DOI: https://doi.org/10.33994/kndise.2023.68.06
УДК 330.354:004+001.891

Антоніна Іванівна Черемнова
кандидат юридичних наук, доцент,
вчений секретар

ORCID: https://orcid.org/0000-0002-0221-6337
E-mail: cheremnova2506@gmail.com

Одеський науково-дослідний інститут
судових експертиз
Міністерства юстиції України

Лариса Степанівна Бєлік
кандидат юридичних наук, доцент,
доцент кафедри криміналістики

ORCID: https://orcid.org/0000-0003-2183-6635
E-mail: larysa.bielik1@gmail.com

Національний університет «Одеська юридична академія»

ЦИФРОВА ІНФОРМАЦІЯ ЯК ОБ'ЄКТ ЕКСПЕРТНОГО ДОСЛІДЖЕННЯ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Стаття присвячена проблемним питанням розгляду цифрової інформації як об'єкта експертного дослідження. Запропоновано внести зміни до чинного кримінального процесуального законодавства, доповнивши ч. 2 ст. 84 Кримінального процесуального кодексу України новими джерелами доказів – цифровими. Виокремлено дві групи цифрової інформації, яка виступає об'єктом експертного дослідження під час досудового розслідування.

Ключові слова: *діджиталізація, досудове розслідування, цифрові докази, цифрова інформація, судова експертиза, об'єкт експертного дослідження.*

Постановка проблеми. Діджиталізація, що стала пріоритетним напрямом на шляху становлення України як соціальної, демократичної, правової держави, передбачає насамперед масштабну та широкоаспектну роботу як з боку держави, так і суспільства в цілому, оскільки вимагає відповідального підходу до розроблення та впровадження в діяльність державних, правоохоронних органів та судової системи нового для останніх виду інформації – цифрової, проте окреслене явище не оминуло й злочинну діяльність, зазначене призвело до потреби проведення судової експертизи, що вимагає насамперед підготовки фахівців – експертів, оскільки будь-який цифровий файл чи документ є кодом, дослідження якого без наявності спеціальних знань та спеціального обладнання є неможливим.

Актуальність теми дослідження пояснюється насамперед тим, що електронні дані набагато легше змінити чи підробити, ніж традиційні форми викладення інформації, тому правоохоронцям потрібно дотримуватися певних правил поводження з даними, які нададуть можливість забезпечити їхнє легітимне використання під час доказування. Джерелами доказів, що представлені в електронній формі можуть бути: різноманітні носії інформації; моноблоки, мобільні пристрої (мобільні телефони, планшетні комп'ютери), цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, звуко- та відеозаписи тощо, тобто джерелом доказів може бути будь-який електронний пристрій, який знаходиться на місці обшуку. Варто також зазначити, що постійно з'являються нові види електронних пристроїв, які можуть містити електронні докази. [1, с. 6-7]. Зважаючи на наведене, постає нагальна потреба у визначенні механізму проведення експертизи цифрової інформації.

Аналіз останніх досліджень і публікацій. Питанням розгляду електронних/цифрових доказів присвятили свої роботи такі видатні вітчизняні та зарубіжні науковці: Г. Авдєєва, Т. Авер'янова, О. Антонюк, І. Апалькова, В. Бахін, Р. Бєлкін, П. Біленчук, С. Веретенюк, Н. Вілкінс, М. Гетманцев, Н. Дєєва, А. Добринін, М. Долженко, А. Дулов, П. Еліот, М. Жижина, В. Журавель, Г. Карчева, І. Когутич, О. Козицька, С. Коляденко, В. Коновалова, В. Куйбіда, О. Лазько, Т. Матюшкова, В. Петренко, М. Салтевський, Р. Степанюк, Т. Стоянова, С. Теппер, Д. Цехан, О. Чорний, Ю. Чорноус, В. Шепітько, А. Штефан та інші дослідники.

Мета дослідження полягає у розгляді проблемних аспектів використання цифрової інформації як об'єкта експертного дослідження та визначення перспективних напрямків розвитку таких експертиз під час досудового розслідування.

