DOI: https://doi.org/10.71404/ppss.2025.1.7

КІБЕРЗЛОЧИННІСТЬ ЯК ВИД ШАХРАЙСТВА: НЕДОЛІКИ КРИМІНАЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Артем Іванович ПЕТРУСЕНКО,

аспірант відділу аспірантури (ад'юнктури) і докторантури Харківського національного університету внутрішніх справ

У контексті стрімкого розвитку цифрових технологій кіберпростір дедалі більше стає платформою для вчинення правопорушень, зокрема шахрайства. Традиційні форми обману зазнають трансформації: зловмисники використовують не лише людську довірливість, а й технічні засоби, алгоритми, програмне забезпечення. Відтак, постає об'єктивна потреба у переосмисленні підходів до кримінально-правової кваліфікації та протидії шахрайству, що вчиняється в інформаційному середовищі.

Шахрайство як кримінально-караний прояв обману з метою заволодіння чужим майном давно стало об'єктом як теоретичних досліджень, так і правозастосовної практики. Проте перехід багатьох сфер суспільного життя у цифрову площину спричинив суттєві зміни у механізмах вчинення шахрайських дій. Сутність діяння заволодіння через введення в оману - зберігається, однак засоби й обставини реалізації злочинного наміру докорінно змінюються. Саме ця трансформація обумовлює необхідність окремого розгляду кібершахрайства як нової форми класичного шахрайства, що характеризується підвищеним рівнем латентності, технічною складністю та часто транскордонним характером. Цифрове шахрайство найчастіше проявляється у використанні спеціальних програм, підроблених вебресурсів, обманних електронних повідомлень або мобільних застосунків, які імітують справжні банківські сервіси чи сервіси державних органів. Жертва добровільно надає зловмиснику доступ до конфіденційної інформації або переказує кошти, перебуваючи в омані щодо справжньої природи запиту[1, с. 5]. Водночас такий добровільний характер передачі майна є результатом маніпулятивного впливу, що в юридичному значенні кваліфікується як обман.

Особливістю кібершахрайства є те, що обман часто не має безпосереднього людського носія. Його реалізатором виступає не конкретна особа, яка веде діалог з жертвою, а алгоритм, чат-бот, програмний код або інтерфейс, що створює ілюзію легітимності. У зв'язку з цим традиційне розуміння обману як усного чи письмового повідомлення неправдивої інформації втрачає релевантність у сучасних умовах. Визначення, які були вироблені судовою практикою щодо шахрайства у фізичному світі, не завжди придатні для застосування у віртуальній реальності, де зловмисник може залишатися повністю

анонімним, а процес вчинення злочину автоматизований. Крім того, цифрове шахрайство дедалі частіше виходить за межі звичного посягання на майно[2, с. 83]. Зловмисники прагнуть отримати не лише фінансову вигоду, а й персональні дані, облікові записи, криптовалютні ключі, доступ до цифрової ідентичності особи. Таким чином, розширюється предмет злочину, що також має відображатися у правовій оцінці. Злочин перестає бути виключно посяганням на власність і набуває ознак посягання на безпеку інформаційного простору, приватність особи, свободу волевиявлення.

Юридична доктрина та судова практика стикаються з труднощами у доведенні наявності обману у випадках, коли він реалізується не в очевидній формі, а шляхом створення оманливого середовища. Наприклад, фальшивий сайт може повністю дублювати зовнішній вигляд офіційного банківського ресурсу, що унеможливлює візуальне розпізнання підробки без технічного аналізу[3, с. 54]. У такій ситуації лише комплексна експертиза, що поєднує правові та кібернетичні знання, може дозволити кваліфікувати діяння як шахрайство і виявити суб'єкта злочину. Зокрема, це стосується випадків, коли зловмисник використовує шкідливе програмне забезпечення або фішингові листи, які розсилаються автоматично і не передбачають безпосередньої взаємодії з жертвою. Відсутність чітко визначених ознак кібершахрайства у законодавстві створює проблеми як для розслідування, так і для подальшого судового розгляду. Неоднозначність тлумачення, складність встановлення причинно-наслідкового зв'язку між діями зловмисника та наслідками для потерпілого, низький рівень технічної обізнаності правозастосовних органів усі ці фактори сприяють як зростанню латентності злочинів, так і уникненню кримінальної відповідальності з боку винних осіб.

На нашу думку, кібершахрайство як явище поєднує у собі риси класичного шахрайства, інформаційних злочинів і маніпуляцій з електронними даними. Його природа вимагає перегляду підходів до визначення обману, засобів доказування вини та кваліфікації злочину. Без відповідного теоретичного обґрунтування та нормативної конкретизації ефективна протидія цій формі злочинності залишається малореалістичною.

