є одним із різновидів кіберзлочинів, що включає в себе використання інформаційних технологій та мереж для вчинення злочинів. Це актуалізувало потребу змін у правовому підході щодо незаконних втручань у роботу інформаційних систем та мереж і необхідність удосконалення нормативно-правового регулювання у сфері кібербезпеки, й особливо – врахування сучасних технологічних і правових викликів, а також покращення можливостей правоохоронних органів у реагуванні на кіберзлочини. **Метою** статті є оцінка відповідності законопроєкту "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство" за реєстр. № 10190 від 25.10.2023 р. контексту змісту електронних комунікацій та врахування вимог і викликів сучасного інформаційного суспільства. Використані такі **методи:** правового аналізу з вивчення, розгляду та оцінки чинного законодавства, що регулює шахрайство через електронні комунікації, та його конкретних положень і нормативних актів для з'ясування їх змісту, логіки й ефективності; метод юридичного критичного аналізу для виокремлення непослідовностей, виявлення можливих негативних наслідків введення нових правових норм щодо електронних комунікацій в галузі шахрайства, а також розгляду пропозицій щодо удосконалення законодавства. **Результати.** Встановлено, що з урахуванням широкого поширення сучасних електронних технологій, в останній час особливого значення набула проблема визначення особливостей електронних комунікацій як складової електронно-комунікаційного шахрайства в контексті сучасних тенденцій та розвитку інформаційного суспільства, в тому числі, й щодо використання в правовому полі. Змістом вітчизняного законодавства у контексті електронних комунікацій стало правове осучаснення змісту технологічних новацій, пов'язаних із комунікаційними та інформаційними системами та протидією електронно-комунікаційному шахрайству. Деякими недоліками законопроєкту визначені термінологічна неоднозначність тлумачення визначення "електронно-комунікаційне шахрайство"; можливість існування у кібершахрайстві інших аспектів, не врахованих із заволодінням майном чи отриманням права на майно; можливість становлення неадекватними для нових методів атак чи шахрайства вже сформульованих термінів при швидкому розвитку технологій електронних комунікацій; занадто широкий обсяг визначення із різних аспектів створення, керівни-

ISSN 1995-6134

цтва, участі у шахрайських організаціях та їх спільнотах. **Висновки.** Показано, що законопроєкт був викликаний лише ілюзорною можливістю надмірної адаптації сучасного розуміння електронних комунікацій до використовуваних протягом багатьох років норм Кримінального кодексу України стосовно шахрайства, не вдаючись до необґрунтованого змішування понять і категорій. Вирішення проблеми кібершахрайства вимагає більш обережного та обґрунтованого підходу до правового регулювання, де враховувалися би як сучасні виклики, так і вже існуючі стандарти та норми.

Ключові слова: *шахрайство; електронні комунікації; законодавство з кібербезпеки; законопроєкт*

***

Problem statement. In the era of active development of digital technologies and increasing society's reliance on electronic communications, issues of cybersecurity and crimes related to these technologies become extremely relevant. Cybercrime, in particular, is one type of cybercrime that involves the use of information technologies and networks to commit offenses. This has highlighted the need for changes in the legal approach to illegal interventions in the operation of information systems and networks, as well as the necessity to enhance regulatory frameworks in the field of cybersecurity, particularly taking into account modern technological and legal challenges, and improving law enforcement capabilities in responding to cybercrimes. The **purpose** of the article is to assess the effectiveness and compliance of the bill law "On Amendments to the Criminal Code of Ukraine on Establishing Liability for Electronic Communications Fraud" under registration number 10190 dated October 25, 2023, with the requirements and challenges of the modern information society. The following **methods** have been employed: legal analysis involving the study, examination, and evaluation of the current legislation regulating fraud via electronic communications, as well as its specific provisions and regulatory acts to clarify their content, logic, and effectiveness; legal critical analysis method to identify inconsistencies, potential negative consequences of introducing new legal norms related to electronic communications in the field of fraud, and consideration of proposals for improving legislation. The **results.** Established that considering the widespread use of modern electronic technologies, the issue of defining the specifics of electronic communications as a component of electronic communications fraud in the context of current trends and the development of information society has become particularly relevant. In the content of domestic legislation in the context of electronic communications, there has been a legal modernization of the content of technological innovations related to communication and information systems and countering electronic communications fraud. Some drawbacks of the bill law include terminological ambiguity in interpreting the definition of "electronic communications fraud"; the possibility of the existence of other aspects in cyber fraud not considered involving property acquisition or obtaining rights to property; the possibility of becoming inadequate for new methods of attacks or fraud already formulated terms with the rapid development of electronic communications technologies; a too broad scope of definition from various aspects of creating, leading, participating in fraudulent organizations and their communities. **Conclusions.** The bill was prompted only by the illusory possibility of excessively adapting the modern understanding of electronic communications to the norms of the Criminal Code of Ukraine regarding fraud used for many years, without resorting to the unjustified mixing of concepts and categories. Solving the problem of cyber fraud requires a more cautious and reasoned approach to legal regulation, taking into account both modern challenges and existing standards and norms.

