В. В. Іванова
здоб. ІІІ курсу, спеціальність «Право»
Одеський національний університет імені І. І. Мечникова
***Науковий керівник:** д. ю. н. доцент кафедри кримінального права, кримінального процесу та криміналістики Б. М. Орловський*

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ОНЛАЙН-ШАХРАЙСТВО: СУЧАСНІ СХЕМИ ТА ПОКАРАННЯ

У сучасному цифровому суспільстві злочинність дедалі частіше набуває нових форм, серед яких онлайн-шахрайство займає одне з провідних місць. З розвитком інформаційних технологій зростає не лише рівень комфорту для користувачів, а й спектр загроз – від фішингових атак до складних схем виманювання персональних даних і грошей. Відповідно, зростає і кількість постраждалих, серед яких не лише необізнані користувачі, а й бізнес-структури та державні установи. За інформацією Кіберполіції, онлайн-шахрайство стало однією з найпоширеніших категорій кіберзлочинів в Україні [3].

Попри закріплення загальних норм про шахрайство в Кримінальному кодексі України, специфіка вчинення таких злочинів через Інтернет потребує не лише оновлення правозастосовчої практики, а й глибшого наукового аналізу. Актуальність теми зумовлена необхідністю адаптації кримінального законодавства до цифрових викликів, а також пошуку ефективних механізмів

виявлення та притягнення до відповідальності осіб, які вдаються до онлайн-шахрайства [1, ст. 190].

Онлайн-шахрайство – це новий виклик для кримінального права, що потребує оперативної реакції. На відміну від класичного шахрайства, злочинець діє дистанційно, приховуючи свою особу й часто перебуваючи поза юрисдикцією України [2, с. 641].

Стаття 190 КК України визначає шахрайство як заволодіння майном шляхом обману або зловживання довірою, але не враховує особливостей цифрового середовища. Тому онлайн-шахрайство кваліфікується за цією ж нормою, хоча його специфіка значно ширша.

Найтиповішими схемами інтернет-шахрайства є: створення фейкових сайтів і онлайн-магазинів, де товари або послуги не мають наміру бути доставленими; фішинг, що передбачає збір особистої інформації користувачів через електронні листи чи сайти-двійники; телефонні дзвінки або повідомлення, які імітують спілкування з банками чи державними органами з метою отримання доступу до рахунків [3]. Злочинці вміло використовують психологічний тиск, паніку та навіть штучний інтелект для генерації правдоподібних повідомлень, що підвищує ефективність обману.

За даними досліджень, з 2022 року кількість звернень громадян щодо шахрайства в мережі зросла більш ніж на 30 %, а кількість завершених судових проваджень у справах про онлайн-шахрайство залишається порівняно низькою [3]. Це свідчить про наявність серйозних проблем у процесі виявлення, фіксації та доведення вини зловмисника.

Шахраї часто діють через підставних осіб, анонімні акаунти чи криптовалюти, що ускладнює розслідування. Для доведення вини потрібна співпраця слідства з кіберпідрозділами, банками та іноземними платформами.

Об’єкт шахрайства змінився: замість грошей чи техніки зловмисники все частіше посягають на персональні дані, цифрову репутацію, криптоактиви. Через нормативну невизначеність складно притягти їх до відповідальності, тому актуальним є доповнення законодавства, зокрема введення ознаки «шахрайство з використанням інформаційних технологій».

І.М. Чекмарьова зазначає, що відсутність єдиного підходу до кваліфікації та прогалини в доказуванні дозволяють окремим видам онлайн-шахрайства уникати оцінки [2, с. 642]. Це свідчить про відставання кримінального права від цифрових реалій.

Транснаціональний характер онлайн-шахрайства змушує українські правоохоронні органи звертатися до інших держав за правовою допомогою. Через затримки або відмови, особливо з боку недружніх юрисдикцій, це часто ускладнює або унеможливлює розслідування [3].

У 2022 році Кіберполіція разом із НБУ та Держспецзв'язку започаткували кампанію з інформування громадян про онлайн-шахрайство [3]. Проте злочинці постійно адаптують нові технології - deepfake, боти, криптовалюти, анонімні сервіси - що ускладнює протидію.

Найефективніше вдається притягувати до відповідальності учасників організованих груп, де кожен має роль — від оператора до «дропа». Такі злочини кваліфікують не лише за ст. 190, а й за ст. 255 і 361 КК України [1, ст. 255; ст. 361].

Онлайн-шахрайство охоплює юридичні, соціальні й технічні аспекти, тому боротьба з ним потребує не лише змін у законодавстві, а й міжгалузевої співпраці фахівців і установ.

Динаміка схем онлайн-шахрайства вимагає адаптації кримінального права, зокрема запровадження ознак злочинів, пов'язаних з ІТ [2, с. 643; 3], а також посилення технічного й кадрового забезпечення слідства.

Частина 4 статті 190 КК України вже передбачає відповідальність за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки [1, ст. 190]. Однак цей термін є вузьким і технічно застарілим, адже не охоплює сучасні засоби - мобільні пристрої, хмарні сервіси, штучний інтелект. Термін «інформаційні технології» є ширшим, сучасним і узгоджується з іншими нормативними актами. Тому доцільно уточнити або доповнити ч. 4 ст. 190 КК України відповідною кваліфікуючою ознакою: «вчинення шахрайства з використанням інформаційних технологій».

Подолання онлайн-шахрайства можливе лише за умови оновлення законодавства, ефективного правозастосування та взаємодії держави з ІТ-сферою і суспільством.

Література:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // *Верховна Рада України*. URL: https://zakon.rada.gov.ua/ laws/show/2341-14 (дата звернення: 02.04.2025).

2. Чекмарьова І. М. Шахрайство в Інтернеті як один із видів шахрайства // *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2024. № 2. С. 639–643. URL: https://app-journal.in.ua/wp-content/uploads/2024/04/108.pdf (дата звернення: 02.04.2025).

3. Як захистити свої гроші від шахраїв в інтернеті: спільний проект Кіберполіції, Держспецзв'язку та НБУ [Електронний ресурс] // Київська обласна військова адміністрація. 2022. 16 червня. URL: https://koda.gov.ua/yak-zahystyty-svoyi-groshi-vid-shahrayiv-v-interneti-spilnyj-proekt-kiberpolicziyi-derzhspeczzvyazku-ta-nbu/ (дата звернення: 02.04.2025).