

ПРОТИДІЯ ПРАВООХОРОННИМИ ОРГАНАМИ ШАХРАЙСТВУ, ЩО ВЧИНЯЄТЬСЯ З ВИКОРИСТАННЯМ МЕРЕЖІ «ІНТЕРНЕТ»: ДОСВІД ЄВРОПИ

COUNTERACTING FRAUD COMMITTED VIA THE INTERNET BY LAW ENFORCEMENT AGENCIES: EUROPEAN EXPERIENCE

Севрук І.Ю., аспірантка наукової лабораторії
з проблем протидії злочинності

Навчально-науковий інститут № 1
Національної академії внутрішніх справ

У статті проаналізовано положення нормативно-правових актів і відповідну правозастосовну практику діяльності іноземних правоохоронних органів щодо протидії шахрайству, що вчиняється через мережу «Інтернет». Установлено, що правоохоронними органами світового масштабу, що здійснюють запобігання та протидію шахрайству, що вчиняється через мережу «Інтернет», є: Інтерпол (International Criminal Police Commission), Європол (European Police Office), Європейський центр кіберзлочинності (EC3), Європейський відділ з боротьби з шахрайством (OLAF), Робоча група Європейського Союзу з протидії інтернет-шахрайствам, Інтернет-поліція LEO (1) силові структури: «Керівництво», «Цивільний підрозділ», «Підготовчий підрозділ», (2) урядовці, (3) волонтери), Група з розробки фінансових заходів боротьби з відмиванням грошей (Financial Action Task Force – FATF), Євроюст (Eurojust – європейське агентство, що співпрацює з судовими та поліцейськими органами країн-членів ЄС). Існування вказаних структур є відповіддю світової спільноти на протиправну діяльність організованих груп, які спеціалізуються на шахрайстві, що вчиняється з використанням мережі «Інтернет». Дослідженням установлено, що більшість іноземних країн не містять спеціальних норм, які регламентують відповідальність за шахрайство, що вчиняється з використанням мережі «Інтернет», відповідно підходи до протидії таким злочинам обумовлені особливостями національного законодавства. Отже, для пошуку ефективних моделей протидії шахрайству, що вчиняється з використанням мережі «Інтернет», було вивчено іноземний досвід та структуру їх спеціальних підрозділів, поліцейських відомств, а також їх функцій, що абсолютно різняться за своєю сутністю. Так, у європейських країнах та США функції протидії поступаються місцем запобіганню, на відміну від вищевказаних країн та США, азійські держави суворо дотримуються жорстких репресивних заходів. На основі опрацьованого та узагальненого сучасного передового іноземного досвіду розроблено науково обґрунтовані рекомендації щодо протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет».

Ключові слова: кіберполіція, спеціальні підрозділи, протидія, розслідування, взаємодія, шахрайство, мережа «Інтернет», зарубіжний досвід.

The article analyzes the provisions of regulatory legal acts and the relevant law enforcement practice of foreign law enforcement agencies in terms of combating fraud committed via the Internet. It has been established that the authorities of worldwide scope preventing and counteracting fraud committed via the Internet are: Interpol (International Criminal Police Commission), Europol (European Police Office), European Cybercrime Center (EC3), European Anti-Fraud Office (OLAF), European Union Working Group on Internet Fraud, Internet Police LEO (1) law enforcement agencies: «Leadership», «Civilian Unit», «Training Unit», (2) government officials, (3) volunteers), Financial Action Task Force (FATF), Eurojust (Eurojust is a European agency that cooperates with judicial and police authorities of EU Member States). The existence of these structures is the international community's response to the illegal activities of organized groups specializing in fraud committed via the Internet. The study has established that most foreign countries do not have special rules regulating liability for fraud committed via the Internet, and accordingly, the approaches to combating such crimes are conditioned by the peculiarities of national legislation. Therefore, in order to find effective models for combating fraud committed using the Internet, foreign experience and structure of their special units, police departments, as well as their functions, which are completely different in nature, have been studied. Thus, in European countries and the United States, the functions of counteraction give way to prevention; in contrast to the named countries, Asian States strictly adhere to strict repressive measures. Based on the processed and generalized modern foreign best practices, the author develops scientifically sound recommendations for law enforcement agencies to counteract fraud committed via the Internet have been developed.