Keywords: *fraud; electronic communications; cybersecurity legislation; bill*

Постановка проблеми

В часи активного цифрового розвитку та зростаючої залежності суспільства від електронних комунікаційних технологій, питання кібербезпеки та шахрайства через ці засоби стають актуальнішими, ніж будь-коли. Віртуальний простір став полем діяльності й для незаконних дій шахраїв та зловмисників. З цього приводу І.О. Коновалова зазначає, що "світ змінився, став віртуальним, а поряд із цими процесами трансформується шахрайство, набуваючи нових форм" [1, с.111]; Т.А. Діброва, Д.О. Пісенко, Н.В. Сметаніна – що "кібершахрайство є цілком новим явищем, оскільки безпосередньо воно пов'язане з розвитком новітніх інформаційних технологій" [2, с.546]. На думку А.М. Бабенко та М.В. Палій, необхідним є "провадження ефективної державної політики у сфері протидії та запобігання корисливої злочинності в цілому, та крадіжкам і шахрайствам як найбільш поширеним формам протиправних посягань у сфері власності" [3, с.567].

При цьому, зі зростанням кількості електронних комунікаційних злочинів, ініціативи щодо удосконалення законодавства також набувають обертів.

Вже згадані Т.А. Діброва, Д.О. Пісенко, Н.В. Сметаніна зазначають, що "було внесено зміни до відповідних законів: "Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" з питання підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам" № 2137-IX від 15 березня 2022 року та "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєн-

ISSN 1995-6134

ного стану" № 2149-IX від 24 березня 2022 року" [2, с.547].

Зокрема, у Закон України "Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам" від 15.03.2022 р. № 2137-IX [4] були внесені деякі термінологічні зміни із заміни, наприклад, слів "(у тому числі електронні)" словами "(у тому числі комп'ютерні дані)" та слова "телекомунікаційних системах, інформаційно-телекомунікаційних системах" – словами "електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах" у ст.99; слова "носії комп'ютерної інформації" – словами "носії комп'ютерних даних" у ст.105; слова "електронних інформаційних системах або їх частинах" – словами "електронних інформаційних системах, комп'ютерних системах або їх частинах" у ст.159; слова "телекомунікаційну мережу, кінцеве обладнання" замінити словами "електронну комунікаційну мережу, кінцеве (термінальне) обладнання" у ст.248; слова "транспортні телекомунікаційні мережі" замінити словами "електронні комунікаційні мережі" у ст.265 тощо.

Так, наприклад, термін "комп'ютерні дані" може включати не лише інформацію, що фізично зберігається на носіях, але й дані, які обробляються та передаються електронними засобами, підкреслюючи, що це не просто фізичний носій, а інформація, яка має значення в контексті комп'ютерної обробки. Використання цього терміну дозволяє уникнути асоціації з конкретними фізичними носіями (наприклад, дисками чи флешкартами) і акцентує на важливості самої інформації, незалежно від того, яким чином вона зберігається чи передається.

Такі зміни були викликані *тогочасною потребою осучаснення термінології* та більш точного або широкого визначення технологічних аспектів, пов'язаних із комунікаційними та інформаційними системами. Зокрема, щодо відображення ширшого спектра технологій, які включають не лише традиційні телекомунікації, але й інші форми електронного зв'язку та обміну інформацією; підкреслення важливості обробки та обміну інформацією, що може включати не тільки голосові та текстові комунікації, але й обробку даних; врахування зростаючої ролі комп'ютерів у телекомунікаціях та обміну інформацією, а також підкреслення їхньої ключової участі у сучасних технологічних процесах.

Відповідно, Законом України "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану" від 24.03.2022 р. № 2149-IX [5] була введена нова редакція ст.361 "Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж" Кримінального кодексу України [6]. Це свідчило про актуалізацію потреби змін у правовому підході щодо незаконних втручань у роботу інформаційних систем та мереж і необхідність удосконалення нормативно-правового регулювання у сфері кібербезпеки, й особливо – врахування сучасних технологічних і правових викликів, а також покращення можливостей правоохоронних органів у реагуванні на кіберзлочини.

