Желєзньова К. О., здобувач
Науковий керівник:Татаренко С. В.,
доктор філософії в галузі права,
Донецький державний університет внутрішніх справ
місто Кропивницький

ОПЕРАТИВНО-РОЗШУКОВА ПРОТИДІЯ ШАХРАЙСТВАМ, ВЧИНЕНИМ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ, В УМОВАХ ВОЄННОГО СТАНУ

Шахрайство (ст. 190 КК України) [1] залишається одним із найпоширеніших кримінальних правопорушень проти власності, а з розвитком інформаційно-комунікаційних технологій воно дедалі частіше вчиняється дистанційно: через телефонні дзвінки, месенджери, соціальні мережі та фейкові вебсайти. За даними Офісу Генерального прокурора, наведеними А. В. Ковальським, кількість облікованих кримінальних правопорушень, передбачених ч. 2–4 ст. 190 КК України, зросла з 14 760 у 2021 році до 53 547 у 2023 році [2, с. 603]. Ю. Ю. Царук слушно зазначає, що в умовах воєнного стану вчинення таких діянь значною мірою полегшується, а ризик особи стати потерпілою зростає [3, с. 100].

Воєнний стан зумовив появу нових шахрайських схем, які використовують емоційний стан громадян. Серед типових Ю. Ю. Царук називає шахрайство під час збору коштів на потреби ЗСУ чи на автомобілі для військових, фейкові збори на лікування дітей, фейкові оголошення про продаж автомобілів, а також повідомлення на кшталт «ваш син потрапив у полон» [3, с. 102–103]. Поширеними залишаються й «класичні» способи: фішинг, тобто надсилання повідомлень з посиланнями на фейкові вебсайти, та соціальна інженерія, коли зловмисник видає себе за працівника банку чи іншу довірену особу [2, с. 604–605].

Для ефективної протидії таким правопорушенням оперативні підрозділи мають спиратися на їх оперативно-розшукову характеристику. За Ю. Ю. Царуком, вона охоплює відомості про вид злочину та його суспільну небезпечність, предмет посягання, середовище вчинення, способи готування, вчинення та приховання слідів [3, с. 100–101]. А. В. Ковальський виокремлює три групи осіб, які вчиняють кібершахрайства: особи з різним рівнем навичок, які раніше не вчиняли правопорушень; особи без спеціальних навичок, які діють у складі злочинних угруповань; особи з високим рівнем навичок, які вчиняють такі правопорушення систематично [2, с. 605]. Важливо, що сліди кібершахрайства можуть залишатися й поза кіберпростором, зокрема у вигляді матеріальних слідів знищення пристроїв чи серверів [2, с. 605]. На нашу думку, саме поєднання цифрових і «традиційних» слідів (рух коштів через банківські картки, придбання SIM-карток, оренда приміщень для кол-центрів, переміщення так званих «дропів») дає оперативним працівникам найбільше можливостей для встановлення організаторів схем.

Держава посилює кримінально-правові засоби протидії цим явищам. 16 вересня 2026 року Верховна Рада України ухвалила, а 17 вересня 2026 року Президент України підписав закон (законопроєкт № 10190), яким КК України доповнюється, зокрема, ст. 190-1 «Шахрайство з використанням електронних комунікацій» та статтями про відповідальність за створення шахрайських організацій (кол-центрів), керівництво ними, участь у них і залучення до них інших осіб [4]. Ці зміни створюють нові правові підстави для оперативного документування діяльності організованих шахрайських груп.

Водночас оперативно-розшукове законодавство не встигає за розвитком технологій. Правові засади оперативно-розшукової діяльності визначає Закон України «Про оперативно-розшукову діяльність» [5]. О. С. Тарасенко та О. М. Стрільців наголошують, що цей Закон ухвалено ще 1992 року, наявні зміни до нього не враховують сучасних інформаційних технологій, і йому бракує системної інтеграції з національним кіберзаконодавством [6, с. 17]. Зокрема, не визначено порядок збору, збереження та використання електронних (цифрових) доказів під час оперативно-розшукової діяльності, а також спеціальні процедури доступу правоохоронних органів до даних, які зберігаються за кордоном [6, с. 19–20]. Для протидії шахрайствам це особливо відчутно, оскільки кол-центри часто розміщують сервери та облікові записи за межами України. Закон України «Про основні засади

забезпечення кібербезпеки України» відносить Національну поліцію до основних суб'єктів національної системи кібербезпеки [7], проте механізми взаємодії підрозділів кримінальної та кіберполіції під час документування таких правопорушень потребують чіткішого врегулювання.

З огляду на викладене, пропонуємо: по-перше, доповнити Закон України «Про оперативно-розшукову діяльність» положеннями про порядок збору, збереження та використання цифрових даних; по-друге, налагодити оперативний обмін інформацією між підрозділами кримінальної поліції, кіберполіції, банківськими установами та операторами мобільного зв'язку щодо рахунків, карток і номерів, які використовуються в шахрайських схемах; по-третє, під час планування оперативних заходів ураховувати оперативно-розшукову характеристику цих правопорушень і поєднувати оперативно-розшукові заходи з негласними слідчими (розшуковими) діями, на чому наголошує і Ю. Ю. Царук [3, с. 104]; по-четверте, посилити профілактичну роботу з населенням щодо найпоширеніших шахрайських схем воєнного часу.

Узагальнюючи викладене вважаємо, що шахрайства з використанням інформаційно-комунікаційних технологій в умовах воєнного стану набули масового характеру й нових форм. Ефективна протидія їм потребує оновлення оперативно-розшукового законодавства, налагодженої взаємодії правоохоронних органів з банками та операторами зв'язку, а також належної підготовки оперативних працівників до роботи з цифровими слідами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний кодекс України : Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 05.10.2026).

2. Ковальський А. В. Криміналістична характеристика шахрайств, вчинених із використанням інформаційних комп'ютерних технологій. Юридичний науковий електронний журнал. 2024. № 1. С. 603–606. DOI: https://doi.org/10.32782/2524-0374/2024-1/143.

3. Царук Ю. Ю. Оперативно-розшукова характеристика шахрайств, вчинених в умовах воєнного стану з використанням електронно-обчислювальної техніки. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2024. № 2. С. 98–105.

4. Зеленський підписав закон про криміналізацію діяльності шахрайських кол-центрів. Mind. 2026. 17 верес. URL: https://mind.ua/news/20309904(дата звернення: 04.10.2026).

5. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2135-12 (дата звернення: 05.10.2026)

6. Тарасенко О. С., Стрільців О. М. Напрями вдосконалення законодавства, що регулює оперативно-розшукову діяльність, з метою протидії кримінальним правопорушенням в інформаційному просторі. Наука і правоохорона. 2025. № 4 (70). С. 17–23. DOI: https://doi.org/10.33270/05257004.2.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 05.10.2026)