DOI: 10.33270/05257004.2
УДК 343.13 (477)

ТАРАСЕНКО Олег
доктор юридичних наук, професор, проректор Національної академії внутрішніх справ
м. Київ, Україна
ORCID: https://orcid.org/0000-0002-3179-0143;
СТРІЛЬЦІВ Олександр*
кандидат юридичних наук, старший науковий співробітник, уповноважений з антикорупційної діяльності Національної академії внутрішніх справ
м. Київ, Україна
ORCID: https://orcid.org/0000-0002-8324-3053

Напрями вдосконалення законодавства, що регулює оперативно-розшукову діяльність, з метою протидії кримінальним правопорушенням в інформаційному просторі

Анотація. У статті акцентовано на проблемах нормативно-правової регламентації в Законі України «Про оперативно-розшукову діяльність» можливостей оперативних підрозділів правоохоронних органів здійснювати оперативно-розшукові заходи в інформаційному просторі. Зазначена необхідність зумовлена тим, що протягом останнього десятиліття злочинці дедалі активніше застосовують сучасні інформаційні технології для вчинення кримінальних правопорушень, постійно вдосконалюють способи їх вчинення з використанням мережі Інтернет, хмарних сервісів, криптовалюти, штучного інтелекту, deepfake тощо. Встановлено, що в прийнятому 1992 року Законі України «Про оперативно-розшукову діяльність» бракує системної інтеграції з національним кіберзаконодавством, зокрема із законами України «Про основні засади забезпечення кібербезпеки», «Про електронні комунікації», «Про санкції», «Про захист інформації в інформаційно-телекомунікаційних системах». Визначено недоліки Закону України «Про оперативно-розшукову діяльність», серед яких – обмеженість прав і повноважень оперативних підрозділів діяти в межах закону в інформаційному просторі для ефективного здійснення пошукової діяльності; здійснювати фіксацію фактичних даних про протиправну діяльність окремих осіб і груп, які використовують сучасні інформаційні технології з протиправною метою, а саме збирати, зберігати та використовувати електронні (цифрові) докази; застосовувати спеціальні процедури для доступу правоохоронних органів до даних, що зберігають за кордоном (сервери Google, Meta тощо); створювати й використовувати для реалізації завдань оперативно-розшукової діяльності анонімні акаунти, облікові записи, інтернет-сторінки, вебресурси тощо, а також захисту конституційних прав громадян від протиправного втручання правоохоронних органів у приватність фізичних і юридичних осіб в інформаційно-комунікаційних мережах. Запропоновано внести зміни й доповнення до Закону України «Про оперативно-розшукову діяльність», норми якого спрямовані на захист приватності в інформаційно-комунікаційних мережах, визначення напрямів діяльності оперативних підрозділів у сфері електронних комунікацій, запровадження нового методу негласного виявлення та запобігання кримінальним правопорушенням «комп'ютерне втручання», забезпечення отримання та використання електронних (цифрових) доказів під час проведення оперативно-розшукової діяльності, взаємодію з іноземними провайдерами або компетентними органами іноземних держав.

Ключові слова: комп'ютерне втручання; електронні (цифрові) докази; оперативно-розшукова діяльність; кіберзлочинність; приватність; оперативний підрозділ; інформаційний простір.

Історія статті:
Отримано: 04.08.2025
Переглянуто: 05.09.2025
Прийнято: 07.10.2025

Рекомендоване посилання:
Тарасенко О., Стрільців О. Напрями вдосконалення законодавства, що регулює оперативно-розшукову діяльність, з метою протидії кримінальним правопорушенням в інформаційному просторі. *Наука і правоохорона.* 2025. Вип. 4 (70). С. 17–23. DOI: 10.33270/05257004.2

*Відповідальний автор

Вступ

Сучасні інформаційні досягнення людства (можливостей мережі Інтернет, штучного інтелекту, банкінгу) активно бере на озброєння криміналітет з метою полегшення вчинення кримінальних правопорушень, зокрема перенесення протиправної діяльності у віртуальний інформаційний простір. Системними стали хакерські атаки на сайти органів державної влади, об'єкти критичної інфраструктури, «відмивання» коштів за допомогою криптовалюти, розповсюдження предметів, вилучених з обігу (наркотики, зброя, ядерні матеріали тощо) з використанням можливостей мережі Інтернет тощо. Протиправне застосування інформаційних технологій протягом останнього десятиліття фактично змінило кримінальну сцену, удосконалило способи вчинення та приховування кримінальних правопорушень (Shevchuk, 2024; Stepanenko, & Piddubnyi, 2024).