Викладення основного матеріалу. На початковому етапі розвитку комп'ютерної техніки проблема використання у доказуванні цифрової інформації виникла у США, де існували правила використання «нетрадиційних доказів» (novel evidence). З урахуванням особливостей англосаксонської системи права, джерелом таких правил став судовий прецедент у справі Фрай проти США (Frye vs United States), який стосувався використання у доказуванні нових даних та методик науки і складався із двох елементів: по-перше, суду необхідно визначити, до якої галузі наукового знання відносяться дані та методики, які покладені в основу доказу, а по-друге, чи визнається провідними вченими-фахівцями цієї галузі принцип, на основі якого сформований доказ [9, с. 256]. Від розуміння природи електронної інформації, правильного поводження з нею не лише при проведенні судової комп'ютерно-технічної експертизи та інших видів експертиз, а й при збиранні доказів, які містять такі сліди, залежить можливість їх застосування у кримінальному провадженні [3, с. 14].

Варто підкреслити, що в науковому колі наявна певна дискусія щодо правильності визначення таких доказів як «електронних», «цифрових» чи ототожнення цих двох представлених варіантів.

Зокрема, О. Козицька під електронними доказами розуміє цифрові об'єкти, що були засобом чи знаряддям вчинення кримінального правопорушення, зберегли електронно-цифрові сліди кримінального правопорушення, були предметом або об'єктом вчинення кримінального правопорушення або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [4, с. 418-420].

Електронні докази — це докази у кримінальних провадженнях, які можна отримати в електронній формі. Електронні докази отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу Інтернет. Вони стають доступними для сприйняття людиною після обробки засобами комп'ютерної техніки. Разом із поняттям «електронні докази» (electronic evidence), часто застосовують поняття «цифрові докази» (digital evidence). Оскільки на законодавчому рівні ці поняття ще не окреслені, їх використовують паралельно [1, с. 5].

Д. Цехан під цифровими доказами пропонує розуміти фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною. При цьому, обов'язковою ознакою цифрового доказу є конвергентність, під якою розуміється здатність одиничного доказу входити у сукупність інших доказів і набувати у зв'язку з цим доказового значення. Саме тому цифровий об'єкт, який є нематеріальним, не має відповідних якісних фізичних характеристик, має специфічну процедуру та середовище створення, здатний до копіювання та переміщення без втрати характеристик, сприймається людиною лише після обробки ЕОМ та виведення інформації на відповідний технічний пристрій (монітор), його неможливо визнати матеріальним об'єктом і, як наслідок, речовим доказом чи традиційним документом. У даному випадку необхідно оцінювати власне інформацію, а не матеріальний об'єкт, на якому вона зафіксована [9, с. 257].

Поняття електронних доказів отримало своє нормативне закріплення у Цивільному процесуальному кодексі України, Кодексі адміністративного судочинства України та Господарському процесуальному кодексі України, проте Кримінальний процесуальний кодекс України не передбачає такого процесуального джерела доказів як електронні, закріплюючи у п. 2 ст. 84 лише показання, речові докази, документи, висновки експертів [6]. На наш погляд, така позиція законодавця є доволі незрозумілою, оскільки вказаний нормативно-правовий акт передбачає обов'язкову відеофіксацію проведення слідчих, негласних слідчих/розшукових дій та й самого безпосереднього судового засідання, тобто робота законодавця щодо використання цифрових технологій під час досудового розслідування та судового розгляду проводиться, проте, на жаль, має наразі низку неузгодженостей, що тягне за собою «затягування» процесу розслідування кримінального правопорушення та певним чином обмежує діяльність слідчого.

Зважаючи на наведене, вважаємо що доцільним буде доповнення ч. 2 ст. 84 Кримінального процесуального кодексу України таким процесуаль-

ним джерелом доказів як цифрові. Пропонуємо викласти зазначену статтю у наступній редакції: *«2. Процесуальними джерелами доказів є показання, речові докази, цифрові докази, документи, висновки експертів».* Та зробити відповідні доповнення до § 4. Речові докази і документи Глави 4. Докази і доказування.