І саме кібершахрайство є одним із різновидів кіберзлочинів, що включає в себе використання інформаційних технологій та мереж для вчинення злочинів. Небезпека кібершахрайства полягає у величезному спектрі загроз, які можуть вплинути на індивідів, компанії, урядові установи та суспільство в цілому. При цьому, деякі основні аспекти небезпеки кібершахрайства включають втрату особистої інформації, фінансові втрати, крадіжку корпоративної інтелектуальної власності, порушення конфіденційності та репутації, атаки на критичну інфраструктуру, загрозу національній безпеці. Тому *метою* статті є оцінка відповідності законопроєкту "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство" за реєстр. № 10190 від 25.10.2023 р. контексту змісту електронних комунікацій та врахування вимог і викликів сучасного інформаційного суспільства. Її *новизна* полягає в розгляді особливостей електронних комунікацій як складової електронно-комунікаційного шахрайства з урахуванням сучасних тенденцій та розвитку інформаційного суспільства. *Завданнями* роботи є визначення електронних комунікацій як сфери законопроєктного регулювання шахрайства; оцінка аргументації Пояснювальної записки законопроєкту щодо шахрайства через електронні комунікації; інтерпретація електронних комунікацій у законопроєкті в контексті шахрайства.

ISSN 1995-6134

Електронні комунікації як сфера законопроєктного регулювання шахрайства

Слід зазначити, що недавній законопроєкт "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство" за реєстр. № 10190 від 25.10.2023 р. [7] сьогодні вже стає об'єктом уваги та обговорення, в тому числі, й стосовно актуальності, логічності та доцільності деяких його положень.

В обґрунтуванні необхідності прийняття проєкту Закону України "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство" у Пояснювальній записці до нього [8] йдеться про "існування безлічі видів шахрайських схем"… "з використанням інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж", а також з позначкою, на думку авторів законопроєкту, що "діюча ст.190 "Шахрайство" Кримінального кодексу України (далі – КК України) не відповідає сучасним реаліям нормативно-правового регулювання, не дає можливості для ефективної реалізації функції превенції та містить застарілі поняття, наприклад, "електронно-обчислювальна техніка", що частково унеможливлює її доказування правоохоронними органами". Тому, *на впевненість законодавця, акцент щодо шахрайства має переноситись у сферу електронних комунікацій.*

Разом із тим, стаття 190 "Шахрайство" чинного Кримінального кодексу України вже містить базове *поняття шахрайства як "заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою"*, до того ж, стосовно "вчиненого повторно, або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому" (ч.2), "вчиненого в умовах воєнного чи надзвичайного стану, що завдало значної шкоди потерпілому" (ч.3), *"вчиненого у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки" (ч.4),* "вчиненого в особливо великих розмірах або організованою групою" (ч.5) [6].

При цьому, шахрайство – це вид махінацій чи обману, при якому особа намагається обманути іншу особу з метою здобуття фінансової вигоди або іншої користі. *Шахрайство може приймати багато форм,* включаючи інтернет-й фінансове шахрайство, лотерейні, шлюбні, телефонні та лікарські шахрайства, шахрайства з нерухомістю тощо. Тобто, *шахрайство в цілому відноситься до родового поняття, а його різновиди – до видового.* І серед вказаних видів шахрайства до таких, що за природою мають *безпосереднє відношення до електронних комунікаційних, є інтернет- та телефонне шахрайство.* При цьому, електронні комунікації можуть бути задіяні в якості "резервного елемента" інших шахрайських схем для регулювання нестандартних ситуацій або виняткових обставин.

Як відомо, *електронні комунікації* – це передача та обмін інформацією, даними, повідомленнями або спілкування між людьми, комп'ютерами, пристроями чи системами за допомогою електронних засобів і засобів зв'язку. Вони включають в себе такі засоби комунікації, як електронна пошта, миттєві повідомлення, соціальні мережі, телефонію через Інтернет (VoIP), відеоконференції, текстовий чат, мобільний зв'язок та інші форми обміну інформацією, які базуються на електронних пристроях та мережах.

Або, більш строго, за п.28 ч.1 ст.2 Закону України "Про електронні комунікації" від 16.12.2020 р. № 1089-IX [9], *"електронна комунікація (телекомунікація, електрозв'язок)* – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій". Тобто, під *електронною комунікацією (телекомунікацією, електрозв'язком) слід розуміти процес передавання та/або приймання інформації у вигляді електромагнітних сигналів.* При цьому, щодо синонімічності певних термінів, *телекомунікація* – це передача і обмін інформацією (звуковою, візуальною, текстовою, даними) за допомогою електронних, оптичних чи радіотехнічних систем. Вона включає в себе передачу сигналів, голосу, даних, зображень і відео між пристроями або мережами за великими відстанями. Або, за ст.1 сьогодні нечинного Закону України "Про телекомунікації" від 18.11.2003 р. № 1280-IV, *"телекомунікації (електрозв'язок)* – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах". В свою чергу, *"електрозв'язок"* може вказувати на передачу сигналів, даних або інформації за допомогою електронних засобів, таких як комп'ютери, телефони, електронні пристрої тощо. А також включати в себе використання електронних комунікаційних технологій та мереж для передачі інформації на відстань.