Key words: cyber police, special units, counteraction, investigation, interaction, fraud, Internet, foreign experience.

Постановка проблеми. З поширенням інтернету, розвитком інформаційних технологій та запровадженням процесів діджиталізації у всі сфери життя та суспільства загалом з'являються нові можливості для отримання прибутку. Проте поряд із позитивними аспектами впровадження мережі «Інтернет» і стрімкого розвитку цифрових технологій міжнародна спільнота зіткнулася зі збільшенням кількості кіберзлочинів. За оцінками міжнародних експертів, щорічно за останні п'ять років майже 60 % усіх вчинених кіберзлочинів були інтернет-шахрайствами, від яких глобальні фінансові втрати сягають близько 55 млрд дол. щороку [1].

Наразі шахрайство в інтернеті набуває дедалі більших масштабів. Саме анонімність, відсутність безпосереднього контакту з потерпілим та масовість користувачів привертає значну увагу шахраїв до мережі «Інтернет». Однак види, способи, схеми та методи шахрайства невинно еволюціонують, що значно ускладнює їх виявлення та документування і впливає на організаційно-тактичні аспекти розслідування.

Як справедливо зауважує Л. В. Лефтеров, навіть у розвинених економічно країнах існують серйозні труднощі

з профілактикою та боротьбою зі шахрайствами, що здійснюються за допомогою комп'ютерних технологій. Це підкреслює актуальність цієї проблеми і вимагає більш глибокого дослідження, аналізу, а також розробки та впровадження ефективних професійних рішень, методичних, юридичних та загальносоціальних заходів для запобігання таким видам шахрайства [2, с. 90–91].

Необхідно прискорити процес впровадження та адаптації міжнародних норм і стандартів до законодавчої системи України в інформаційній сфері. Ключовим є активний обмін даними між правоохоронними органами різних країн щодо кібершахрайств, що вже скоєні або знаходяться на стадії підготовки. Найбільш ефективним способом боротьби з будь-яким видом злочину є його недопущення, запобігання, а також виявлення причин і умов, які сприяють його скоєнню, з подальшим їх обмеженням, нейтралізацією і усуненням, а вже після цього – розслідування та розкриття [3, с. 189; 4, с. 294].

Таким чином, вивчення іноземного досвіду протидії спеціальними підрозділами поліції шахрайству, що вчиняється з використанням мережі «Інтернет», є неможливим без комплексного аналізу нормативно-правових актів

та правозастосовної практики правоохоронних органів різних держав, що зумовило **актуальність вибраної теми**.

Аналіз останніх досліджень і публікацій. Окремі засади зарубіжного досвіду протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет» досліджували такі вчені, як: Ю.В. Гаруст, М.В. Гуцалюк, Д.В. Долбнева, М.В. Дубина, В.Б. Коба, О.І. Кривенко, І.П. Лежненко, С.І. Лепський, Л.В. Лефтеров, С.Ю. Лівчук, М.І. Малій, В.І. Мельник, С.О. Павленко, Н.В. Павлова, О.М. Петровський, Ю.М. Піщик, А.В. Рейнгольд, І.В. Садчикова, В.Г. Севрук, І.О. Середюк, О.С. Тарасенко, І.М. Чайка, С.В. Шапочка тощо.

Мета статті полягає у аналізі європейського досвіду щодо протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет».

Виклад основного матеріалу дослідження. Вивчаючи іноземний досвід і здійснюючи конструктивний аналіз підходів різних держав до питання протидії злочинам, що вчиняються організованими групами і злочинними організаціями, варто констатувати, що у світі за останні десятиліття змінилися підходи, які визначали природу і сутність цього явища, а також концепція правоохоронних органів щодо протидії організованим злочинності [5].