Ми підтримуємо точку зору А. Мурашко, що електронні докази можуть подаватися в паперових копіях, при цьому остання не буде вважатися письмовим доказом, тобто у цьому випадку, постає питання що саме слід розуміти під оригіналом документа та вміти правильно визначити що саме є оригіналом (письмовим документом), а що – паперовою копією електронного документа. [7, с. 370]. Саме тому необхідно визначити що саме слід розуміти під цифровою інформацією.

В цілому підтримуючи погляди науковців, які було нами попередньо розглянуто, вважаємо, що під цифровою інформацією в контексті розслідування кримінальних проваджень слід розуміти дані, представлені в електронній (цифровій) формі, що містять відомості, які мають значення для справи, містять сліди вчиненого кримінального правопорушення, були знаряддям чи засобом його вчинення, які зберігаються на матеріальних носіях інформації: комп'ютерних, мобільних пристроях, цифрових камерах, роутерах тощо, або нематеріальних ресурсах, таких як мережа Інтернет, локальні мережі установ та організацій тощо, при цьому на зазначених носіях інформації можуть міститися: файли (що містять текстову інформацію, аудіо- чи відео-); різноманітне програмне забезпечення, що використовується як «знаряддя» вчинення злочину чи задля приховання слідів його вчинення; файли, що містять сліди підробки чи фальсифікації; бази даних, вільний доступ до яких заборонено чинним законодавством у сфері охорони державної таємниці, захисту персональних даних тощо; відсканові копії, фотокопії документів, обмежених для обігу, тощо.

Зважаючи на те, що цифрова інформація обов'язково повинна міститися або на матеріальному носії, або нематеріальному, як було попередньо зазначено, вважаємо за доцільне виокремити дві групи першої, зважаючи на заявлений критерій.

Так, особливостями дослідження цифрової інформації, що знаходиться на матеріальних носіях інформації, є насамперед те, що певна доказова інформація щодо події вчиненого кримінального правопорушення може міститися безпосередньо на ньому.

Беручи до увагу судову практику, зокрема нами було розглянуто постанову Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29 березня 2021 року по справі № 554/5090/16-к, де суд звертається до проведення судово-технічної експертизи, експертам було поставлено такі запитання: 1) чи є носії інформації автентичними; 2) чи виготовлені вони у встановлену слідством дату; 3) чи є вони копіями з оригіналів; 4) яка техніка використовувалася в ході проведення НС(Р)Д і яка техніка використовувалася під час виготовлення копій із первинних носіїв, чи є вони ідентичними; 5) чи наявні на наданих носіях відповідні фрази про початок зйомок та про їх закінчення; 6) чи маються сліди стороннього втручання в записи, в тому

числі знищення, накладання, зміни тощо, та механізм їх утворення за наявності [8]. Тобто, як ми можемо помітити, що фактично наразі мова йде про проведення експертного дослідження безпосередньо носія інформації та наявного відеозапису проведеної негласної слідчої (розшукової) дії. Тобто, на наш погляд, можна говорити про дві складові частини проведення судової експертизи:

– експертиза матеріального носія інформації, на якому безпосередньо зберігається цифрова інформація, при цьому. М. Климчук зазначає, що експертному дослідженню підлягають також сліди, що містяться на самому мобільному телефоні (приміром, IMEI-код, SMS-повідомлення, відомості про надіслані повідомлення, телефонні з'єднання, абонентська книга телефону, телефонні номери, що використовуються, сліди мікрочастинок, пальців рук. Сліди, присутні на SIM-карті і наявні на мобільному телефоні, зазвичай ідентичні) [2]. Варто підкреслити, що якщо мова йде про експертизу матеріального носія секретної інформації, тоді додатково перевіряється дотримання вимог Закону України «Про державну таємницю», зокрема на предмет наявності відповідної захищеності пристрою та його облік;

– експертиза цифрового файлу (файлу (що містить текстову інформацію, аудіо- чи відео-); різноманітне програмне забезпечення, що використовується як «знаряддя» вчинення злочину чи задля приховання слідів його вчинення; файли, що містять сліди підробки чи фальсифікації; бази даних, вільний доступ до яких заборонено чинним законодавством у сфері охорони державної таємниці, захисту персональних даних тощо; відскановані копії, фотокопії документів, обмежених для обігу тощо).