ISSN 1995-6134

При цьому за розділом XIX Закону [9] сьогодні можна побачити загальну *тенденцію термінологічного переходу* законодавця від вживання терміну "телекомунікації" *до терміну "електронні комунікації".*

Оцінка аргументації Пояснювальної записки законопроєкту щодо шахрайства через електронні комунікації

Основна теза Пояснювальної записки до законопроєкту "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство" про *"не відповідність чинної ст.190 сучасним реаліям нормативно-правового регулювання"* [8, с.2] насправді виглядає *занадто штучною стосовно унікальності та винятковості цифрової трансформації* в переліку аспектів і тенденцій, які відбивають зміни в суспільстві, технологіях та природному середовищі. *До сучасних реалій нормативно-правового регулювання також входять* не менш важливі кліматичні зміни, біотехнології та генетична інженерія, права людини та соціальна справедливість, міжнародна співпраця, зміни в трудових відносинах, здоров'я та медицина тощо. Ці тенденції впливають на створення нових норм і правил, а також на перегляд і модернізацію існуючого нормативного середовища з метою відповіді на сучасні виклики та потреби суспільства.

Щодо аналогічної тези Пояснювальної записки до проєкту Закону про відсутність "можливості для ефективної реалізації функції превенції" [8, с.2], то *ефективна реалізація функції превенції стосовно шахрайства можлива навіть без введення окремого поняття "електронно-комунікаційне шахрайство".* Основною ідеєю превенції є запобігання вчиненню правопорушень шляхом впливу на можливих злочинців, потенційних жертв, і на суспільство загалом. Вона включає свідомість і освіту, законодавство, захист та безпеку, співпрацю, споживацькі практики тощо і становить важливий аспект забезпечення правопорядку та зменшення кількості правопорушень.

Щодо наступної тези Пояснювальної записки про *"застарілість поняття "електронно-обчислювальна техніка",* що частково унеможливлює її доказування правоохоронними органами" [8, с.2], то це пряме посилання на ч.4 "Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки" ст.190 Кримінального кодексу України. Разом із тим, *у сучасних реаліях термін "електронно-обчислювальна техніка" дуже умовно може вважатися застарілим* або менш уживаним у порівнянні з більш загальними синонімічними термінами "комп'ютери" чи "обчислювальна техніка". Так, О.О. Книженко взагалі їх розглядає виключно як технічні синоніми, враховуючи, що "в ККУкраїни не розкривається, що саме охоплюється поняттям "електронно-обчислювальна техніка" [10, с.91]. До того ж, А.А. Васильєв і Д.В. Пашнєв зазначають, що "якщо б законодавець вважав би за необхідне обмежити незаконні операції з використанням ЕОТ у ч.3 *(сьогодні частина 4. – Авт.)* ст.190 КК тільки діяннями Розділу XVI КК, то доцільно було б використати термінологію вказаного розділу. Очевидно, що термін "електронно-обчислювальна техніка" нерівнозначний терміну "електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку. Логічним є висновок, що до вказаних незаконних операцій повинні відноситися будь-які дії з використанням будь-якої ЕОТ" [11, с.139].

Тобто, *поняття "електронно-обчислювальна техніка" є більш широким і загальним, ніж "електронно-обчислювальні машини",* воно охоплює всі електронні засоби, призначені для обчислень і обробки інформації, включаючи комп'ютери, смартфони, планшети, сервери, та інші пристрої. "Електронно-обчислювальні машини" – це підкатегорія "електронно-обчислювальної техніки" і вказує на конкретні машини, які призначені для цих завдань. "Електронно-обчислювальна техніка" використовується для створення, обробки та збереження інформації, включаючи інструменти, які використовуються у вже згаданих "електронних комунікаціях" для обміну цією інформацією через мережі та засоби зв'язку. Електронні комунікації використовують "електронно-обчислювальну техніку" для передачі та прийому даних.

Щодо сумнівів законодавця за ще однією тезою Пояснювальної записки *стосовно "здатності доказування правоохоронними органами "електронно-обчислювальної техніки"* [8, с.2], то правоохоронні органи зазвичай використовують сучасні методи і технології для збору електронних доказів, і вживання більш сучасних термінів у нормативно-правових документах не впливає на їх здатність здійснювати дослідження та доказування відповідних злочинів.

