УДК 343.98

Лугіна Наталія Анатоліївна –
к. ю. н., доцент
Державний податковий університет
https://orcid.org/0000-0001-6005-2943

Nataliia A. Luhina –
Candidate of Juridical Sciences, Associate Professor
State Tax University
(31 Universytetska Street, Irpin, 08200, Ukraine)
https://orcid.org/0000-0001-6005-2943

Бак Надія Сергіївна –
здобувач вищої освіти
Державний податковий університет
https://orcid.org/0009-0004-0257-5446

Nadiia S. Bak –
Higher Education Seeker,
State Tax University
(31 Universytetska Street, Irpin, 08200, Ukraine)
https://orcid.org/0009-0004-0257-5446

Бак Софія Сергіївна –
здобувач вищої освіти
Державний податковий університет
https://orcid.org/0009-0000-4582-1441

Sofiia S. Bak –
Higher Education Seeker,
State Tax University
(31 Universytetska Street, Irpin, 08200, Ukraine)
https://orcid.org/0009-0000-4582-1441

Сучасні виклики у розслідуванні кіберзлочинів: кримінально-правові та процесуальні аспекти

У статті досліджено правовий аналіз сучасних тенденцій розвитку кіберзлочинності та визначено основні проблеми, що виникають при її кримінально-правовому переслідуванні. Розглянуто основні типи кіберзлочинів, аспекти виявлення, реєстрації та дослідження цифрових доказів, а також труднощі, пов'язані з ідентифікацією осіб, які їх вчинили. Акцентовано увагу на необхідності удосконалення чинного законодавства у сфері кібербезпеки, узгодження національних правових норм із міжнародними стандартами та підсилення міжнародного співробітництва у протидії кіберзлочинності. Сформульовано практичні рекомендації, спрямованих на підвищення ефективної діяльності правоохоронних органів у виявленні, розслідуванні та запобіганні кримінальних правопорушень, здійсненим з використанням інформаційно-комунікаційних технологій.

Актуальність дослідження кіберзлочинності зумовлена низкою факторів, а саме: кіберзлочини мають транснаціональний характер; кіберзлочинці використовують сучасні технології для приховування своєї ідентичності, шифрування даних, анонімізації онлайн-активності; наслідки кіберзлочинів можуть бути катастрофічними не лише для окремих громадян або підприємств, але й для

держави в цілому, адже ураження інформаційних систем критичної інфраструктури може паралізувати енергетичні, транспортні, фінансові та державні процеси

Дослідження викладене в статті необхідне для формування ефективної системи захисту інформаційних ресурсів, підвищення безпеки суспільства, захисту прав і свобод громадян, а також забезпечення належного рівня правової та технічної підготовки фахівців у сфері кримінального правосуддя та кібербезпеки. Саме тому дослідження кіберзлочинності, дає змогу оцінити наступні кроки правопорушників та запобігти вчиненню новим кіберзлочинам, а також дасть змогу формувати пропозиції щодо вдосконалення законодавства та підготовки методичних рекомендацій для фахівців у даній сфері.

Ключові слова: *кіберзлочини, кіберзлочинність, кібербезпека цифрові докази, міжнародна співпраця, кримінальне провадження.*

N.A. Luhina, N.S. Bak, S.S. Bak Current Challenges in Investigating Cybercrime: Criminal Legal and Procedural Aspects

The article examines legal and procedural issues related to the investigation and prosecution of cybercrimes in the context of intensive digitalization and technological change. It emphasizes that the spread of information and communication technologies has changed the structure of criminal behavior in cyberspace, creating new threats and significantly complicating the work of law enforcement agencies at all stages of criminal proceedings. The study analyzes the main manifestations of cybercrime, including unauthorized interference with information systems, illegal modification or destruction of digital data, technologically mediated fraud, and cyberattacks targeting critical infrastructure, with an emphasis on their cross-border nature, covert nature, and high level of adaptability to technological innovations. Particular attention is paid to procedural difficulties related to the identification, collection, preservation, verification, and legal assessment of digital evidence, in particular with regard to ensuring its reliability, integrity, authenticity, and proper documentation in the chain of custody. The article also addresses the problem of identifying offenders who actively use encryption, anonymization services, decentralized networks, and transnational digital platforms to mask their activities and avoid criminal liability. It justifies the need to update national legislation in the field of cybersecurity, including the revision of criminal procedure rules to take into account technological progress and bring domestic legal regulation into line with international legal instruments and standards. Significant emphasis is placed on the role of international cooperation, operational coordination, and information exchange between competent authorities as integral elements of effective cybercrime prevention. Based on the analysis, the article formulates practical recommendations aimed at strengthening institutional resilience, improving the professional competence of investigators, improving interagency cooperation, and developing preventive legal mechanisms capable of countering new cyber threats in a sustainable and forward-looking manner.