Тобто, можна констатувати, що характерною рисою експертизи цифрової інформації, віднесеної нами до вищезазначеної групи, є проведення фактичного дослідження двох об'єктів: матеріального носія інформації та безпосередньо цифрової інформації, що на ньому міститься.

До другої групи пропонуємо віднести цифрову інформацію, що зберігається в Інтернеті чи в хмарних сховищах. Головною відмінністю такої цифрової інформації від тієї, що виокремлювалася нами у першу групу, є те, що вона фактично не зберігається на конкретному матеріальному носії інформації і особа/особи може мати до неї доступ з різноманітних пристроїв, які мають можливість виходу в Інтернет, водночас так само особа/особи має можливість видалити таку інформацію у будь-який момент дистанційно з різноманітних пристроїв. Варто наголосити, що за таких обставин експертному дослідженню можуть підлягати не лише цифрові документи чи файли, а й «сліди», що залишаються після відповідних дій, вчинюваних у кіберпросторі. Як слушно зазначає В. Коршенко, для того, щоб зазначені сліди могли перетворитись на докази, необхідно їх знайти, процесуальним шляхом виявити та зафіксувати. Основним процесуальним способом перетворення невидимої інформації та слідів кримінальних правопорушень на докази є проведення судової експертизи [5].

Окремим підвидом, на наш погляд, можна виокремити інформацію, яка міститься та розповсюджується в месенджерах, зокрема, за допомогою приватних чатів, спільнот та каналів. Зважаючи на ситуацію, яка склалася

в Україні в умовах збройної агресії з боку російської федерації, правоохоронці стикнулися з ситуацією, коли використовуючи найбільш розповсюджені месенджери: Telegram, WhatsApp, Viber тощо, особи розповсюджували інформацію щодо розміщення позицій та/або пересування техніки, що несе для ворога стратегічне значення та наносить шкоду державним інтересам, те саме стосується розміщення у вищезгаданих спільнотах аудіо-, відео- чи текстових файлів, що носять ознаки підробки та/або спотворення викладених в них даних.

Особливої уваги заслуговує дослідження інформації, що знаходиться у так званому darknet, оскільки зазвичай особи, які провадять злочинну діяльність з його використанням, застосовують доволі розгалужену систему захисту даних задля унеможливлення правоохоронними органами з'ясування особи злочинця:

– використовуються «захищені» операційні системи: Linux, Kodachi Linux тощо;

– застосовуються браузери, які не перебувають у широкому використанні споживачами, такі як, наприклад, Tor Browser, що дозволяє встановити анонімне мережеве підключення та має певний захист від стороннього втручання;

– вихід до Інтернету здійснюється з використанням VPN, задля того аби унеможливити визначення справжнього місцезнаходження особи та її IP-адреси.

Тобто, головною проблемою під час проведення експертизи цифрових файлів створених, завантажених чи використаних за допомогою такої системи є складність, а іноді й неможливість визначення особи, що провадить такого роду діяльність та вчиняє правопорушення. Проте, слід зазначити, що вчинення зазначеної низки дій вимагає від злочинців наявності спеціальних знань, що свідчить про високий рівень володіння ними Інформаційними технологіями. Тобто, як можна помітити з наведеного, такий вид експертизи є найбільш складним, оскільки за таких обставин особа використовує серйозну систему захисту інформації, яка може надати слідству дані про особу злочинця.