Щодо Європейського відділу з боротьби з шахрайством (OLAF), то його ключовими завданнями є: розслідування випадків шахрайства, корупції та інших незаконних дій; виявлення та розслідування серйозних порушень з боку працівників ЄС, що пов'язані з шахрайськими діями; надання підтримки Європейській комісії у розробці та впровадженні політики, спрямованої на попередження та виявлення шахрайства [6; 7, с. 209].

У відповідь на зростання кіберзлочинності Europol заснував у 2013 році Європейський центр кіберзлочинності (EC3) з метою посилення реакції правоохоронних органів на кіберзлочини в ЄС та забезпечення захисту громадян, бізнесу та урядів Європи від онлайн-злочинців [8; 7, с. 209]. Цей центр має повноваження вирішувати питання кіберзлочинності, зокрема ті, що пов'язані з організованими групами, які займаються злочинною діяльністю з метою отримання великих доходів, таких як онлайн-шахрайство; завдають значної шкоди жертвам, наприклад, у випадках сексуальної експлуатації дітей в інтернеті; а також впливають на критичну інфраструктуру та інформаційні системи Європейського Союзу [8; 7, с. 209].

У 2015 році з метою оптимізації діяльності Європейського центру кіберзлочинності була створена Робоча група Європейського Союзу з боротьби з інтернет-шахрайствами. Ця група готує звіт щодо «повернення грошей», що передбачає можливість для споживачів отримати компенсацію від компанії, яка видає кредитні картки, якщо придбаний товар не був доставлений. Незалежно від умов договору з емітентом картки або національних законодавчих норм, споживачі повинні насамперед звертатися до постачальника кредитних карт для отримання відшкодування [6; 7, с. 210].

М. І. Малій, здійснюючи аналіз іноземного досвіду протидії спеціальними підрозділами поліції шахрайству, що вчиняється через мережу «Інтернет» відзначає, що для виявлення і затримання комп'ютерних злочинців, а також з метою запобігання кіберзлочинності в інтернет-просторі створено спеціальний орган – інтернет-поліцію. Слід зазначити, що інтернет-поліція – це повноправна силова структура, яка забезпечує кібербезпеку мережі «Інтернет» від зловмисних дій комп'ютерних злочинців та здійснює заходи з боротьби з інтернет-злочинністю. Загалом інтернет-поліція складається з силових структур, урядовців та волонтерів понад 70 країн світу. Тісна співпраця інтернет-поліції та урядових структур повною мірою

сприяє виявленню і затриманню комп'ютерних злочинців, причому місце знаходження такого зловмисника або підозрюваного значення не має, оскільки віртуальний світ існує без кордонів [9, с. 123]. Інтернет-поліція структурно складається з трьох основних підрозділів. Підрозділ LEO (силові структури) об'єднує представництва інтернет-поліції всіх країн-членів віртуального світу. Цивільний підрозділ об'єднує всі волонтерські формування країн-членів віртуального світу. Підготовчий підрозділ забезпечує навчання новачків-кіберполіцейських. Керівництво цим підрозділом покладено на LEO [9, с. 123].

Інтернет-поліція займається виявленням комп'ютерних злочинців та запобіганням інтернет-злочинності. Спеціально підготовлені офіцери інтернет-поліції володіють сучасними технологіями виявлення та затримання хакерів і крєкерів, які зловмисляють у віртуальному інтернет-просторі. База даних інтернет-поліції містить інформацію про всі кіберінциденти і вчинені інтернет-злочини, починаючи з 1986 року. Це значною мірою сприяє швидкому виявленню зловмисних дій комп'ютерних злочинців, встановленню й аналізу нових видів інтернет-злочинів та поліпшенню оперативності прийняття запобіжних дій з дійснюваних інтернет-поліцейськими [10, с. 36–37; 9, с. 124].