Проблематика нормативного забезпечення протидії кібершахрайству в українському кримінальному праві залишається відкритою та потребує глибокого осмислення. Законодавець досі не виокремив кібершахрайство як самостійний склад злочину, що негативно впливає як на точність кваліфікації відповідних діянь, так і на ефективність притягнення до відповідальності осіб, які їх вчиняють. Наявна редакція статті 190 Кримінального кодексу України передбачає відповідальність за заволодіння майном шляхом обману або зловживання довірою, проте не враховує специфіку кіберпростору, де обман реалізується шляхом технічних засобів, складних програмних рішень, штучного інтелекту чи автоматизованих алгоритмів. Водночас

використання новітніх технологій кардинально змінює як спосіб вчинення злочину, так і його наслідки. Зловмисники діють не в реальному фізичному середовищі, а в мережевому просторі, де інформація має цінність не меншу, ніж матеріальні активи. Особливої актуальності набуває відсутність у кримінальному праві України положень, які визнавали би обтяжуючими обставинами використання технологічних засобів під час вчинення шахрайських дій[4, с. 105]. Ані бот-мережі, ані сервіси анонімізації, ані технології розподіленого реєстру чи елементи глибокого навчання, які зловмисники активно застосовують у своїй діяльності, не знаходять відображення у законодавстві. Це ускладнює доведення особливого характеру суспільної небезпеки цифрових форм шахрайства та не дозволяє ефективно диференціювати покарання.

Особливої уваги потребує питання нормативного розмежування шахрайства як класичного злочину проти власності та кримінально караних діянь, пов'язаних із несанкціонованим втручанням в електронні системи. Статті 361–363 Кримінального кодексу стосуються посягань на інформаційну безпеку, проте на практиці важко відмежувати такі діяння від шахрайства, якщо їх результатом є незаконне заволодіння чужим майном. У таких випадках правозастосувачі нерідко опиняються перед необхідністю обирати між кількома статтями, які не мають чіткого розмежування щодо об'єкта посягання, способу його реалізації або суб'єктивної сторони злочину. Невизначеність меж складів порушує принцип правової визначеності та створює підґрунтя для неоднакової практики, що знижує довіру до системи правосуддя. Ситуація ускладнюється ще й тим, що кіберзлочини майже завжди мають міжнародний характер[5, с. 118]. Операції часто здійснюються з території інших держав, сервери, які використовуються для реалізації шахрайських схем, розміщуються у країнах із різною правовою культурою та рівнем правового регулювання, а встановлення місцезнаходження зловмисника нерідко є практично неможливим.

Анонімізуючі технології, такі як Tor або VPN, лише поглиблюють цю проблему, унеможливлюючи ідентифікацію конкретної особи. У таких обставинах правоохоронні органи стикаються із серйозними труднощами у сфері міжнародного співробітництва, зокрема при виконанні запитів про правову допомогу або екстрадицію, а також у частині доступу до цифрових доказів, які зберігаються за межами України.

Незважаючи на загальне визнання актуальності боротьби з кіберзлочинністю, українське кримінальне право залишається фрагментарним і реактивним щодо цієї категорії правопорушень. Відсутність законодавчого узагальнення понять, які описують типові сценарії вчинення цифрового шахрайства, призводить до правової невизначеності як на етапі розслідування, так і під час судового розгляду. З огляду на швидкий розвиток технологій, саме гнучкість правової системи, її здатність оперативно адаптуватися до нових

викликів, повинна стати визначальним фактором ефективної протидії цифровим формам обману. Без системного оновлення кримінального законодавства в частині регулювання кібершахрайства неможливо говорити про повноцінну реакцію держави на загрози, які продукує інформаційне суспільство.

Отже, кібершахрайство є новітнім викликом для кримінального права, що вимагає системного і гнучкого реагування. Наявне кримінально-правове регулювання не здатне в повній мірі охопити специфіку цифрових форм обману, що призводить до правових прогалин та ускладнює ефективну протидію.

З огляду на це, необхідним є:

- розроблення окремої норми або підрозділу в межах Кримінального кодексу України, присвяченої саме шахрайству у сфері інформаційних технологій;
- чітке визначення поняття "кібершахрайства" на законодавчому рівні;
- розробка єдиної методики кваліфікації кіберзлочинів з елементом обману;
- розширення міжнародного співробітництва у сфері кримінального переслідування осіб, які вчиняють такі діяння транснаціонально.

Лише за умови комплексного підходу до кодифікації і тлумачення норм кримінального законодавства можливо створити правове середовище, здатне ефективно протистояти кіберзагрозам, не втрачаючи при цьому засад правової визначеності та справедливості.

Список використаних джерел

1. Антощук С. А. Кібершахрайство в Україні в умовах війни. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України. Львів. ЛьвДУВС. 2024. С. 4-6.
2. Джафарова О.В., Дзюбенко М.О., Зінченко Д.А. Аналіз ефективності методів криміналістичного аудиту в діяльності національної поліції України для протидії організованій злочинності. *Актуальні питання судової експертизи і криміналістики.* М-во юстиції України, Нац. наук. центр «Ін-т суд. експертиз ім. Засл. проф. М. С. Бокаріуса». Харків, 2024. – С. 82-84.
3. Жаров Л. В. Основні види кібершахрайства та способи протидії. *Застосування інформаційних технологій у діяльності правоохоронних органів.* МВС України. Харків. ХНУВС. 2021. С. 52-54.
4. Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів. *Застосування інформаційних технологій у правоохоронній діяльності.* МВС України. Харків. ХНУВС. 2023. 105-107.
5. Зінченко Д. А., Макарова О.П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. *Протидія кіберзлочинності та торгівлі людьми. МВС України.* Наук. парк «Наука та безпека». Вінниця. ХНУВС. 2023. С. 118-121.