Висновки. На основі проведеного аналізу можна дійти висновку, що експертиза цифрової інформації в умовах розвитку інформаційних технологій та запровадження електронного документообігу в Україні передбачає удосконалення чинного на сьогодні кримінального процесуального законодавства у частині включення цифрових доказів до джерел доказів у кримінальному провадженні.

Перелік посилань

1. Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. рек. Київ : НАВС, 2020. 104 с. URL: http://elar.naiau.kiev.ua/bitstre-

References

1. Korneiko, O. V. (Ed.) (2020). The use of electronic (digital) evidence in criminal proceedings: guidelines. Kyiv. National Academy of Internal Affairs. 104 p. Retrieved from: http://elar.naiau.kiev.ua/bitstream/123456789/17

am/123456789/17605/1/Використання%20електронних%20%28цифрових%29%20доказів.pdf

2. Климчук М. П. Сліди кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, та особливості їх виявлення. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід*. Київ : НАВС, 2020. С. 86.

3. Климчук М. П., Комiссарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні: навч. посіб.. Львів : Львів. держ. ун-т внутрішніх справ, 2022. 112 с.

4. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418-421.

5. Коршенко В. А. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jumalul juridic national: teorie i practica.* 2017. № 2. С. 192.

6. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 №4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text

7. Мурашко А. С. Проблемні питання доказування у цивільному процесі. *Сучасна цивілістика : 15 років наукових звершень* : матеріали XV Міжнар. наук.- практ. конф., 22 травня 2020 року. Одеса: Юрид. література, 2020. С. 369-371.

8. Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29 березня 2021 року

605/1/Використання%20електронних%20%28цифрових%29%20доказів.pdf (in Ukrainian).

2. Klymchuk, M. P. (2020). Traces of criminal offenses committed using cellular communications, and features of their detection. *Topical issues of detecting and solving crimes by the National Police: domestic and foreign experience*. Kyiv. National Academy of Sciences. P. 86 (in Ukrainian).

3. Klymchuk, M. P., Komissarchuk, Yu. A., Marko, S. I., Stetsyk, B. V. (2022). Forensic computer-technical expertise in criminal proceedings: a study guide. Lviv. Lviv State University of Internal Affairs. 112 p. (in Ukrainian).

4. Kozytska, O. H. (2020). Regarding the concept of electronic evidence in criminal proceedings. *Legal scientific electronic journal*. No. 8. P. 418-421 (in Ukrainian).

5. Korshenko, V. A. (2017). Forensic telecommunications expertise as a source of evidence in cybercrime investigations. *Jumalul juridic national: teorie i practica.* No. 2. P. 192 (in Ukrainian).

6. Criminal Procedure Code of Ukraine: Law of Ukraine dated April 13, 2012. No. 4651-VI. Retrieved from: https://zakon.rada.gov.ua/laws/show/4651117#Text (access date 12.02.2023) (in Ukrainian).-

7. Murashko, A. S. (2020). Problematic issues of proof in civil proceedings. *Modern civics: 15 years of scientific achievements*: proceedings of the XV International Scientific and Practical Conference, May 22. Odesa. P. 369-371 (in Ukrainian).

8. Resolution of the Joint Chamber of the Criminal Court of Cassation of the Supreme Court dated March 29, 2021

по справі № 554/5090/16-к. URL : https://reyestr.court.gov.ua/Review/96074938

9. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.* 2013. № 5. С. 256-260. URL: http://www. vstnik-pravo.mgu.od.ua/archive/jurspradenc5/56.pdf

in case No. 554/5090/16-k. Retrieved from: https://reyestr.court.gov.ua/Review/96074938 (access date 10.02.2023) (in Ukrainian).

9. Tsekhan, D. M. (2013). Digital evidence: concepts, features and place in the evidence system. *Scientific Bulletin of the International Humanitarian University. Jurisprudence.* No. 5. P. 256-260. Retrieved from: http://www.vestnik-pravo.mgu.od.ua/archive/jurspradenc5/56.pdf (in Ukrainian).