Усталеною практикою реагування на випадки шахрайства у міжнародних організаціях є залучення зовнішніх форензик-експертів для аналізу та розслідування таких випадків, а також розробки практичних рішень, що сприяють запобіганню, виявленню і ліквідації наслідків шахрайства. В Україні ж лише 3 % респондентів за останні два роки мали такий досвід, порівняно з 20 % респондентів у світі. Незважаючи на збільшення витрат на боротьбу з шахрайством, чимало українських організацій усе ще не займаються профілактикою шахрайства, а лише реагують або захищаються, коли факт шахрайства вже скоєний [11; 12, с. 174–175]. В економічно розвинених країнах значну популярність здобули послуги з «фінансових розслідувань», що активно розвиваються в консалтингових та аудиторських компаніях. Для цього були створені спеціалізовані підрозділи, відомі як групи «форензик» (forensic), які займаються фінансовими розслідуваннями в таких напрямках: судовий облік (forensic accounting), аудит шахрайств (fraud audit) та управління ризиками в контексті шахрайства (fraud risk management), пошук і відновлення активів (asset tracking and recovery), а також виявлення і запобігання відмиванню грошей (money laundering detection and prevention) [13, с. 193; 14, с. 73].

Послуги «форензик» включають перелік робіт, що виконуються на замовлення підприємства, серед яких: врегулювання фінансових і ділових конфліктів між сторонами; виявлення та оцінка прихованих комерційних ризиків; захист інтелектуальної власності; проведення корпоративної розвідки; попередження фінансових та репутаційних втрат; перевірка виконання контрактних зобов'язань і надійності бізнес-партнерів; аналіз звернень по «гарячій лінії»; проведення позасудових та досудових експертиз, а також підтримка під час судових розглядів; реалізація комплаєнс-розслідувань; боротьба з легалізацією незаконних доходів; розробка процедур протидії шахрайству, корупції, виведенню коштів та привласненню активів; розслідування шахрайств із використанням інформаційних технологій; управління шахрайськими ризиками; проведення фінансових експертиз документів [15, с. 26; 14, с. 73].

Здебільшого користувачі службових, приватних пристроїв під час налаштування мережі «Інтернет» використовують стандартні паролі. Як наслідок, бразильська арена кіберзлочинності є лідером у сфері інтернет-зловживань. Бразилія посідає друге місце за кількістю шахрайств онлайн-банкінгу та фінансових інтернет-шахрайств [16]. Зазвичай кіберзлочинці використовують такі засоби для

вчинення злочину як троян, фішинг на основі зображення або фальшивого браузера, велику кількість векторів атак тощо. Зі свого боку, користувачі глобальної мережі не видаляють незрозумілі електронні листи, підключаються до незахищених загальнодоступних бездротових мереж, як наслідок шість із десяти користувачів інтернету стали жертвами кіберзлочинів [17; 18]. Існують також інші державні органи, які займаються розслідуванням злочинів у межах своєї компетенції, хоча це не є їх основним завданням. Ці установи проводять розслідування, коли кримінальні правопорушення виявляються під час виконання їхніх звичних функцій. Наприклад, Екологічне агентство (Ibama) відповідає за розслідування екологічних правопорушень, Служба внутрішніх доходів (Receita Federal) займається розслідуванням злочинів, пов'язаних з ухиленням від податків та фінансовими шахрайствами, Центральний банк (Banco Central do Brasil) розслідує фінансові злочини, Комісія з цінних паперів і бірж Бразилії (Comissão de Valores Mobiliários – CVM) розслідує порушення на ринку цінних паперів, а COAF (Бразильський підрозділ фінансової розвідки) бореться з відмиванням грошей і фінансуванням тероризму [19].

Серед європейських держав, згідно з даними статистики фінансового шахрайства, лідерами є Велика Британія і Франція, що несуть найбільші збитки від шахрайства [20]. Тому досвід цих та інших європейських держав, які стикнулися з проблемами кібершахрайства, зокрема й у сфері е-комерції, та віднайшли ефективні шляхи боротьби із ним, можна взяти за основу [12, с. 172]. Окремо слід зосередити увагу на досвіді Великої Британії щодо протидії спеціальними підрозділами поліції шахрайству, що вчиняється через мережу «Інтернет».