Keywords: *cybercrimes, cybercrime, cybersecurity, digital evidence, international cooperation, criminal proceedings.*

Постановка проблеми. Із розвитком інформаційної та цифрової технологій у всі сфери життя суспільства зростають і загрози, пов'язані з кіберзлочинністю. Кіберзлочини відзначаються швидкістю поширення, відсутністю чітких кордонів у просторі та великою технічною складністю. Це створює складні виклики для правоохоронних органів і, зокрема, для прокуратури, яка має забезпечувати законність та ефективне підтримання кримінального переслідування у таких провадженнях. Особливість кіберзлочинів у тому, що у них цифрові технології виступають, як засіб і об'єкт кримінального правопорушення, що ускладнює їх виявлення, документування та доказування. В Україні, з огляду на активну діджиталізацію усіх сфер, протидія кіберзлочинності набуває стратегічного значення і потребує вдосконалення існуючих правових механізмів та методів прокурорської діяльності.

Метою статті є виявлення ключових проблем щодо притягнення до відповідальності за кіберзлочинність у прокурорській практиці, аналіз чинного законодавства та судової практики та визначення основних напрямів удосконалення прокурорської діяльності для підвищення ефективності кримінального

переслідування у сфері кібербезпеки. Ця стаття має на меті сприяти розумінню складності сучасних викликів та окреслити конструктивні шляхи їх подолання.

Аналіз останніх досліджень і публікацій. Питання розслідування кіберзлочинності привертає увагу багатьох вчених, таких як С.Є. Абламський, В.В. Романюк, В.В. Абламська, О.В. Таран, В.Д. Гавловський, Л. Рибальченко, О. Сумовська, О. Є. Користін, Ю. Р. Кардашевський, Л. Рибаченко, О. Сумовський та ін., які у своїх працях виділяють основні види кіберзлочинів превентивні методи, проблематику зародження та існування таких кримінальних правопорушень.

Виклад основного матеріалу. Кіберзлочинність на сьогодення є однією з головних загроз для національної та міжнародної безпеки. Вона охоплює широкий спектр протиправних дій, здійснюваних із використанням інформаційно-комунікаційних технологій, і характеризується високим рівнем прихованості. Як справедливо зазначають експерти, кіберзлочини стають все більш організованими, використовують складні технічні інструменти, а збитки від них обчислюються мільярдами доларів.

Вона виявляється як у кількісному зростанні, так і у значному ускладненні методів, засобів і мотивації відповідних дій. Зокрема, застосування штучного інтелекту (ШІ), технологій блокчейн, криптовалют і даркнету надає нові виклики для кримінально-правового реагування і ускладнює використання лише традиційних підходів у боротьбі [1]. Як слушно зауважують науковці, «використання блокчейну дасть змогу підвищити надійність та прозорість також, наприклад, у державному управлінні, реалізації права громадян на вибори, земельного обліку та інше (з огляду на технічні особливості неможливості довільних змін даних)» [10, с. 78].

Серед основних видів кіберзлочинності виділяють несанкціонований доступ до комп'ютерних систем, втручання у роботу програмного забезпечення, незаконне копіювання або видалення інформації, комп'ютерне шахрайство, поширення шкідливих програм, кібербулінг, кіберпереслідування, порушення права на приватність, а також кібертероризм і шпигунство. Особливу небезпеку становлять злочини проти критичних інформаційних інфраструктур, таких як атаки на державні реєстри, банківські системи чи мережі енергопостачання [2 с. 295].

Пропонуємо більш детальніше розібратися із видами кіберзлочинів. Рибальченко Л. та Сумовський О. стверджують, що одна із форм, що використовують кіберзлочинці є у фінансових махінаціях, що базуються на шахрайстві з картками та крадіжка банківських даних, які спрямовані на конфіденційну інформацію. Також автори спрямовують увагу на кібертероризм на державні установи чи банки, що має на меті спантеличити суспільство. Для цього зазвичай використовують вірусні системи та шкідливе програмне забезпечення. Прикладом цього може виступати злиття файлу із даними українців, із системи ДіЯ. Такими даними, що відомі суспільству є те що наразі цей файл можна знайти у закритих чатах програми Telegram [2, с. 295].

Наступною проблема у інформаційній системі проявляється у кібербулінгу, що проявляється у залякуванні та шантажі особи. Також можна віднести анонімне переслідування потерпілого, що супроводжується «сталкерством», найчастіше у такі ситуації потрапляють молоді дівчата. Так кіберзлочинці спочатку виманюють інформацію про місце роботи або проживання, що згодом переростає у переслідування.