І, нарешті, в останній тезі Пояснювальної записки йдеться, що "Законом України "Про електронні комунікації" визначені такі поняття, як

ISSN 1995-6134

"електронна комунікація", "технічні засоби електронних комунікацій", які повністю охоплюють необхідну кваліфікацію електронно-комунікаційного шахрайства, що вирішує питання притягнення до відповідальності при вчиненні трансграничних злочинів, встановлюючи при цьому формальний склад злочину. Отже, для того, щоб злочин вважався закінченим, достатньо лише вчинення зловмисником будь-якої дії, зазначеної в диспозиції нової статті 190[1] КК України" [8, с.2].

Разом із тим, "Закон України "Про електронні комунікації" від 16.12.2020 р. № 1089-IX [9] може не враховувати або відставати від новітніх технологій електронних комунікацій[1], що робить його менш ефективним у протидії найбільш сучасним видам кіберзлочинності, та містити неоднозначності, що ускладнюють його правильну інтерпретацію й використання в судовій практиці. Крім того, дуже обмежено можна вважати, що визначені у Законі України "Про електронні комунікації" поняття "електронна комунікація", "технічні засоби електронних комунікацій" повністю охоплюють необхідну кваліфікацію електронно-комунікаційного шахрайства, що вирішує питання притягнення до відповідальності при вчиненні трансграничних злочинів, встановлюючи при цьому формальний склад злочину. Це обумовлено потребами достатньо точних і широких визначень "електронна комунікація" та "технічні засоби електронних комунікацій" у Законі, щоб охоплювати різні аспекти електронно-комунікаційного шахрайства; адаптованості Закону до розвитку технологій, оскільки електронно-комунікаційне шахрайство може використовувати нові методи та інструменти; достатньої кваліфікації Законом різних видів електронно-комунікаційного шахрайства, а також визначення формального складу злочинів.

А безпосередньо визначення понять "електронна комунікація" та "технічні засоби електронних комунікацій" в Законі України [9] можуть надавати тільки основний каркас для кваліфікації електронно-комунікаційного шахрайства з визначенням, які види обману чи втручання вважаються шахрайством у контексті електронних комунікацій; якою повинна бути мета дій для визнання їх шахрайством; які саме технічні засоби можуть використовуватися для вчинення шахрайства, і чи адекватно вони описані в Законі.

До речі, у самому Законі України "Про електронні комунікації" від 16.12.2020 р. № 1089-IX [9] *про шахрайство йдеться тільки один раз* у ч.2 ст.80, що "постачальники електронних комунікацій повинні блокувати доступ до номерів або послуг при виявленні несанкціонованого втручання в мережі чи *шахрайства"*.

Інтерпретація електронних комунікацій у законопроєкті в контексті шахрайства

Не набагато більше порозумінь щодо шахрайства через електронні комунікації вніс і сам проєкт Закону із доповнення Кримінального кодексу України новою статтею 190[1] "Електронно-комунікаційне шахрайство": "1. Електронно-комунікаційне шахрайство, тобто протиправне збирання, зберігання, обробка та використання персональних даних, інформації, яка містить банківську таємницю, у тому числі індивідуальну облікову інформацію, реквізити платіжного інструменту, платіжної картки, код авторизації, з метою заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою з використанням електронної комунікації та/або технічних засобів електронних комунікацій… 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб… 3. Дії, передбачені частинами першою або другою цієї статті вчинені в умовах воєнного або надзвичайного стану або якщо вони вчинені організованою групою…".

А також статтею 255[4] "Створення, керівництво електронно-комунікаційною шахрайською організацією, а також участь у ній": 1. Створення електронно-комунікаційної шахрайської організації, керівництво такою організацією або її структурними частинами… 2. Надання послуг, участь у електронно-комунікаційній шахрайській організації… 3. Дії, передбачені частинами першою, другою або третьої цієї статті, вчинені в умовах воєнного або надзвичайного стану або якщо вони вчинені організованою групою… 4. Створення спільноти електронно-комунікаційних шахрайських організацій, тобто об'єднання двох чи більше електронно-комунікаційних шахрайських організацій, керівництво такою спільнотою… 5. Звільняється від кримінальної відповідальності особа, крім організатора або керівника електронно-комунікаційних шахрайських організацій, за вчинення злочину, передбаченого частиною другою або третьою цієї статті, якщо вона до повідомлення їй про підозру у вчиненні цього злочину добровільно повідомила

[1] І таке відставання дійсно має місце на практиці – раніше вже повідомлялось, що останні термінологічні зміни щодо технологій електронних комунікацій вносились у Закон біля двох років тому [4].

ISSN 1995-6134

про створення електронно-комунікаційної шахрайської організації або участь у ній та активно сприяла її розкриттю" [12].