Так, у Великій Британії реєстратори доменних імен веб-сайтів активно працюють над запобіганням шахрайству, ще до того, як сайти починають функціонувати. Вони перевіряють відповідність доменних імен вимогам щодо їх змісту та юридичних прав замовників на використання конкретного імені. Якщо виявляється невідповідність вимогам, реєстрація таких сайтів не здійснюється. Цей підхід спрямований на попередження різних видів шахрайства, таких як ті, що пов'язані з банківською діяльністю чи сплатою податків, і допомагає зменшити кількість шахрайських ресурсів на етапі реєстрації. За допомогою спеціальних алгоритмів здійснюється аналіз спроб реєстрації доменів, що містять певні ключові слова, для їх подальшої оцінки. Уже було призупинено реєстрацію 600 підозрілих веб-сайтів, пов'язаних із темою коронавірусу [21, с. 78–79].

У 2017 році в Англії та Уельсі за законом про комп'ютерні злочини було винесено менше 50 вироків, хоча, за даними Бюро національної статистики Великої Британії, в період з квітня 2017 по березень 2018 року було зафіксовано понад 1,2 мільйона правопорушень [22; 21, с. 83].

Згідно з даними Національного бюро боротьби з шахрайством Великої Британії, можна виділити такі ключові характеристики жертв кіберзлочинності:

- 85 % усіх випадків кіберзлочинів стосуються фізичних осіб, тоді як юридичні особи складають лише 13 %;
- близько 24 % жертв кіберзлочинів визначені як потенційно вразливі, тобто такі, які можуть стати жертвами повторно;
- найбільша кількість жертв – особи у віці від 15 до 49 років;
- чоловіки втрачають через кіберзлочинність утричі більше, ніж жінки;
- найбільші збитки спричинені крадіжкою інтелектуальної власності та конфіденційної комерційної інформації;
- жінки у шість разів частіше стають жертвами шахрайства в інтернет-магазинах порівняно з чоловіками [23; 18].

Франція націлена на забезпечення здатності інформаційних систем протистояти подіям у кіберпросторі, які

можуть негативно вплинути на доступність, цілісність та конфіденційність даних. Країна приділяє особливу увагу технічним засобам захисту інформації, боротьбі з кіберзлочинністю та впровадженню заходів кіберзахисту [24, с. 56; 12, с. 173].

Пункт «а» частини 3 статті 138ab КК Нідерландів передбачає відповідальність за «віртуальне шахрайство». Згідно з цим пунктом «неправомірне проникнення в комп'ютер, вчинене через телекомунікаційну інфраструктуру або телекомунікаційний пристрій, що використовується для обслуговування населення (інтернет) з ціллю набуття незаконних доходів, карається позбавленням волі на строк до чотирьох років або штрафом четвертої категорії». Цікавим є той факт, що цей злочин розташований у Розділі V «Злочини проти громадського порядку» [25; 26, с. 109].

Серед інших підрозділів та відділів Фінансової гвардії Італії варто виділити такі, як GRF (Gruppi Repressioni Frodi) – Групи з боротьби з шахрайством, підрозділ з боротьби з кіберзлочинністю (GAT), а також служби, що відповідають за охорону здоров'я та інші напрями [27, с. 146; 28, с. 247].