Ситуація обтяжується також низкою факторів, серед яких слід виокремити такі: більшість інформаційних ресурсів знаходяться поза межами нашої держави, що обмежує можливість фізичного доступу до них; до вчинення кримінальних правопорушень залучають членів транснаціональних злочинних угруповань, а також органи влади країни-агресора, які мають потужний фінансовий, організаційній, кадровий і технічний потенціал; неналежна взаємодія з правоохоронними органами країн – членів ЄС, США, Великої Британії тощо; недосконаліть нормативно-правової бази для протидії сучасним викликам кримінального світу тощо.

Зазначене спонукає правоохоронні органи України до активних дій з розроблення нових асиметричних методів і заходів з протидії зазначеним й іншим небезпечним викликам, а також їх нормативно-правове регулювання і подальше вдосконалення тактики застосування.

З огляду на основні завдання правоохоронних органів нашої держави, що спрямовані на запобігання протиправним викликам криміналітету у віртуальному інформаційному просторі, а в разі вчинення кримінального правопорушення з використанням мережі Інтернет – забезпечення своєчасного й ефективного встановлення причетних до його вчинення осіб, реалізацію зазначених заходів покладено на спеціалізовані підрозділи протидії кіберзлочинності та кримінальної аналітики правоохоронних органів. Отже, постала потреба розроблення законодавчих ініціатив, спрямованих на забезпечення можливостей діяльності таких спеціалізованих підрозділів не лише здійснювати ефективні пошукові заходи, а й проводити активні втручання з метою припинення протиправної діяльності злочинних угруповань в інформаційному просторі з використанням сучасних засобів оперативно-розшукової діяльності, що спонукає до здійснення відповідних досліджень та зумовлює актуальність цієї статті.

Метою публікації є дослідження правових аспектів діяльності оперативних підрозділів правоохоронних органів в інформаційному просторі щодо запобігання та протидії кримінальним правопорушенням для формування нових законодавчих підходів, які надавали б можливість ефективно в правовому полі діяти з метою запобігання та протидії кримінальним правопорушенням, які вчиняють у цій сфері.

Матеріали та методи

Аналіз наукових публікацій з дослідження проблематики законодавчого забезпечення здійснення оперативно-розшукової діяльності в інформаційному просторі засвідчує, що в наукових колах цю тему вивчало чимало дослідників. Серед них слід виокремити наукові погляди таких учених, як В. Г. Хахановський, М. В. Гуцалюк (2019), Р. В. Білоус, В. І. Василинчук, О. В. Таран (2021), О. Ухно (2021), Н. М. Ахтирська, О. Ю. Костюченко (2022), М. К. Гнєтнєв, О. М. Махлай (2022), О. П. Метелев (2022), С. Матуєлене, В. Шевчук, Ю. Балтрунене (2023), Г. К. Авдеєєва (2023), В. М. Бабакін, Ю. Д. Борисенко (2024), В. С. Боднар, В. Ю. Парфьонов (2024), О. О. Козленко (2024), М. А. Погорецький (2025) та ін.

Водночас більшість наукових публікацій стосувалися напрямів протидії злочинам в інформаційному просторі без розроблення пропозицій до чинного законодавства щодо нормативного забезпечення такої діяльності в оперативно-розшуковій сфері. Унаслідок цього майже немає пропозицій до Закону України «Про оперативно-розшукову діяльність»[1] щодо нормативного закріплення регламентації здійснення пошукової діяльності в інформаційному просторі та фіксації фактичних даних про протиправну діяльність окремих осіб і груп, які вчиняють протиправну діяльність з використанням мережі Інтернет, хмарних сервісів, криптовалюти, штучного інтелекту, deepfake, атак на критичні ІТ-сервіси, поширення шкідливих програмних продуктів тощо, що вкотре засвідчує актуальність цієї статті.

