LEGAL SCIENCES

Diana Vakulenko
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
Scientific supervisor:
Oksana Ilina
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID iD: 0000-0003-4848-3120

WAR AS A CATALYST FOR DIGITAL CRIME: A CRIMINOLOGICAL PROFILE OF OFFENDERS COMMITTING CRIMINAL OFFENCES USING INFORMATION TECHNOLOGIES UNDER MARTIAL LAW IN UKRAINE

Abstract. The paper examines the influence of the full-scale war on digital crime in Ukraine, focusing on fraud committed using information technologies. It considers the social and demographic characteristics, motivations and organizational features of offenders, as well as the conditions facilitating their involvement in criminal activity. Particular attention is paid to fraudulent call centres, changes in criminal legislation and the challenges of combating digitally mediated offences under martial law. The paper emphasizes the need for a comprehensive approach combining legal, organizational and preventive measures.
Keywords: digital crime, criminological profile, information technologies, fraud, martial law, crime prevention.

Діана Вакуленко
Київський національний університет
імені Тараса Шевченка, Київ, Україна
Науковий керівник:
Оксана Ільїна
Київський національний університет
імені Тараса Шевченка, Київ, Україна
ORCID iD: 0000-0003-4848-3120

ВІЙНА ЯК КАТАЛІЗАТОР ЦИФРОВОЇ ЗЛОЧИННОСТІ: КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ОСОБИ ЗЛОЧИНЦЯ, ЯКИЙ ВЧИНЯЄ КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Анотація. Розглянуто вплив повномасштабної війни на цифрову злочинність в Україні з акцентом на шахрайство з використанням інформаційних технологій. Проаналізовано соціально-демографічні характеристики, мотивацію та організаційні особливості осіб, які вчиняють такі правопорушення, а також умови залучення до злочинної діяльності. Увагу приділено шахрайським кол-центрам, змінам кримінального законодавства та проблемам протидії цифровим правопорушенням в умовах воєнного стану. Наголошено на потребі комплексного поєднання правових, організаційних і профілактичних заходів.
Ключові слова: цифрова злочинність, особа злочинця, інформаційні технології, шахрайство, воєнний стан, запобігання злочинності.

Повномасштабна війна, розпочата російською федерацією проти України 24 лютого 2022 року, стала не лише військовим, а й потужним соціальним і криміногенним каталізатором. Вона суттєво трансформувала структуру злочинності, особливо у сфері використання інформаційних технологій. Найбільш помітним і суспільно небезпечним проявом цієї трансформації стало стрімке зростання шахрайства, вчинюваного з використанням електронних комунікацій. Умови воєнного стану, економічна криза, масове внутрішнє переміщення населення, психологічне напруження, зниження реальних доходів і широке поширення смартфонів та месенджерів створили ідеальне середовище для розквіту цифрової злочинності [1]. Актуальність дослідження особи злочинця, який вчиняє кримінальні правопорушення з використанням інформаційних технологій в умовах воєнного стану, зумовлена кількома чинниками. По-перше, шахрайство в інтернеті набуло масового характеру і щодня завдає значної матеріальної шкоди громадянам України та іноземцям. По-друге, саме особа злочинця є центральним елементом кримінологічної характеристики, оскільки саме через розуміння мотивів, соціально-демографічних і психологічних рис можна ефективно будувати систему запобігання. По-третє, війна не лише збільшила кількість таких злочинів, а й якісно змінила портрет особи, яка їх вчиняє [2].

Статистичні дані переконливо свідчать про масштаби явища. У 2025 році зареєстровано майже 49 тис. кримінальних проваджень за ст. 190 КК України. Онлайн-шахрайства становили близько 38–40 % від загальної кількості. За даними Національного банку України, у 2025 році зафіксовано 256 тис. шахрайських операцій з платіжними картками. Хоча кількість операцій дещо зменшилася, сума збитків зросла на 24 % і досягла 1,4 млрд грн. Середня сума однієї афери перевищила 5,5 тис. грн. Найбільш поширеними схемами стали фішинг від імені банків і "СБУ", романтичне шахрайство, продаж неіснуючих дронів, тепловізорів і автомобілів "для потреб ЗСУ", а також фейкові волонтерські збори [1; 3].