Наведемо приклад. З 2019 по 2022 роки злочинна група використовувала зламані дані клієнтів іноземних банків для покупок в онлайн-магазинах. Придбані товари перепродавались, що приносило учасникам прибуток. Спільно з німецькими та литовськими правоохоронними органами, за координації Офісу Генерального прокурора, кіберполіція розкрила 40-річного співорганізатора цієї шахрайської схеми. Він, разом із громадянином Молдови, організував схему викрадення грошей у громадян Євросоюзу, залучивши до неї осіб з ЄС та суміжних країн. Користуючись довірою європейців до онлайн-покупок, шахраї заволоділи викраденими банківськими картками і замовляли товари на великі суми. Оплачуючи покупки картками потерпілих, вони через мережу агентів збували товари у східноєвропейських країнах. Ця транснаціональна злочинна група діяла в ЄС та Україні протягом трьох років, за цей час вони заволоділи понад 600 тис. євро. В рамках кримінального провадження кіберполіція Харківської області, разом із міжнародною слідчо-оперативною групою, провела обшуки у домівці одного з фігурантів, де була вилучена техніка, що використовувалась для шахрайства. Затриманий співорганізатор був арештований польськими прикордонниками на основі ордеру від німецьких правоохоронців під час перетину кордону з Білоруссю. Інший співучасник наразі перебуває під вартою в Німеччині в рамках розслідування [29; 30, с. 103–104].

В Іспанії найбільш поширеними видами шахрайства є фішинг (надсилання підроблених електронних листів, які виглядають як повідомлення від законних компаній, з метою крадіжки особистих даних, зокрема банківських реквізитів і паролів), шахрайство з орендою (реклама неіснуючої нерухомості), шахрайство через онлайн-знайомства та створення фальшивих веб-сайтів. Відповідно до статті 248 Кримінального кодексу Іспанії шахрайство вчиняють ті, хто обманом отримує матеріальні вигоди, вводячи іншу особу в оману, щоб змусити її здійснити розпоряджувальні дії, що завдають шкоди їй або іншому. Частина 2 цієї статті встановлює окремі форми шахрайства, зокрема через використання комп'ютерних маніпуляцій або подібних схем, а також через створення, завантаження, володіння чи надання програмного забезпечення, призначеного для шахрайства, або використання кредитних та дебетових карток, дорожніх чеків чи будь-яких даних, що містяться в них [31; 32, с. 80].

Варто відзначити досвід Естонії, де реалізується проєкт «Інтернет-констеблі». Його головною метою є створення віртуальних поліцейських осередків на найбільш відвідуваних веб-платформах, популярних серед молоді. Поліція організувала власні акаунти та електронні адреси в інтер-

нет-просторі, що активно використовується молоддю. За цими акаунтами стоять реальні офіцери поліції, що дозволяє кожному користувачеві мережі знати, з ким саме він спілкується віртуально [33]. Такий підхід має суттєвий психологічний запобіжник для осіб, що ставали свідками кримінального правопорушення, або потерпілими від шахрайських дій. Для громадян є дуже важливим усвідомлення уособлення звернення до поліції. Тим паче – можливість звернутись через найбільш популярні веб-портали значно полегшує процес комунікації громадян з поліцією. Слід зазначити, що подібні проекти запроваджені й у інших країнах Європи, Північної Америки та інших континентів [32, с. 88]. Враховуючи зазначене, результати опитування показали, що 96 % респондентів підтримують досвід Естонії у протидії шахрайству в мережі «Інтернет», який базується на запобіжній діяльності та моніторингу веб-порталів поліцейськими «інтернет-констеблями».

Отже, різницею в підходах до боротьби з шахрайством, яке здійснюється через інтернет, між вітчизняною практикою та практиками Європейського Союзу і США є те, що в зазначених іноземних країнах значну увагу приділяють превенції таких злочинів і роботі з населенням, а не лише розслідуванню вже скоєних правопорушень [7, с. 201–211].

Отже, використання ефективного зарубіжного досвіду правоохоронні органи повинні застосовувати лише в контексті існуючої системи права, з огляду на певні правові принципи, традиції, правову культуру та правосвідомість громадян [34; 35].