Результати й обговорення

Більшість інформаційних ресурсів, які використовують злочинці з протиправною метою, знаходяться поза межами нашої держави, що обмежує можливість фізичного доступу до них, блокування, вилучення, а також встановлення осіб, які причетні до їх використання, і це зумовлює необхідність проведення дистанційних оперативно-розшукових заходів щодо таких ресурсів. Оперативні підрозділи використовують у своїй діяльності Закон України «Про оперативно-

[1] Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. URL: http://zakon2.rada.gov.ua/laws/show/2135-12

розшукову діяльність», у якому, зокрема, визначено права для здійснення заходів з метою запобігання та виявлення кримінальних правопорушень, зокрема в інформаційному просторі. Водночас необхідно зауважити, що цей Закон було ухвалено ще 1992 року й наявні після цього зміни та доповнення до нього не враховують сучасних інформаційних технологій, зокрема можливості протиправного використання мережі Інтернет, наявність хмарних сервісів, використання криптовалюти, штучного інтелекту, deepfake, атак на критичні ІТ-сервіси, поширення шкідливих програмних продуктів тощо. Йому бракує системної інтеграції з національним кіберзаконодавством, зокрема із законами України «Про основні засади забезпечення кібербезпеки»[1], «Про електронні комунікації»[2], «Про санкції»[3], «Про захист інформації в інформаційно-телекомунікаційних системах»[4] тощо.

Якщо врахувати положення ст. 25 Закону України «Про Національну поліцію»[5], згідно з якими до повноважень поліції у сфері інформаційно-аналітичного забезпечення віднесено можливість здійснення інформаційно-пошукової та інформаційно-аналітичної роботи, доходимо висновку, що це стосується передусім спостереження, а не активної оперативно-розшукової діяльності.

Наявні положення Закону України «Про оперативно-розшукову діяльність» засвідчують, що підрозділи, які здійснюють оперативно-розшукову діяльність, наділені обмеженими правами для ефективного здійснення пошукової діяльності в інформаційному просторі та фіксації фактичних даних про протиправну діяльність окремих осіб і груп. Зокрема, до таких прав можна віднести лише можливість: негласно виявляти та фіксувати сліди тяжкого або особливо тяжкого злочину, документи й інші предмети, що можуть бути доказами підготовки або вчинення такого злочину, зокрема шляхом проникнення та обстеження публічно недоступних місць, житла чи іншого володіння особи відповідно до положень ст. 267 Кримінального процесуального кодексу України, а також здійснювати аудіо-, відеоконтроль особи, зняття інформації з електронних комунікаційних мереж, електронних інформаційних мереж згідно з положеннями ст. 260, 263–265 Кримінального процесуального кодексу України, що не відповідає сучасним викликам.

Водночас положення Закону України «Про оперативно-розшукову діяльність» не визначають порядок збору, збереження та використання електронних (цифрових) доказів під час здійснення оперативно-розшукової діяльності, попри те, що такі докази в умовах сьогодення є основними під час розслідування злочинів, які вчиняють з використанням інформаційних технологій. Цей Закон не передбачає спеціальні процедури для доступу правоохоронних органів до даних, які зберігають за кордоном (сервери Google, Meta тощо). Також не регламентовано порядок на законних підставах створення та використання оперативними підрозділами анонімних акаунтів, облікових записів, інтернет-сторінок, вебресурсів тощо, які не дають змоги встановити їх належність, а також належність їх користувачів до правоохоронного органу. Зазначене надало б можливість:

– здійснювати кримінальну розвідку з метою виявлення в інформаційному просторі осіб, які мають намір вчинити кримінальні правопорушення;

– виявляти та встановлювати облікові записи, інтернет-сторінки, які планують використовувати для вчинення кримінальних правопорушень в інформаційному просторі;

– забезпечувати негласний контроль за користувачами облікових записів, інтернет-сторінок, щодо яких є інформація про намір вчинити кримінальні правопорушення, з метою своєчасного виявлення та припинення їхніх злочинних намірів або викриття у вчиненні кримінального правопорушення;

– на постійній основі здійснювати аналіз облікових записів, інтернет-сторінок, користувачі яких виявили намір вчинити кримінальні правопорушення, з метою своєчасного виявлення та припинення їх злочинних намірів або викриття у вчиненні кримінальних правопорушень;

– проведення профілактичних заходів щодо осіб, які мають намір або вже вчиняють кримінальне правопорушення в інформаційному просторі;

– блокувати протиправний контент, який розповсюджують через мережу Інтернет;

– здійснювати в інформаційному просторі заходи, спрямовані на виявлення та припинення кримінальних правопорушень, зокрема шляхом безпосереднього втручання в діяльність комп'ютерних й інформаційних систем (Tarasenko, 2021).