Особу злочинця, який вчиняє шахрайство з використанням інформаційних технологій в умовах воєнного стану, можна охарактеризувати за кількома групами ознак. Соціально-демографічна характеристика: переважна більшість таких осіб це чоловіки. Вік більшості виконавців коливається в межах 18–35 років, проте дедалі частіше до злочинної діяльності залучаються неповнолітні. Значна частина має середню або незакінчену вищу освіту. Професійні ІТ-спеціалісти серед них зустрічаються рідко, а тому здебільшого це особи з базовими навичками роботи зі смартфоном, месенджерами та соціальними мережами. Жінки частіше виконують роль операторів соціальної інженерії, ведуть романтичне листування або "волонтерські" збори. Саме підлітків і молодь зараз найлегше втягнути в злочинну організацію через обіцянки швидкого заробітку та відсутність видимих ризиків [2]. Морально-психологічна характеристика: типовими рисами є низька емпатія, цинічне ставлення до жертв ("самі винні, що повірили"), орієнтація на швидке збагачення, готовність працювати в умовах високої анонімності та знижений страх перед покаранням. Багато хто з них виправдовує свої дії тим, що "обманює тільки багатих" або "бере

гроші у тих, хто може собі дозволити". В умовах війни з'явилася ще одна небезпечна риса — використання патріотичних почуттів громадян як інструменту маніпуляції. Важливим психологічним фактором є орієнтація молоді на суспільство, у якому вона живе і з яким комунікує. Як і герой роману Панаса Мирного та Івана Білика "Хіба ревуть воли, як ясла повні?" Чіпка Варениченко, який став на злочинний шлях під впливом оточення, сучасна молодь також формує свої цінності під впливом середовища. Якщо в оточенні панує культ "легких грошей", підліток з високою ймовірністю обере саме цей шлях [3]. Мотиваційна сфера: домінуючою залишається корислива мотивація (70–80 %). Низький рівень заробітних плат у легальній сфері, особливо серед молоді, відсутність стабільної роботи, інфляція та бажання мати гроші "на свої забаганки" (гаджети, одяг, розваги), які батьки не можуть або не хочуть забезпечувати, штовхають підлітків і молодих людей на злочинний шлях. У соціальних мережах (Telegram, Instagram, TikTok) масово поширювалися оголошення про "роботу у кол-центрі з високим доходом", "легкі гроші без досвіду та відповідальності". Багато хто замість навчання йшов працювати в шахрайські кол-центри, де отримував від кількох сотень до кількох тисяч доларів на місяць залежно від результативності та суми вчинюваного шахрайства. Якщо всі навколо прагнуть заробити "легкі гроші", підліток логічно, що не піде на низькооплачувану роботу для початківців, бо має альтернативу — кол-центр, який обіцяє тисячі доларів на місяць без особливого досвіду. Це все відкриває нам системну проблему всієї країни, а саме відсутність можливості отримати нормальну роботу, не маючи досвіду, і не можливість його отримати, бо нікуди без нього не беруть. Війна лише посилила цю тенденцію.

Важливим фактором став низький поріг входу в злочинну діяльність і мала ймовірність викриття. Для роботи в кол-центрі або для створення схеми "закладок" наркотиків достатньо мати смартфон, базові навички спілкування та готовність працювати за відсоток від "здобичі". Анонімність інтернету, використання VPN, віртуальних номерів і криптовалюти суттєво знижували відчуття ризику. Саме мала ймовірність бути викритим через особливості цифрового простору є одним із ключових чинників, чому особи обирають саме цей вид злочинної діяльності. Окремо слід відзначити роль війни як каталізатора. Втрата роботи, житла, близьких, постійний стрес і почуття невизначеності призвели до того, що частина громадян, які раніше не мали судимостей, почала шукати швидкі способи заробітку. Особливо вразливою виявилася молодь. Саме вона стала основним кадровим резервом шахрайських кол-центрів [5].

16 вересня 2026 року Верховна Рада України ухвалила Закон України № 4986-IX "Про внесення зміни до Кримінального кодексу України щодо посилення відповідальності за створення електронно-комунікаційних шахрайських організованих груп (шахрайських кол-центрів) та залучення до участі в них". Президент України Володимир Зеленський підписав цей Закон того ж дня. Ним Кримінальний кодекс України доповнено статтею 255-4 "Створення, керівництво електронно-комунікаційною шахрайською організованою групою або участь у ній". Створення або керівництво такою групою карається позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна, участь у ній — від

п’яти до десяти років. Після набрання чинності законом частина працівників кол-центрів дійсно припинила діяльність через страх жорсткого покарання. Однак повністю викорінити явище не вдалося, бо схеми почали дробитися на менші групи та переходити в більш законспірований формат [4].