Недоліком такого формулювання ст.190[1] може бути термінологічна неоднозначність, коли визначення "електронно-комунікаційне шахрайство" може тлумачитись різними способами та викликати непорозуміння чи непродуктивність при застосуванні закону. Формулювання ст.190[1] зосереджене на конкретних вчинках, пов'язаних із заволодінням майном чи отриманням права на майно, однак у кібершахрайстві можуть існувати інші аспекти, не враховані цим визначенням. При швидкому розвитку технологій електронних комунікацій може виникнути ситуація, коли сформульовані терміни для нових методів атак чи шахрайства стануть застарілими або неадекватними. Відповідно, *недоліком такого формулювання ст.255[4]* може бути занадто широкий обсяг визначення із різних аспектів створення, керівництва, участі у шахрайських організаціях та їх спільнотах. Це робить таке визначення менш ефективним і збільшує його можливу неоднозначність.

Нарешті, слід тут навести й в цілому негативні зауваження Головного науково-експертного управління на проєкт Закону України "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство" [13], в якому "замість коригування термінологічного апарату, вжитого у чинній ст.190 КК, із врахуванням положень Закону України "Про електронні комунікації", пропонується *встановити кримінальну відповідальність за один із різновидів шахрайства – електронно-комунікаційне шахрайство".* А за "новою ст.190[1] КК пропонується встановити, що електронно-комунікаційне шахрайство вважається закінченим з моменту вчинення винною особою зазначених у законі діянь (формальний склад кримінального правопорушення). Тобто, фактично йдеться про пропозицію встановити кримінальну відповідальність за один із різновидів шахрайства на більш ранніх стадіях його вчинення".

При цьому, *"використання електронної комунікації та/або технічних засобів електронних комунікацій визнається електронно-комунікаційним шахрайством,* якщо відповідні діяння вчиняються з метою заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою". Тому й "пропозиція формулювання одного із різновидів шахрайства (електронно-комунікаційного) у межах окремого складу кримінального правопорушення з формальним складом, за наявності при цьому чинної ч.4 ст.190 КК (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки), виглядає сумнівною".

Важливо також зауважити, що термін "шахрайство" використовується й у статтях 192, 222, 262, 308, 312, 313, 320, 357, 410 Кримінального кодексу України. А кіберзлочини, до яких власне відноситься й кібершахрайство, розглядаються у Розділі XVI "Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" Кримінального кодексу України.

Таким чином, можна вважати, що цей законопроєкт був викликаний лише ілюзорною можливістю надмірної адаптації сучасного розуміння електронних комунікацій до використовуваних протягом багатьох років норм Кримінального кодексу України стосовно шахрайства, не вдаючись до необґрунтованого змішування понять і категорій. Вирішення проблеми кібершахрайства вимагає більш обережного та обґрунтованого підходу до правового регулювання, де враховувалися би як сучасні виклики, так і вже існуючі стандарти та норми.

Висновки

1. Кібершахрайство є формою кіберзлочинів, яка використовує інформаційні технології та мережі для вчинення злочинів. Їх поява викликала зміни у правовому підході до протидії незаконним втручанням у роботу інформаційних систем і мереж. А з урахуванням широкого поширення сучасних електронних технологій, в останній час особливого значення набула проблема визначення особливостей електронних комунікацій як складової електронно-комунікаційного шахрайства в контексті сучасних тенденцій та розвитку інформаційного суспільства, в тому числі, й щодо використання в правовому полі.

2. Вітчизняне законодавство з 2021 року набуло декілька профільних нормативно-правових актів, серед яких Закони України "Про електронні комунікації", "Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам", "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії

ISSN 1995-6134

воєнного стану". Їх змістом стало правове осучаснення технологічних новацій, пов'язаних із комунікаційними та інформаційними системами та протидією електронно-комунікаційному шахрайству.

3. Останній Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство передбачав встановлення нових складів злочину для реалізації механізму захисту від шахрайства з використанням електронних комунікацій, але фактично без врахування наявності злочину такого складу у чинній ст.190 Кримінального кодексу України. При цьому в якості недоліку сучасного кримінального законодавства Проєкт посилається на появу нових видів шахрайства, застарілість технічних термінологій, складність правового осучаснення, але занадто переоцінює контекст електронних комунікацій, які є тільки каркасом для кваліфікації електронно-комунікаційного шахрайства.

4. Деякими недоліками законопроєкту визначені термінологічна неоднозначність тлумачення визначення "електронно-комунікаційне шахрайство"; можливість існування у кібершахрайстві інших аспектів, не врахованих із заволодінням майном чи отриманням права на майно; можливість становлення неадекватними для нових методів атак чи шахрайства вже сформульованих термінів при швидкому розвитку технологій електронних комунікацій; занадто широкий обсяг визначення із різних аспектів створення, керівництва, участі у шахрайських організаціях та їх спільнотах тощо.

Конфлікт інтересів

Автори повідомляють про відсутність потенціального конфлікту інтересів.