Проте основним недоліком Закону України «Про оперативно-розшукову діяльність» є брак такого заходу, як комп'ютерне втручання, використання якого дасть змогу здійснювати оперативним підрозділам негласного виявлення протиправного контенту, встановлення осіб, які

[1] Про основні засади забезпечення кібербезпеки : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

[2] Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

[3] Про санкції : Закон України від 14 серп. 2014 р. № 1644-VII. URL: https://zakon.rada.gov.ua/laws/show/1644-18#Text

[4] Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

[5] Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

мають відношення до нього, здійснювати заходи із запобігання вчиненню кримінальних правопорушень, зокрема з припинення поширення та блокування забороненого й обмеженого до обігу контенту, а також фіксації електронних (цифрових) слідів в інформаційному просторі в разі вчинення кримінального правопорушення.

Проте найважливішим результатом упровадження комп'ютерного втручання оперативними підрозділами є можливість здійснювати безпосереднє втручання в діяльність комп'ютерних систем й інформаційних мереж з метою прихованої фіксації відомостей, припинення кримінального правопорушення, зокрема шляхом знищення інформаційних ресурсів, які використовують з протиправною метою (IT-інфраструктура, віртуальні сервери, файлові сховища, програмні продукти, криптогаманці тощо), а також здійснювати DOC-атаки на інформаційні ресурси злочинних угруповань, поширювати фішингові листи, упроваджувати шкідливі програмні продукти (віруси) в інформаційні системи, знищувати криптогаманці, які використовують з протиправною метою злочинці, або здійснювати їх вилучення, зберігання та подальше блокування до них доступу злочинців з метою припинення кримінального правопорушення, а в разі його вчинення – для подальшого накладання на них арешту та конфіскації.

Такий перелік засобів передбачає надмірне втручання в приватне життя фізичних і юридичних осіб, тому має бути зазначено порядок здійснення комп'ютерного втручання або аналогічних заходів як прокурорського контролю, а в окремих випадках – їх реалізацію на підставі ухвали слідчого судді, чого також немає в Законі України «Про оперативно-розшукову діяльність». Зазначене зумовлює чітке встановлення в законодавстві меж у здійсненні комп'ютерного втручання в приватне життя осіб з боку правоохоронних органів, а також заборони на провокування (підбурювання) особи на вчинення кримінальних правопорушень з метою його подальшого викриття.

У зв'язку з викладеним запропоновано внести зміни й доповнення в Закон України «Про оперативно-розшукову діяльність» такого змісту:

– ч. 2 ст. 6 викласти в такій редакції: «Проведення оперативно-розшукових заходів, що пов'язані з обмеженням конституційних прав громадян на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, а також втручанням у приватність в інформаційно-комунікаційних мережах, допускається лише на підставі ухвали слідчого судді»;

– доповнити ст. 7 новою частиною такого змісту: «Оперативно-розшукові заходи у сфері електронних комунікацій здійснюються з метою перехоплення даних трафіка, доступу до збережених даних у хмарних сервісах і датах-центрах, фіксації та вилучення електронних (цифрових) доказів, блокування та знищення забороненого й обмеженого до обігу контенту»;

– доповнити ч. 1 ст. 8 новим п. 7^2 такого змісту: «7^2) здійснювати комп'ютерне втручання з метою негласного виявлення та запобігання кримінальним правопорушенням, зокрема з припинення поширення та блокування забороненого та обмеженого до обігу контенту, а також фіксувати сліди в разі вчинення кримінального правопорушення.