У сфері кіберзлочинності найбільш поширеною є система ботнетів, суть якої полягає в тому, що у комп'ютерній мережі, у яку входить декілька шкідливих програмних забезпечень, влаштовані боти. Для прикладу можна навести систему продажу квитків Укрзалізниці онлайн. У перші секунди після виставлення квитків системою, перекупи, а зазвичай це боти, купують усі квитки, для особистого заробітку. Хоча керівництво Укрзалізниці запровадило верифікацію у системі, але це не дуже рятує, оскільки шахраї знайшли можливість обходити і таку систему.

Також розповсюдженою є кіберзлочинність із використанням фішингових сайтів та електронної пошти. Одна із систем полягає у тому що від імені microsoft відправляють листи у вигляді rnicrosoft, що просять надати конфіденційну інформацію. Можливо і ви не побачили різницю, однак

різниця полягає, що літеру «m» замінили на «r» та «n». Така необачність може призвести до витоку особистої інформації у злочинних цілях.

Вагоме місце займає даркнет, що включає у себе систему купівлі-продажу закритої інформації та фінансування забороненої діяльності [2, с. 295].

Кримінально-правовий аналіз кіберзлочинів передбачає вивчення об'єкта посягань (інформаційна безпека, власність, права громадян), об'єктивної сторони (дії або бездіяльності з використанням ІТ-технологій), суб'єкта кримінального правопорушення (особи зі спеціальними знаннями) та суб'єктивної сторони (умисел, мотиви, цілі). У законодавстві України ця сфера регулюється розділом XVI Кримінального кодексу України під назвою «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [3].

Однією із ключових проблем у боротьбі з кіберзлочинністю є складність отримання, запису та оцінки цифрових доказів. На відміну від традиційних речових доказів, електронні докази існують у віртуальному середовищі та можуть бути змінені чи знищені, що включає складність їх використання у кримінальному провадженні. Згідно за статтею 5 Законом України «Про електронні документи та електронний документообіг», електронний документ – це документ, в якому інформація записана електронним способом, включаючи обов'язкові дані документа [4].

Для детальнішого дослідження електронних доказів, варто звернути увагу на статтю 99 Кримінального процесуального кодексу України (далі КПК), де зазначено про те, що : документ – це матеріальний об'єкт, спеціально створений з метою зберігання інформації, що містить інформацію, зафіксовану в письмовій формі, звук, зображення, яка може бути використана як доказ факту чи обставини, встановлених під час кримінального провадження (за ч. 1 ст. 99 КПК). Документи, за умови, що вони містять зазначену інформацію, можуть включати фотоматеріали, звукозаписи, відеозаписи та інші носії інформації, включаючи комп'ютерні дані. Оригіналом електронного документа є його відображення, якому надається те саме значення, що й документу за ч. 3 ст. 99 КПК. У цьому випадку дублікат документа – це документ, складений у тому ж порядку, що й його оригінал, а також копії інформації, включаючи комп'ютерні дані, що містяться в інформаційних системах, системах електронного зв'язку, телеінформаційних системах, комп'ютерних системах та їх невід'ємних частинах (за ч. 4 ст. 99 КПК) [5].

З вище сказаного випливає наступне твердження про те, що електронні докази – це інформація в електронній (цифровій) формі, що містить дані про обставини, що стосуються справи, зокрема електронні документи. До них належать: текстові документи, графічні зображення, плани, фотографії, відео- та аудіозаписи, веб-сайти, текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші електронні дані. Ці дані можуть знаходитися на портативних пристроях (картах пам'яті, мобільних телефонах, флешка), серверах, системах резервного копіювання та інших місцях зберігання електронних даних, зокрема в Інтернеті.

У науковій роботі М. І. Пашковський наголошує, що основними критеріями корисності цифрових доказів є їх автентичність, цілісність і допустимість. Важливо дотримуватися принципу «ланцюга зберігання», який забезпечує відстежуваність кожного етапу обробки доказів – від моменту їх виявлення до моменту передачі до суду. Порушення цього ланцюга може призвести до визнання доказів недопустимими [6, с.157-161].

Українська судова практика також стикається з низкою викликів. У своїх постановах Верховний Суд неодноразово наголошував на необхідності ретельного дотримання процесуальних вимог при встановленні електронних доказів, зокрема тих, що стосуються перевірки джерела інформації, достовірності та цілісності записів [7].