Висновок. Проведеним дослідженням встановлено, що більшість іноземних країн не містять спеціальних норм, які регламентують відповідальність за шахрайство, що вчиняється з використанням мережі «Інтернет», відповідно підходи до протидії таким злочинам обумовлені особливостями національного законодавства. Отже, для пошуку ефективних моделей протидії шахрайству, що вчиняється з використанням мережі «Інтернет», було вивчено іноземний досвід та структуру їх спеціальних підрозділів, поліцейських відомств, а також їх функції, що абсолютно різняться за своєю сутністю. Так, у європейських країнах та США функції протидії поступаються місцем запобіганню, на відміну від вищевказаних країн та США, азійські держави суворо дотримуються жорстких репресивних заходів. На основі опрацьованого та узагальненого сучасного передового іноземного досвіду розроблено науково обґрунтовані рекомендації щодо протидії правоохоронними органами шахрайству, що вчиняється з використанням мережі «Інтернет».

ЛІТЕРАТУРА

1. Шахрайство в Інтернеті. URL: <https://kidslox.com/ua/guide-to/online-scams/>.
2. Лефтеров Л. В. Загальносоціальні заходи запобігання шахрайству, що вчиняється шляхом використання засобів електронних комунікацій. LEX PORTUS. № 1 (15). 2019. С. 89–101. DOI 10.26886/2524-101X.1.2019.6.
3. Шапочка С.В. До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет. Інформаційна безпека та кібершахрайство: матеріали Міжн. наук.-практ. конф. Внутрішні та зовнішні загрози національній безпеці держави, (Київ, 2 квітня 2013 р.), НАВС. Київ: ТОВ «Три К», 2013. С. 188–191.
4. Павлова Н. В. Основні профілактичні заходи при розслідуванні кримінальних правопорушень, вчинених шляхом шахрайства. Вісник ЛДУВС ім. Е.О. Дідоренка. 2023. Вип.1(101). С. 288–298. DOI:10.33766/2524-0323.101.288-298.
5. Севрук В. Г. Протидія злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі: теорія та практика: монографія. Київ: «Видавництво Людмила», 2022. 1092 с.
6. Phenomenon of Economic Criminality and the Legal Tools for its Elimination. URL: <https://lawconference.sk/bpf/sprava/files/zborniky/9.sekcia.pdf>.
7. Кривенко О. І. Міжнародний досвід протидії шахрайствам, що вчиняються через мережу Інтернет (на прикладі Європейського Союзу та Сполучених Штатів Америки). Форум права: електрон. наук. фахове вид. 2017. № 5. С. 208–212. URL: http://nbuv.gov.ua/jpdf/FP_index.htm_2017_5_32.pdf DOI: <http://doi.org/10.5281/zenodo.1202450>.
8. Fraud in cross-border e-commerce. URL: <http://ecc-croatia.hr/resources/files/Fraud%20in%20crossborder%20e-commerce.pdf>.
9. Малій М.І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження. Дисертація на здобуття освітньо-наукового ступеня доктора філософії за спеціальністю 081 Право. Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2022. 224 с.
10. Косік Ю. «Інтернет»-поліція – ваш захисник. Столична міліція. 2004. № 7. С. 36–37.
11. Економічні злочини та шахрайство: досвід українських організацій. URL: <https://www.epravda.com.ua/columns/2020/12/17/669308/>.
12. Коба В. Б. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції. Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. – Дніпропетровський державний університет внутрішніх справ, Дніпро, 2024. 266 с.
13. Лепський С. І. Зарубіжний досвід використання фінансових розслідувань у правоохоронній діяльності. *Право і суспільство*. 2014. № 2. С. 189–194.
14. Олійничук О., Купер М. Міжнародний досвід використання економічної експертизи у фінансових розслідуваннях. Актуальні проблеми правознавства. 2020. №3 (23). С. 69–75.
15. Долбнева Д. В. Шляхи трансформації системи боротьби з економічними злочинами в Україні з урахуванням досвіду країн Європейського Союзу. ScienceRise. 2019. № 2–3. С. 21–27.
16. Going for Gold: Cybercrime and the Brazilian Threat Landscape. July 21, 2016. URL: <https://securityintelligence.com/going-for-gold-cybercrime-and-the-brazilian-threat-landscape/>.
17. Teixeira M. Largest Cybercrime Threats in Brazil. Published. 8 Apr. 2015. URL: <https://techinbrazil.com/largest-cybercrime-threats-in-brazil>.
18. Тарасенко О. С. Теорія та практика протидії кримінальним правопорушенням, пов'язаним з обігом протиправного контенту в мережі Інтернет: монографія. Одеса: Видавничий дім «Гельветика», 2021. 426 с.
19. Andrey Borges de Mendonça. The Criminal Justice System in Brazil: a brief account. 2014. P. 65. URL: <https://independent.academia.edu/borgesandrey>; Косторниченко М., Циліорик І. Кримінальний процес Бразилії. *Право і суспільство*. 2020. № 2. Ч. 3. С. 115. DOI: 10.32842/2078-3736/2020.2-3.18.
20. Дубина М. В., Садчикова І. В., Середюк І. О. Концептуальні підходи до підвищення рівня безпечності банківського платіжного середовища України. URL: https://www.business-inform.net/export_pdf/business-inform-2020-3_0-pages-349_359.pdf.
21. Гуцалюк М.В. Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю. *Інформація і право*. 2020. № 3(34). С. 75–87.
22. Crime in England and Wales: year ending March 2018, United Kingdom Office for National Statistics (19 July 2018). URL: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018>.
23. Cyber Crime – Victimology Analysis : February 2016 / National Fraud Intelligence Bureau. City of London Police – National Policing Lead For Fraud. 2010. P. 3. URL: <https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf>.
24. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Молодий вчений*. 2019. № 12/1. С. 55–59.