Комп'ютерне втручання, пов'язане з втручанням у роботу інформаційно-комунікаційних мереж, облікових записів осіб без відома їх власників і користувачів, проводиться на підставі ухвали слідчого судді, постановленої в порядку, передбаченому ст. 246, 248, 249 Кримінального процесуального кодексу України»;

– доповнити новою ст. 8^1 «Отримання та використання цифрових доказів під час проведення оперативно-розшукової діяльності» такого змісту:

«Оперативні підрозділи мають право збирати електронні (цифрові) докази під час здійснення комп'ютерного втручання.

Отримання електронних (цифрових) доказів здійснюють шляхом:

– копіювання або вилучення інформації з електронних інформаційних ресурсів;

– перехоплення електронних комунікацій;

– тимчасового доступу до електронних інформаційних ресурсів;

– запиту до операторів електронних комунікацій, провайдерів, адміністраторів мереж чи дата-центрів;

– взаємодії з іноземними провайдерами або компетентними органами іноземних держав відповідно до міжнародних договорів України.

Отримана інформація повинна бути зафіксована із застосуванням криптографічних методів захисту (хешування, цифровий підпис), що забезпечує незмінність і цілісність даних.

Електронні (цифрові) докази, здобуті оперативними підрозділами з порушенням встановленого порядку, не можуть бути використані як докази в кримінальному провадженні.

Електронні (цифрові) докази, отримані в межах оперативно-розшукової діяльності, можуть бути використані в кримінальному провадженні за умови підтвердження їх цілісності, джерела походження та відповідності вимогам КПК України».

Висновки

Норми Закону України «Про оперативно-розшукову діяльність» не дають оперативним підрозділам можливостей повноцінно використовувати у своїй діяльності права на здійснення активних пошукових заходів з метою виявлення, запобігання кримінальним правопорушенням, які вчиняють в інформаційному просторі.

Запропоновано розв'язання цієї проблеми на законодавчому рівні шляхом внесення відповідних змін і доповнень до Закону України «Про оперативно-розшукову діяльність» нормами, які спрямовані на захист приватності в інформаційно-комунікаційних мережах, визначення напрямів діяльності оперативних підрозділів у сфері електронних комунікацій, запровадження нового методу негласного виявлення та запобігання кримінальним правопорушенням «комп'ютерне втручання», забезпечення отримання та використання електронних (цифрових) доказів під час проведення оперативно-розшукової діяльності, взаємодії з іноземними провайдерами або компетентними органами іноземних держав.

References

[1] Akhtyrska, N.M., & Kostiuchenko, O.Yu. (2022). Procedural and Organizational Aspects of Collecting Electronic Evidence in International Cooperation. *Scientific Bulletin of Uzhhorod National University*, 2(72), 192-198. DOI: 10.24144/2307-3322.2022.72.64

[2] Avdieieva, H.K. (2024). The use of digital information obtained during operational-search activities in solving crimes. *Current issues and prospects for the use of operational-search means in solving crimes under martial law:* materials of the interdepartmental scientific-practical conference (pp. 22-25). Kyiv: National Academy of Internal Affairs. Retrieved from https://dspace.nlu.edu.ua//jspui/handle/123456789/19975

[3] Babakin, V.M., & Borysenko, Yu.D. (2024). Directions of Obtaining Operative and Investigative Information by Operative Officers in Counteraction to Crimes Committed by Youth under Martial Law. *Scientific Bulletin of Uzhhorod National University. Series "Law",* 5(86), 11-16. DOI: 10.24144/2307-3322.2024.86.5.1

[4] Bilous, R.V., Vasylynchuk, V.I., & Taran, O.V. (2021). Use of Criminal Analysis Methods During Operative Proceedings and Pre-Trial Investigation. *Scientific Bulletin of the National Academy of Internal Affairs,* 1(118), 131-136. DOI: 10.33270/01211181.131

[5] Bondar, V.S., & Parfionov, V.Yu. (2024). On the features of the application of new technologies in documenting war crimes. *Prykarpatskyi yuridichnyi visnyk*, 6, 118-123. DOI: 10.32782/pyuv.v6.2024.22

[6] Hnietniev, M.K., & Makhlai, O.M. (2022). Reflections on the prospects for the development of operational-search legislation. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs,* 3, 237-243. DOI: 10.31733/2078-3566-2022-3-237-243