Міжнародне співтовариство визнало кіберзлочинність глобальною загрозою, що потребує спільної протидії. Важливим міжнародним документом у цій сфері є Конвенція Ради Європи про кіберзлочинність 2001 р. (Будапештська конвенція), до якої Україна приєдналася у 2005 р. Її положення визначають стандарти криміналізації діянь, процесуальні механізми розслідування (збереження комп'ютерних даних, доступ до

інформації, взаємодія компетентних органів), а також процедури міжнародної правової допомоги [8].

Однією з найбільш складних правових проблем у розслідуванні кіберзлочинів виступає питання юрисдикції. Нерідко місце вчинення кримінального правопорушення, місцезнаходження злочинця, серверів і точка заподіяння шкоди розташовані в різних країнах. Це створює неможливість застосування традиційних принципів територіальної підсудності та вимагає розвитку механізмів міжнародної правової співпраці. Українські слідчі стикаються із затримками у відповідях від іноземних компетентних органів, що збільшує ризик втрати цифрових доказів. Особливу увагу слід приділити захисту персональних даних. Під час збору електронних доказів правоохоронні органи отримують доступ до значного обсягу інформації, включно з даними третіх осіб. Це створює потенційні ризики порушення права на приватність, гарантованого статтею 32 Конституції України та статтею 8 Європейської конвенції з прав людини. Європейський суд з прав людини неодноразово підкреслював, що втручання у приватне життя може бути виправданим лише за умови законності, необхідності та пропорційності досягнутій меті. Це підтверджується, зокрема, рішенням у справі Klass and others v. Germany 1978 рік [9].

Удосконалення правового регулювання у сфері цифрових доказів має поєднувати баланс між інтересами правосуддя та гарантіями прав людини. Це означає, що слідчі (розшукові) дії щодо електронної інформації повинні проводитись лише на підставі ухвал суду, із чітким визначенням обсягу даних, строків їх збереження та кола уповноважених осіб.

У XXI столітті кіберпростір став не лише платформою для розвитку технологій, науки та комунікацій, а й ареною для нових форм злочинності. Кіберзлочинність вийшла за межі традиційної концепції злочинності, ставши глобальною загрозою економічній стабільності, національній безпеці та конфіденційності. Боротьба з нею зараз набуває стратегічного значення, а пошук ефективних заходів протидії стає спільною відповідальністю держав, правоохоронних органів і суспільства.

Так із вище викладеного, ми наголошуємо на тому, що боротьба з кіберзлочинністю повинна починатися, насамперед, із вдосконалення законодавства. Національні стандарти мають чітко відображати сучасні технологічні реалії. Потребує доопрацювання Кримінальний кодекс України, зокрема щодо відповідальності за кримінальні правопорушення, пов'язані з використанням криптовалют, фішингом, розповсюдженням шкідливого програмного забезпечення та атаками на критичну інфраструктуру.

Другим кроком має стати створення системи професійного навчання. Більшість кіберзлочинів залишаються нерозкритими не через відсутність технічних можливостей, а скоріше через брак спеціалістів, які розуміються як на техніці, так і на законі. Спеціалізовані освітні програми в університетах необхідні для підготовки кіберрозслідувачів, прокурорів, суддів, експертів з комп'ютерної криміналістики. Такі фахівці можуть не тільки досліджувати, а й прогнозувати майбутні загрози. Міжнародна співпраця відіграє вирішальну роль. Кіберзлочинність не знає кордонів, і злочинці можуть діяти з будь-якої точки світу. Україна вже приєдналася до Будапештської конвенції про кіберзлочинність (2001), але цього недостатньо. Необхідно поглибити участь у міжнародних ініціативах, створювати спільні оперативні групи, обмінюватися інформацією в режимі реального часу. Тільки злагоджені дії держав дозволять швидко реагувати на транскордонні кіберзагрози.

Ще один важливий аспект - технічне забезпечення правоохоронних органів. Без сучасного програмного забезпечення, аналітичних систем, доступу до баз даних і швидкісних каналів обміну інформацією боротьба з кіберзлочинністю стає символічною. В Україні доцільно створити єдину платформу для реагування на кіберзлочини, об'єднавши державні, приватні та наукові структури. Такі центри ефективно працюють в ЄС і США, забезпечуючи швидкий аналіз загроз і координацію дій у разі масштабних атак. Водночас не можна ігнорувати роль суспільства. Жодна, навіть найсучасніша система захисту не працюватиме, якщо у громадян відсутні елементарні знання кібергігієни. Необхідно формувати цифрову правову культуру, починаючи зі шкільної освіти – навчаючи дітей безпечно користуватися Інтернетом, захищати

свої персональні дані та розпізнавати шахрайство. Відповідальність за кібербезпеку має бути поділена – між державою, бізнесом і кожним користувачем.