25. Кримінальний кодекс Нідерландів. URL: <http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum>.
26. Піцик Ю. М. Міжнародний досвід у сфері протидії злочинам проти власності, що вчиняються у кіберпросторі. *Прикарпатський юридичний вісник*. 2016. Випуск 4(13). С. 107-111.
27. Лежненко І. П. Організаційно-правові засади функціонування Фінансової гвардії Італії (La Guardia di Finanza). Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика), 2018. Вип. 1-2. С. 142-148.
28. Гаруст Ю. В., Мельник В. І. Правоохоронні органи на захисті економічної безпеки України: адміністративно-правовий аспект: монографія. Суми: Мрія, 2019. 256 с.
29. Харківські кіберполіцейські спільно з правоохоронцями Німеччини викрили одного з організаторів транснаціональної шахрайської групи: збитки понад 600 тис євро. URL: <https://cyberpolice.gov.ua/>.
30. Рейнгольд А. В. Розслідування шахрайства в інтернет-комерції. Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. Дніпропетровський державний університет внутрішніх справ, Дніпро, 2023. 250 с.
31. Organic Act 10/1995, dated 23rd November, on the Criminal Code. URL: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documentos/Criminal_Code_2016.pdf.
32. Чайка І.М. Кримінологічна характеристика та запобігання шахрайству в Україні. Дисертація на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 – Право. – Донецький державний університет внутрішніх справ Міністерства внутрішніх справ України, Кропивницький. – 2023. 296 с.
33. Enhus E., Ponsaers P., Verhage A. Поліцейська діяльність, орієнтована на громаду, в Європі: концепції, теорія та практика (переклад українською мовою Сизенко С.). URL: https://pravo.org.ua/img/.../14586534582015_community_oriented_policing_in_europe.pdf.
34. Павленко С. О. Зарубіжний досвід у сфері протидії політичній корупції. Стан, проблеми та перспективи сучасної юриспруденції України в умовах євроінтеграції: правові та суспільні аспекти : матеріали підсумк. наук.-теорет. Інтернет-конф. (Київ, 23 квіт. 2015 р.). Київ : Нац. акад. внутр. справ, 2015. С. 138-139.
35. Тарасенко О.С. Окремі засади адміністративно-правового регулювання суб'єктів державного фінансового моніторингу: зарубіжний досвід. *Юридичний науковий електронний журнал*. № 2. 2023. С. 575-579.