[7] Khakhanovskyi, V.H., & Hutsaliuk, M.V. (2019). Peculiarities of using electronic (digital) evidence in criminal proceedings. *Criminology Bulletin,* 1(31), 13-19. DOI: 10.37025/1992-4437/2019-31-1-13

[8] Kozlenko, O.O. (2024). Rights and obligations of units that carry out operational and investigative activities. *Law and Society,* 5, 707-712. DOI: 10.32842/2078-3736/2024.5.102

[9] Matulienė, S., Shevchuk, V., & Baltrūnienė, J. (2023). *Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. Theory and Practice of Forensic Science and Criminalistics*, 4(29), 12-46. DOI: 10.32353/khrife.4.2022.02

[10] Metelev, O.P. (2022). Problematic aspects of recording information obtained from transport telecommunication networks. *Bulletin of Criminal Procedure,* 3-4, 28-37. DOI: 10.17721/2413-5372.2021.3-4/28-37

[11] Pohoretskyi, M.A. (2025). Digital technologies and evidence in the investigation of crimes against the foundations of national security of Ukraine: procedural problems and European standards. *Analytical and comparative law,* 5(3), 239-255. DOI: 10.24144/2788-6018.2025.05.3.37

[12] Shevchuk, M.O. (2024). Modern Challenges and Threats in the Sphere of State Information Security. *Scientific Bulletin of Uzhhorod National University. Series "Law"*, 85(3), 181-186. DOI: 10.24144/2307-3322.2024.85.3.28

[13] Stepanenko, N.V., & Piddubnyi, D.D. (2024). Modern Problems of Prevention and Counteraction of Crime in the Field of Information Technologies. *Legal Bulletin*, 14, 73-80. DOI: 10.31732/2708-339X-2024-14-A10

[14] Tarasenko, O. (2021). Legal Aspects of Computer Interference. *Knowledge, Education, Law, Management*, 3(39), 2, 208-211. DOI: 10.51647/kelm.2021.3.2.32

[15] Ukhno, O. (2021). Genesis and Issues Latest Technologies and Artificial Intelligence in Criminalistics, Forensic Expert Activity and Pre-Trial Investigation. *Theory and practice of forensic examination and criminalistics,* 25(3), 40-59. DOI: 10.32353/khrife.3.2021.04

Список використаних джерел

[1] Ахтирська Н. М, Костюченко О. Ю. Процесуальні та організаційні аспекти збору електронних доказів у міжнародному співробітництві. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2022. № 2 (72). С. 192–198. DOI: 10.24144/2307-3322.2022.72.64

[2] Авдєєва Г. К. Використання цифрової інформації, отриманої під час проведення оперативно-розшукових заходів, у розкритті злочинів. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану* : матеріали міжвідом. наук.-практ. конф. (Київ, 30 берез. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 22–25. URL: https://dspace.nlu.edu.ua//jspui/handle/123456789/19975

[3] Бабакін В. М., Борисенко Ю. Д. Напрями отримання оперативно-розшукової інформації оперативними працівниками у протидії злочинам, що вчиняються молоддю в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2024. Вип. 86. Т. 5. С. 11–16. DOI: 10.24144/2307-3322.2024.86.5.1

[4] Білоус Р. В., Василинчук В. І., Таран О. В. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. *Науковий вісник Національної академії внутрішніх справ.* 2021. № 1 (118). С. 131–136. DOI: 10.33270/01211181.131

[5] Бондар В. С., Парфьонов В. Ю. Про особливості застосування новітніх технологій у документуванні воєнних злочинів. *Прикарпатський юридичний вісник.* 2024. № 6. С. 118–123. DOI: 10.32782/pyuv.v6.2024.22

[6] Гнєтнєв М. К., Махлай О. М. Роздуми про перспективи розвитку оперативно-розшукового законодавства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 3. С. 237–243. DOI: 10.31733/2078-3566-2022-3-237-243

[7] Хахановський В. Г., Гуцалюк М. В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник*. 2019. № 1 (31). С. 13–19. DOI: 10.37025/1992-4437/2019-31-1-13

[8] Козленко О. О. Права та обов'язки підрозділів, які здійснюють оперативно-розшукову діяльність. *Право і суспільство.* 2024. № 5. С. 707–712. DOI: 10.32842/2078-3736/2024.5.102