Вираз вдячності

Дослідження виконано відповідно до плану науково-дослідних робіт Харківського національного університету внутрішніх справ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коновалова І. О. Шахрайство і діджиталізація: історико-правовий аналіз. *Право і суспільство*. 2021. № 3. С. 105–112. http://www.pravoisuspilstvo.org.ua/archive/2021/3_2021/18.pdf
2. Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2022. № 11. С. 546–549. http://lsej.org.ua/11_2022/132.pdf
3. Бабенко А. М., Палій М. В. Крадіжка та шахрайство як види корисливих кримінальних правопорушень проти власності: соціально-правова та віктимологічна характеристика. *Юридичний науковий електронний журнал.* 2023. № 1. С. 564–568. http://lsej.org.ua/1_2023/131.pdf
4. Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам: Закон України від 15.03.2022 № 2137-IX. https://zakon.rada.gov.ua/laws/show/2137-20#Text
5. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX. https://zakon.rada.gov.ua/laws/show/2149-20#Text
6. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131. https://zakon.rada.gov.ua/laws/show/2341-14#Text
7. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство: реєстр. № 10190 від 25.10.2023 / картка. https://itd.rada.gov.ua/billInfo/Bills/Card/43047
8. Пояснювальна записка до проекту Закону України "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство". (27.10.2023). https://itd.rada.gov.ua/billInfo/Bills/pubFile/2040207
9. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. *Офіційний вісник України.* 2021. № 6. Ст. 306. https://zakon.rada.gov.ua/laws/show/1089-20#Text
10. Книженко О. О. Відмежування шахрайства від крадіжок, поєднаних із втручанням у роботу ЕОМ. *Проблеми сучасної поліцеїстики:* тези доп. наук.-практ. конф. (м. Харків, 20 квіт. 2022 р.) / МВС України, Харків. нац. ун-т внут. справ. Харків: ХНУВС, 2022. С. 91–93. http://doi.org/10.5281/zenodo.6532312
11. Васильєв А. А., Пашнєв Д. В. Особливості кваліфікації кіберзлочинів проти власності. *Проблеми правознавства та правоохоронної діяльності.* 2016. № 4 (58). С. 136–143.

12. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство: реєстр. № 10190 від 25.10.2023. https://itd.rada.gov.ua/billInfo/Bills/pubFile/2040203
13. Висновок на проект Закону України "Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство" / Головне науково-експертне управління; до реєстр. № 10190 від 25.10.2023. https://itd.rada.gov.ua/billInfo/Bills/pubFile/2098219