Висновок. Узагальнюючи результати дослідження, можемо стверджувати, що ефективне розслідування кіберзлочинів неможливим без системного та обґрунтованого залучення спеціалістів. Особливість розвитку суспільства, та зростання користувачів мережею Інтернет вимагає комплексного підходу від законодавця.

Таким чином, боротьба з кіберзлочинністю - це не одноразова кампанія, а постійний процес адаптації до нових викликів. Ефективність можлива лише тоді, коли поєднуються три складові: законодавча модернізація, технологічна здатність і суспільна свідомість. Україна має всі передумови, щоб стати не лише об'єктом, а й активним суб'єктом глобальної кібербезпеки - за умови, що її правова система встигатиме за темпами цифрової епохи.

Список використаних джерел:

1. Реагування на кіберзагрози у 2025 – Google. blog.colobridge.net. URL: https://blog.colobridge.net/uk/2025/01/cybersecurity-risks-in-2025-ua/.
2. Рибаченко Л., Сумовський О. Кіберзлочинність у сучасному світі. *Взаємодія органів сектору безпеки, оборони та громадськості у сфері протидії кримінальним правопорушенням: матеріали II Всеукраїнського круглого столу*. 2025. С. 295-298.
3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
4. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV: станом на 31 грудня 2023р. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.
5. Кримінальний процесуальний Кодекс України (стаття 99): Кодекс України від 13.04.2012: станом на 01 серпня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.
6. Пашковський М. І. Ланцюг зберігання доказів (Chain of custody) процесуальна форма. *Збірник наукових праць з матеріалами III міжнародної наукової конференції. Інноваційна наука: пошук відповідей на виклики сучасності*. С.157-161.
7. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/.
8. Конвенція про кіберзлочинність. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
9. Конвенція про кіберзлочинність (Будапешт, 23 листопада 2001 року). Офіційний вебсайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/980_093#Text.
10. Лугіна Н.А., Вартовнік А.М. Блокчейн в Україні: проблеми правового регулювання. *Міжнародний науковий журнал «Інтернаука»*. № 8(88), 2 т., 2020. С. 74-78.

References:

1. Reahuvannia na kiberzahrozy u 2025 – Google. blog.colobridge.net. URL: https://blog.colobridge.net/uk/2025/01/cybersecurity-risks-in-2025-ua/.
2. Rybachenko L., Sumovskyi O. Kiberzlochynnist u suchasnomu sviti. *Vzaiemodiia orhaniv sektoru bezpeky, oborony ta hromadskosti u sferi protydii kryminalnym pravoporushenniam*: materialy II Vseukrainskoho kruhloho stolu. 2025. S. 295-298.
3. Kryminalnyi kodeks Ukrainy: Zakon Ukrainy vid 05.04.2001 № 2341-III. *Vidomosti Verkhovnoi Rady Ukrainy*. 2001. № 25–26. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
4. Pro elektronni dokumenty ta elektronnyi dokumentoobih: Zakon Ukrainy vid 22.05.2003 № 851-IV: stanom na 31 hrudnia 2023r. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.
5. Kryminalnyi protsesualnyi Kodeks Ukrainy (stattia 99): Kodeks Ukrainy vid 13.04.2012: stanom na 01 serpnia 2025 r. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

6. Pashkovskyi M. I. Lantsiuh zberihannia dokaziv (Chain of custody) protsesualna forma. *Zbirnyk naukovykh prats z materialamy III mizhnarodnoi naukovoi konferentsii. Innovatsiina nauka: poshuk vidpovidei na vyklyky suchasnosti*. S.157-161.

7. Suddi KKS VS obhovoryly problemni pytannia dopustymosti elektronnykh dokaziv pid chas sudovoho rozghliadu. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/.

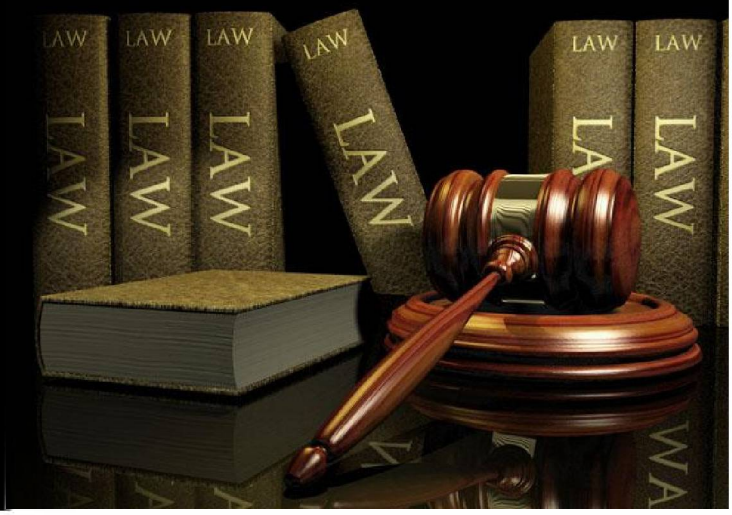
8. Konventsiia pro kiberzlochynnist. Ofitsiinyi vebportal parlamentu Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