[9] Matulienė S., Shevchuk V., Baltrūnienė J. Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. *Theory and Practice of Forensic Science and Criminalistics*. 2023. Vol. 4 (29). P. 12–46. DOI: 10.32353/khrife.4.2022.02

[10] Метелев О. П. Проблемні аспекти фіксації відомостей, отриманих з транспортних телекомунікаційних мереж. *Вісник кримінального судочинства.* 2022. № 3–4. С. 28–37. DOI: 10.17721/2413-5372.2021.3-4/28-37

[11] Погорецький М. А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. *Аналітично-порівняльне правознавство.* 2025. Вип. 5. Ч. 3. С. 239–255. DOI: 10.24144/2788-6018.2025.05.3.37

[12] Шевчук М. О. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2024. Вип. 85. Ч. 3. С. 181–186. DOI: 10.24144/2307-3322.2024.85.3.28

[13] Степаненко Н. В., Піддубний Д. Д. Сучасні проблеми запобігання і протидії злочинності у сфері інформаційних технологій. *Legal Bulletin*. 2024. № 4 (14). С. 73–80. DOI: 10.31732/2708-339X-2024-14-A10

[14] Tarasenko O. Legal aspects of computer interference. *Knowledge, Education, Law, Management.* 2021. No. 3 (39). Vol. 2. P. 208–211. DOI: 10.51647/kelm.2021.3.2.32

[15] Ukhno O. Genesis and Issues Latest Technologies and Artificial Intelligence in Criminalistics, Forensic Expert Activity and Pre-Trial Investigation. *Theory and practice of forensic examination and criminalistics.* 2021. Vol. 25 (3). P. 40–59. DOI: 10.32353/khrife.3.2021.04

TARASENKO Oleh
Doctor of Law, Professor, Vice-Rector of the National Academy of Internal Affairs
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-3179-0143;
STRILTSIV Oleksandr
PhD in Law, Senior Research Fellow, Anti-Corruption Commissioner of the National Academy of Internal Affairs
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-8324-3053

Directions for Improving Legislation Regulating Operational and Investigative Activities in Order to Combat Criminal Offenses in the Information Space

Abstract. The article focuses on the problems of regulatory-legal regulation in the Law of Ukraine «On Operational and Investigative Activities» regarding the capabilities of operational units of law enforcement agencies to carry out operational and investigative measures in the information space. This need is due to the fact that over the past decade, criminals have increasingly used modern information technologies to commit criminal offenses, constantly improving the methods of committing such offenses using the Internet, cloud services, cryptocurrency, artificial intelligence, deepfake, etc. It is indicated that the Law of Ukraine «On Operational and Investigative Activities» adopted in 1992 currently lacks systemic integration with domestic cyber legislation, in particular with the Laws of Ukraine «On the Basic Principles of Ensuring Cybersecurity», «On Electronic Communications», «On Sanctions», «On the Protection of Information in Information and Telecommunications Systems». At the same time, the article points out existing shortcomings of the Law of Ukraine «On Operational and Investigative Activities», namely the limited rights and powers of operational units to: act within lawful frameworks in the information space for the effective conduct of search activities; document factual data on the unlawful activities of individuals and groups that use modern information technologies for illegal purposes, including the collection, storage, and use of electronic (digital) evidence; apply special procedures to enable law enforcement access to data stored abroad (servers of Google, Meta, etc.); create and use anonymous accounts, user profiles, Internet pages, web resources, and similar tools for the purposes of operational-search activity, as well as to ensure the protection of citizens' constitutional rights from unlawful interference by law enforcement agencies with the privacy of individuals and legal entities in information and communication networks. The article proposes introducing amendments and additions to the Law of Ukraine «On Operational and Investigative Activities», the provisions of which are aimed at protecting privacy in information and communication networks, defining the areas of activity for operational units in the field of electronic communications, introducing such a new method of covert detection and prevention of criminal offenses as a «computer interference», ensuring the collection and use of electronic (digital) evidence in the course of operational-search activity, as well as interaction with foreign service providers or competent authorities of foreign states.

Keywords: computer interference; electronic (digital) evidence; operational and investigative activities; cybercrime; privacy; operational unit; information space.