DIGITAL INFORMATION AS AN OBJECT OF EXPERT RESEARCH IN THE CONTEXT OF DIGITALIZATION: PROBLEMS AND DEVELOPMENT PROSPECTS

A. Cheremnova
L. Bielik

The article is devoted to the problems of considering digital information as an object of expert research. It is proposed to amend the current criminal procedural legislation by adding part 2 of Art. 84 of the Criminal Procedure Code of Ukraine with new sources of evidence – digital, namely, to state it in the following wording: «2. Procedural sources of evidence are testimony, material evidence, digital evidence, documents, and expert opinions.

The definition of digital information is formulated in the context of the investigation of criminal proceedings, namely, it is indicated that it can be understood as data presented in electronic (digital) form, containing information relevant to the case, containing traces of a criminal offence that is an instrument or means of committing it, stored on tangible media: computer, mobile devices, digital cameras, routers, etc., or intangible resources such as the Internet, databases, local networks of institutions and organizations, etc., while on the specified media may contain: files (containing text information, audio or video); a variety of software used as a «tool» for committing a crime or to hide the traces of its commission; files containing traces of forgery or falsification; databases, free access to which is prohibited by the current legislation in the field of protection of state secrets, protection of personal data; scanned copies, photocopies of restricted documents, etc.

Two groups of digital information are identified, which are the object of expert research in the course of the pre-trial investigation: digital information located on a material storage medium; digital information located on the Internet or in cloud storage. Attention is drawn to the forensic computer-technical examination of digital information located in the darknet, since persons carrying out criminal activities using it use a fairly extensive data protection system to exclude the possibility of identifying the offender by law enforcement agencies: «protected» operating systems are used: Linux, Kodachi Linux, etc.; browsers are used that are not widely used by consumers, such as, for example, Tor Browser, which allows you to establish an anonymous network connection that has some protection from outside interference;

access to the Internet is carried out using a VPN in order to prevent the determination of the actual location of a person and his IP address.

Key words: digitalization, pre-trial investigation, digital evidence, digital information, forensic examination, object of expert research.

DOI: https://doi.org/10.33994/kndise.2023.68.07
УДК 347.9:346.2

Катерина Миколаївна Дзюбак
кандидат економічних наук

ORCID: https://orcid.org/0000-0001-9227-6538
E-mail: ekaterina.dzubak@gmail.com

Одеський науково-дослідний інститут судових експертиз
Міністерства юстиції України

ОРГАНІЗАЦІЙНО-ПРАВОВІ МЕЖІ ЗАБЕЗПЕЧЕННЯ НАУКОВО-ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ У ГАЛУЗІ ПРАВА – АДМІНІСТРАТИВНОМУ СУДОЧИНСТВІ

Статтю присвячено дослідженню організаційно-правових меж забезпечення науково-експертної діяльності у адміністративному судочинстві, визначеному в Кодексі адміністративного судочинства України. Доводиться необхідність удосконалення норм зазначеного кодексу України в частині визначення процесуальних прав та обов'язків експерта в галузі права в судовому процесі, а також правової природи його висновку. Надано пропозиції про внесення змін до цього кодексу України.

Ключові слова: *експерт у галузі права, висновок експерта у галузі права, адміністративний процес, аналогія права, аналогія закону, науково-експертна експертиза.*

Постановка проблеми. Система наукових знань у сфері правової експертизи охоплює перетворені для потреб судочинства відомості з правових наук. Перш за все, це стосується цивільного, адміністративного та господарського судочинства, в яких передбачено участь експерта у галузі права та надання ним висновку під час розгляду справ зазначених галузей права та процесу. Неоднозначність підходів щодо розвитку нового напряму теоретичного аналізу експертної діяльності зумовлено складністю та невизначеністю правового статусу експерта у галузі права та складеного ним висновку.

Встановлені у ст. ст. 112-113 Кодексу адміністративного судочинства України (надалі – КАС України) [1] законодавчі норми використання висновку експерта у галузі права у адміністративному судочинстві виявили невизначеність основних аспектів діяльності експерта у галузі права, які викликають й досі дискусійність та невирішеність. Серед них: процедура