REFERENCES

1. Konovalova, I. O. (2021). Shakhraystvo i didzhytalizatsiya: istoryko-pravovyy analiz [Fraud and digitalization: historical and legal analysis]. *Pravo i suspilstvo,* (3), 105–112. http://www.pravoisuspilstvo.org.ua/archive/2021/3_2021/18.pdf (in Ukr.).
2. Dibrova, T. A., Pisenko, D. O., & Smetanina, N. V. (2022). Kiberzlochynnist ta kibershakhraystvo v umovakh voyennoho stanu [Cybercrime and cyberfraud under martial law]. *Yurydychnyy naukovyy elektronnyy zhurnal,* (11), 546–549. http://lsej.org.ua/11_2022/132.pdf (in Ukr.).
3. Babenko, A. M., & Paliy, M. V. (2023). Kradizhka ta shakhraystvo yak vydy koryslyvykh kryminalnykh pravoporushen proty vlasnosti: sotsialno-pravova ta viktymolohichna kharakterystyka [Theft and fraud as types of self-interested criminal offenses against property: socio-legal and victimological characteristics]. *Yurydychnyy naukovyy elektronnyy zhurnal,* (1), 564–568. http://lsej.org.ua/1_2023/131.pdf (in Ukr.).
4. *Pro vnesennya zmin do Kryminalnoho protsesualnoho kodeksu Ukrayiny ta Zakonu Ukrayiny "Pro elektronni komunikatsiyi" shchodo pidvyshchennya efektyvnosti dosudovoho rozsliduvannya "za haryachymy slidamy" ta protydiyi kiberatakam* [On making changes to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Electronic Communications" in order to increase the efficiency of pre-trial investigation "on hot tracks" and countering cyberattacks]. Zakon Ukrayiny (15.03.2022 No. 2137-9). https://zakon.rada.gov.ua/laws/show/2137-20#Text (in Ukr.).
5. *Pro vnesennya zmin do Kryminalnoho kodeksu Ukrayiny shchodo pidvyshchennya efektyvnosti borotby z kiberzlochynnistyu v umovakh diyi voyennoho stanu* [On making changes to the Criminal Code of Ukraine in order to increase the effectiveness of the fight against cybercrime in the conditions of martial law]. Zakon Ukrayiny (24.03.2022 No. 2149-9). https://zakon.rada.gov.ua/laws/show/2149-20#Text (in Ukr.).
6. Kryminalnyy kodeks Ukrayiny [Criminal codex of Ukraine]. Zakon Ukrayiny (05.04.2001 No. 2341-3). *Vidomosti Verkhovnoyi Rady Ukrayiny,* (25-26), 131. https://zakon.rada.gov.ua/laws/show/2341-14#Text (in Ukr.).
7. *Proekt Zakonu pro vnesennya zmin do Kryminalnoho kodeksu Ukrayiny shchodo vstanovlennya vidpovidalnosti za elektronno-komunikatsiyne shakhraystvo* [Bill Law on Amendments to the Criminal Code of Ukraine on Establishing Liability for Electronic Communications Fraud]. (reyestr. No. 10190 vid 25.10.2023) / kartka. https://itd.rada.gov.ua/billInfo/Bills/Card/43047 (in Ukr.).
8. *Poyasnyuvalna zapyska do proektu Zakonu Ukrayiny "Pro vnesennya zmin do Kryminalnoho kodeksu Ukrayiny shchodo vstanovlennya vidpovidalnosti za elektronno-komunikatsiyne shakhraystvo"* [Explanatory note to the Bill Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Establishing Liability for Electronic Communications Fraud"]. (27.10.2023). https://itd.rada.gov.ua/billInfo/Bills/pubFile/2040207 (in Ukr.).
9. Pro elektronni komunikatsiyi [About electronic communications]. Zakon Ukrayiny (16.12.2020 No. 1089-9). *Ofitsiynyy visnyk Ukrayiny,* 2021, (6), 306. https://zakon.rada.gov.ua/laws/show/1089-20#Text (in Ukr.).
10. Knyzhenko, O. O. (2022). Vidmezhuvannya shakhraystva vid kradizhok, poyednanykh iz vtruchannyam u robotu EOM [Distinguishing fraud from theft combined with computer tampering]. In: *Problemy suchasnoyi politseyistyky:* tezy dop. nauk.-prakt. konf. (m. Kharkiv, 20 kvit. 2022 r.). Kharkiv: KHNUVS (s. 91–93). http://doi.org/10.5281/zenodo.6532312 (in Ukr.).
11. Vasylyev, A. A., & Pashnyev, D. V. (2016). Osoblyvosti kvalifikatsiyi kiberzlochyniv proty vlasnosti [Features of the qualification of cybercrimes against property]. *Problemy pravoznavstva ta pravookhoronnoyi diyalnosti,* 4(58), 136–143 (in Ukr.).
12. *Proekt Zakonu pro vnesennya zmin do Kryminalnoho kodeksu Ukrayiny shchodo vstanovlennya vidpovidalnosti za elektronno-komunikatsiyne shakhraystvo* [Bill Law on Amendments to the Criminal Code of Ukraine on Establishing Liability for Electronic Communications Fraud]. (reyestr. No. 10190 vid 25.10.2023). https://itd.rada.gov.ua/billInfo/Bills/pubFile/2040203 (in Ukr.).
13. *Vysnovok na proekt Zakonu Ukrayiny "Pro vnesennya zmin do Kryminalnoho kodeksu Ukrayiny shchodo vstanovlennya vidpovidalnosti za elektronno-komunikatsiyne shakhraystvo"* [Conclusion on the Bill Law

ISSN 1995-6134

of Ukraine "On Amendments to the Criminal Code of Ukraine on Establishing Liability for Electronic Communications Fraud"]. (do reyestr. No. 10190 vid 25.10.2023). https://itd.rada.gov.ua/billInfo/Bills/pubFile/2098219 (in Ukr.).

ІНФОРМАЦІЯ ПРО СТАТТЮ (ARTICLE INFO)

Published in:
Форум права: 77 pp. 63–72 (4).

Related identifiers:
10.5281/zenodo.10512327
http://forumprava.pp.ua/files/063-072-2023-4-FP-Zozulia,Zozulia_9.pdf
http://nbuv.gov.ua/UJRN/FP_index.htm_2023_4_9.pdf

Received: 10.11.2023
Accepted: 04.12.2023
Published: 08.12.2023
Available online: 08.12.2023

Cite as:

Зозуля, І. В., Зозуля, О. І. (2023). Шахрайство через електронні комунікації: зауваження до законопроєкту. *Форум Права, 77*(4), 63–72. http://doi.org/10.5281/zenodo.10512327

Zozulia, I. V., & Zozulia, O. I. (2023). Shakhraystvo cherez elektronni komunikatsiyi: zauvazhennya do zakonoproyektu [Fraud via Electronic Communications: Comments to the Bill]. *Forum Prava, 77*(4), 63–72. http://doi.org/10.5281/zenodo.10512327