Варто також відзначити суттєву зміну структури злочинних груп, які спеціалізуються на шахрайстві з використанням електронних комунікацій. Якщо до прийняття Закону України № 4986-IX шахрайські кол-центри переважно функціонували як відносно великі організовані структури з чіткою ієрархією, розподілом ролей (організатор, керівники змін, оператори, IT-спеціалісти, "виводили" коштів) та стаціонарними офісами, то після посилення кримінальної відповідальності спостерігається явна тенденція до їх дроблення. На зміну великим "офісам" приходять невеликі мобільні групи чисельністю 3–5 осіб. Такі міні-групи працюють значно більш конспіративно: вони швидко змінюють місця розташування, використовують орендовані квартири на короткий термін, постійно оновлюють номери телефонів, акаунти в месенджерах і VPN-сервіси. Розподіл функцій у них менш формалізований, а комунікація максимально обмежена. Усе це суттєво ускладнює роботу правоохоронних органів із виявлення, документування та притягнення винних до відповідальності. Зазначена трансформація наочно демонструє високу адаптивність цифрової злочинності до змін у законодавстві та правозастосовній практиці.

Ситуація ускладнюється корупційними ризиками. У вересні 2026 року НАБУ і САП у межах операції "Карфаген" викрили злочинну організацію, яку, за версією слідства, очолював один із керівників структурних підрозділів Офісу Генерального прокурора. Учасники організації систематично одержували неправомірну вигоду від "кришування" шахрайських кол-центрів і легалізовували мільйонні статки. Це свідчить про те, що цифрова злочинність воєнного часу тісно переплітається з корупцією в правоохоронних органах і потребує особливої уваги. Особливу небезпеку становило те, що корупційні зв’язки всередині правоохоронної системи дозволяли організаторам шахрайських схем заздалегідь отримувати інформацію про заплановані перевірки та обшуки. Це давало можливість своєчасно вивозити техніку, знищувати докази та переводити діяльність у більш законспірований формат. Таким чином, корупція виступала не лише як супутник цифрової злочинності, а й як один із ключових факторів її стійкості та адаптивності.

Підсумовуючи, можна констатувати, що війна виступила потужним каталізатором цифрової злочинності, особливо шахрайства з використанням інформаційних технологій. Вона створила комплекс економічних, психологічних і організаційних умов, за яких особа з корисливою мотивацією, базовими цифровими навичками та низьким рівнем соціальної відповідальності легко стає учасником шахрайських схем. Особливо вразливою виявилася молодь, яку активно залучають через соціальні мережі обіцянками "легких грошей" і яка орієнтується на цінності свого оточення. Прийняття Закону № 4986-IX та запровадження статті 255-4 КК України є важливим кроком у протидії цьому явищу. Проте для ефективного запобігання необхідне комплексне поєднання жорсткої кримінальної відповідальності, створення реальних

можливостей для легального працевлаштування молоді без досвіду, підвищення рівня цифрової грамотності населення та очищення правоохоронних органів від корупційних проявів.

СПИСОК ДЖЕРЕЛ

1. Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. Young Scientist. 2022. № 11 (111). С. 546–550.

2. Черніков Б. Ю. Кримінологічна характеристика кіберзлочинності. Young Scientist. 2021. № 11 (63). С. 94–98.

3. Топчій В. В. Цифровізація у системі детермінант злочинності. Ірпінський юридичний часопис. 2024. Вип. 1 (14). С. 132–137.

4. Закон України "Про внесення зміни до Кримінального кодексу України щодо посилення відповідальності за створення електронно-комунікаційних шахрайських організованих груп (шахрайських кол-центрів) та залучення до участі в них" від 16.09.2026 № 4986-IX.

5. Зозуля І. В., Зозуля О. І. Шахрайство через електронні комунікації: зауваження до законопроєкту. Forum Prava. 2023. № 4. С. 63–72.

6. Луценко Ю. В. Проблеми протидії злочинності в сучасних умовах. Таврійський національний університет імені В. І. Вернадського. 2025. Т. 4. С. 117–123.