9. Konventsiia pro kiberzlochynnist (Budapesht, 23 lystopada 2001 roku). Ofitsiinyi vebsait Verkhovnoi Rady Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/980_093#Text.

10. Luhina N.A., Vartovnik A.M. Blokchein v Ukraini: problemy pravovoho rehuliuvannia. *Mizhnarodnyi naukovyi zhurnal "Internauka"*. № 8(88), 2 t., 2020. S. 74-78.

ISSN 2409-6415

Електронне науково-практичне фахове видання



2026 / № 142

Журнал східноєвропейського права

(Протокол № 3 від 08 жовтня 2013 року)
Включено до Переліку наукових фахових видань України
(Наказ Міністерства освіти і науки України від 15.04.2014 № 455)
ISSN 2409-6415
Журнал східноєвропейського права внесений до HeinOnline

Проблематика: висвітлення результатів фундаментальних та прикладних наукових досліджень, дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук з актуальних проблем становлення та прагматичного розвитку східноєвропейського права в умовах глобалізаційних викликів

Галузь науки: юридичні науки

Періодичність: щомісячно

Головний редактор: Мосьондз Сергій Олександрович, доктор юридичних наук, професор, виконуючий обов'язки ректора ПВНЗ «Університет сучасних знань»

Відповідальний секретар: Соколан Тетяна Сергіївна, кандидат юридичних наук

Члени редколегії: **Мельник Роман Сергійович,** доктор юридичних наук, професор, завідувач кафедри адміністративного права, Київський національний університет імені Тараса Шевченка **Янчук Артем Олександрович,** доктор юридичних наук, професор, державний секретар, Міністерство охорони здоров'я, **Кузьменко Оксана Володимирівна,** доктор юридичних наук, професор, професор кафедри теорії та історії права, Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана», **Личенко Ірина Олександрівна**, доктор юридичних наук, професор, завідувач кафедри цивільного права та процесу, Навчально-науковий інститут права, психології та інноваційної освіти Національного університету «Львівська політехніка», **Чорна Вікторія Григорівна,** доктор юридичних наук, доцент, доцент кафедри адміністративного права і процесу, Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана», **Губанова Тамара Олексіївна,** доктор юридичних наук, професор, директор, Приватний вищий навчальний заклад «Фінансово-правовий коледж», **Книш Сергій Володимирович,** кандидат юридичних наук, юрисконсульт, Східноєвропейський національний університет імені Лесі Українки, **доктор Егле Білевічюте,** член Комісії з розгляду адміністративних спорів Литви, професор Університету Миколаса Ромеріса, (Вільнюс, Литва), **доктор Тома Бірмонтієн,** професор Лабораторії правосуддя, Лабораторії прав людини юридичного факультету Інституту публічного права Університету Миколаса Ромеріса, (Вільнюс, Литва), **доктор Агне Тваронавічієн,** Лабораторія соціальних технологій, Лабораторія посередництва та сталого розв'язання конфліктів юридичного факультету Інституту публічного права Університету Миколаса Ромеріса (Вільнюс, Литва)

Адреса редакції: вул. Велика Васильківська, 57/3, м. Київ, Україна, 03150

Тел.: +38 (063) 758 57 24
E-mail: easternlaw.ua@gmail.com
Сайт: http://easternlaw.com.ua

(Order of the Ministry of Education and Science of Ukraine of 15.04.2014 No. 455)
ISSN 2409-6415
The Journal of Eastern European Law is included in HeinOnline

Issue: lighting the results of basic and applied research, dissertations for the degree of doctor and candidate of sciences on current issues of establishment and pragmatic development of Eastern European law within globalization challenges

Branch of science: jurisprudence

Frequency: monthly

Editor in Chief: Mosondz Serhii Oleksandrovych, doctor of juridical sciences, professor, acting rector of the Private Higher Educational Establishment "The University of Modern Knowledge"

Secretary in Charge: Sokolan Tetiana Serhiivna, candidate of juridical sciences

Members of the editorial board: **Melnyk Roman Serhiiovych,** doctor of juridical sciences, professor, head of the Department of Administrative Law of Taras Shevchenko National University of Kyiv, **Yanchuk Artem Oleksandrovych,** doctor of juridical sciences, professor, state secretary, the Ministry of Health, **Kuzmenko Oksana Volodymyrivna,** doctor of juridical sciences, professor, professor of the Department of theory and history of law at the State Higher Educational Establishment "Kyiv National Economic University named after Vadym Hetman", **Lychenko Iryna Oleksandrivna,** doctor of juridical sciences, head of the Department of Civil Law and Procedure at the Training and Scientific Institute of Jurisprudence, Psychology and Innovative Education of Lviv Polytechnic National University, **Chorna Viktoriia Hryhorivna,** doctor of juridical sciences, associate professor, associate professor of the Department of Administrative Law and Proceeding at the State Higher Educational Establishment "Kyiv National Economic University named after Vadym Hetman", **Hubanova Tamara Oleksiivna,** doctor of juridical sciences, professor, director at the Private Higher Educational Establishment "Financial and Law College", **Knysh Serhii Volodymyrovych,** candidate of juridical sciences, legal counsel, Lesya Ukrainka Eastern European National University, **Dr. Eglė Bilevičiute,** member at Lithuania Administrative Disputes Commission, professor at the Mykolas Romeris University (Vilnius, Lithuania), **Dr. Toma Birmontien,** professor at Justice Laboratory, Human Rights Laboratory of Faculty of Law of Institute of Public Law, Mykolas Romeris University (Vilnius, Lithuania), **Dr. Agne Tvaronaviciene,** Social Technologies Laboratory, Mediation and Sustainable Conflict Resolution Laboratory of Faculty of Law, Institute of Public Law of Mykolas Romeris University (Vilnius, Lithuania).

Address of the editorial office: 57/3 Velyka Vasylkivska Street, Kyiv, 03150, Ukraine

Tel.: +38 (063) 758 57 24
E-mail: easternlaw.ua@gmail.com
Website: http://easternlaw.com.ua

ЗМІСТ

Гринько С.Д. Сімейні правовідносини у нотаріальній діяльності в Україні в умовах цифровізації……..7

Кириченко О.А. Особливості інноваційної сутності і видового поділу правопорушень у сфері здійснення медичної та фармацевтичної діяльності і системи громадського здоров'я……...16

Манойло Н.Г. Античні мислителі про суть буття в єдності «штучного» і «природного» в інтелекті людини……26

Проневич О.С. Вітчизняна модель державної служби в органах судової влади: легальний аспект……..38

Волощук О.Т. Регіональна політика та конституційно-правові механізми управління безпекою регіонів України в умовах зовнішньої збройної агресії……51

Гринько Р.В. Правове регулювання виконання договірних зобов'язань та відшкодування збитків у цивільних правовідносинах……..57

Єрмолаєва Т.В., Дзюба К.О. Екоцид: юридична природа та особливості кримінально-правової кваліфікації……66

Жук Н. Особливий період і воєнний стан як чинники впливу на концептуальні засади конституційного ладу та конституційно-правовий статус суб'єктів права в Україні……75

Кириченко О.А., Кириченко О.О. Особливості інноваційного розуміння сутності і видового поділу достовірних і недостовірних відомостей і можливостей їх використання у процесі публічної дискусії в контексті здійснення медичної та фармацевтичної діяльності і системи громадського здоров'я……..88

Лаговська Н.В., Барчан А.Ю. Особливості захисту авторських прав в умовах воєнного стану в Україні……..98

Лугіна Н.А., Бак Н.С., Бак С.С. Сучасні виклики у розслідуванні кіберзлочинів: кримінально-правові та процесуальні аспекти……105

Островський С.О. Розмежування правових категорій «збройний конфлікт» і «воєнний конфлікт» у контексті мобілізації та мобілізаційної підготовки……..112

Панченко С.В. Поняття та сутність способів захисту прав учасників цивільних правовідносин……..119

Славна О.В. Гендерний мейнстрімінг у відновленні: роль Стамбульської конвенції в поствоєнній Україні……128

Сухарєва А.О., Крижановська О.В. Законодавче забезпечення судочинства в Україні……136

Томкіна О.О. Якість нормативно-правового забезпечення державної реєстрації права власності в контексті євроінтеграції……144

Чорномаз О.Б. Поняття та види інформаційно-комунікаційних технологій як спосіб та засіб учинення домашнього насильства……154

Якимчук С.О. Особливості дисциплінарної відповідальності за порушення правил адвокатської етики……163

Музика В.Ф. Особливості початкового етапу розслідування воєнних злочинів, вчинених проти цивільних громадян……171

Обущак В.В. Стратегія запобігання злочинності у сфері оподаткування: міжнародний досвід та напрями імплементації……178

Петровець О.Ф. Протиправне заволодіння майном підприємства, установи, організації: кримінально-правовий аспект……184

Секо С.О. Трансформація уявлень про організовану злочинність у сучасній кримінально-правовій доктрині……191

Маркосян Л.М., Івакіна Є.Т., Ігнатченко Д.О. Проблеми міжнародно-правового регулювання захисту свободи релігії в європейському контексті……199

Фатєєв А.О. Підстави примусової ліквідації юридичної особи корпоративного типу: компаративний підхід……208

Новицький Я.О. Зарубіжні моделі імунітету комбатанта: порівняльно-правовий вимір……218

Стрельченко О.Г., Бухтіярова І.Г. Міжгалузеві аспекти адміністративної відповідальності за порушення земельного законодавства……230

TABLE OF CONTENTS

S.D. Hrynko Family Legal Relations in Notarial Activity in Ukraine under Digitalization Conditions……..7

O.A. Kirichenko Features of the Innovative Essence and Specific Division of Offenses in the Field of Medicine, Pharmacy and Public Health System……...16

N.H. Manoilo Ancient Thinkers on the Essence of Being in the Unity of the "Artificial" and the "Natural" in Human Intellect……26

O.S. Pronevych Domestic Model of Civil Service in the Judiciary: Legal Aspect……..38

O.T. Voloshchuk Regional Policy and Constitutional and Legal Mechanisms for Managing Regional Security in Ukraine under External Aggression……...51

R.V. Hrynko Legal Regulation of the Performance of Contractual Obligations and Compensation for Damages in Civil Legal Relations……...57

T.V. Yermolaeva, K.O. Dziuba Ecocide: Legal Nature and Specifics of Criminal Law Qualification……66

N. Zhuk Special Period and Martial Law as Factors of Influence on the Conceptual Foundations of the Constitutional System and the Constitutional and Legal Status of Legal Subjects in Ukraine……75

O.A. Kirichenko, O.O. Kirichenko Features of Innovative Understanding of the Essence and Specific Division of Reliable and Unreliable Information and the Possibilities of Their Use in the Process of Public Discussion in the Context of Medical and Pharmaceutical Activities and the Public Health System.....88

N.V. Lagovska, A.Yu. Barchan Features of Copyright Protection under Martial Law in Ukraine……98

N.A. Luhina, N.S. Bak, S.S. Bak Current Challenges in Investigating Cybercrime: Criminal Legal and Procedural Aspects……..105

S.O. Ostrovskiy Distribution of Legal Categories "Armed Conflict" and "Military Conflict" in the Context of Mobilization and Mobilization Preparation……..112

S.V. Panchenko Concept and Essence of Methods for Protecting the Rights of Participants in Civil Legal Relations……..119

O.V. Slavna Gender Mainstreaming in Recovery: Role of the Istanbul Convention in Post-War Ukraine……...128

A.O. Sukharieva, O.V. Kryzhanovska Legislative Support for Judicial Proceedings in Ukraine……...136

O.O. Tomkina Quality of Legal Regulation of State Registration of Property Rights in the Context of European Integration……..144

O.B. Chornomaz Concept and Types of Information and Communication Technologies as a Method and Means of Committing Domestic Violence……..154

S.O. Yakymchuk Features of Disciplinary Liability for Violations of Lawyers' Ethical Rules ……...163

V.F. Muzyka Features of the Initial Stage of the Investigation of War Crimes Committed against Civilian Citizens……171

V.V. Obushchak Strategy for Preventing Tax Criminality: International Experience and Directions of Implementation……..178

O.F. Petrovets Unlawful Taking of Property of an Enterprise, Institution, or Organization: A Criminal Law Perspective……..184

S.O. Seko Transformation of Ideas about Organized Crime in Modern Criminal Law Doctrine……191

L.M. Markosian, Ye.T. Ivakina, D.O. Ihnatchenko Problems of International Legal Regulation of the Protection of Freedom of Religion in the European Context……..199

A.O. Fatieiev Grounds for the Compulsory Liquidation of a Corporate-Type Legal Entity: a Comparative Law Approach……..208

Ya.O. Novytskyi Foreign Models of Combatant Immunity: Comparative Legal Aspects……...218

O.G. Strelchenko, I.H. Bukhtiiarova Inter-Sectoral Aspects of Administrative Liability for Violations of Land Legislation……...230