

Сошенко Богдан Олексійович, молодший юрист Адвокатського об'єднання «Богатир і партнери»

ДОКАЗИ, ЩО МАЮТЬ ЦИФРОВУ ФОРМУ, У ВСТАНОВЛЕННІ УМИСЛУ ТА РОЛІ СУДДІ В МЕХАНІЗМІ РЕЙДЕРСЬКОГО ЗАХОПЛЕННЯ

Рейдерське захоплення із залученням судової процедури відрізняється від відкритого силового заволодіння майном тим, що незаконний результат досягається через послідовне використання корпоративних, реєстраційних, процесуальних і фінансових інструментів. Судовий акт у такій схемі може створити формальну підставу для зміни керівника, блокування активів, заборони законному власнику здійснювати управління або проведення реєстраційної дії [1; 15]. Однак скасування рішення, істотне порушення процесуального закону чи незвичайне тлумачення правової норми не доводять злочинного умислу судді. Ключовим завданням доказування є встановлення того, чи усвідомлював суддя спрямованість спільного плану на протиправне заволодіння майном і чи бажав або свідомо допускав використання власних повноважень для його реалізації.

Вирішення цього завдання має узгоджуватися з конституційним статусом судової влади. Незалежність судді та функціональний імунітет захищають свободу внутрішнього переконання і не допускають кримінального переслідування за саме лише ухвалення непопулярного, помилкового або скасованого рішення [2; 8; 9; 12]. Водночас ці гарантії не перетворюються на особистий привілей і не охоплюють умисне використання судових повноважень як складової рейдерського захоплення. Після визнання статті 375 Кримінального кодексу України неконституційною особливого значення набула вимога юридичної визначеності: поведінка судді повинна оцінюватися за ознаками конкретного чинного складу кримінального правопорушення, а не через відновлення скасованої моделі відповідальності під іншою назвою [3; 13].

Метою цих тез є розроблення доказового підходу до встановлення умислу та конкретної ролі судді в механізмі рейдерського захоплення на підставі відомостей, зафіксованих у цифровій формі, з одночасним визначенням меж їх належного, допустимого і достовірного використання у кримінальному провадженні.

Вихідним методологічним положенням є розмежування доказу і цифрової форми його існування. Файл, електронне повідомлення, запис інформаційної системи або набір метаданих не набувають наперед визначеної доказової сили лише через їх цифрове походження. Вони повинні містити фактичні дані, одержані з передбаченого законом процесуального джерела та належно закріплені [5]. Цифрові технології розширюють можливості виявлення прихованих зв'язків і відтворення послідовності подій, але одночасно створюють ризики фрагментарного подання інформації, зміни контексту, помилкової атрибуції облікового запису та неконтрольованого втручання у приватне спілкування [6; 11]. Тому доказування умислу потребує не накопичення цифрових фрагментів, а їх включення до логічно завершеної системи перевірюваних фактичних даних.

Для встановлення умислу судді доцільно застосовувати п'ятикомпонентний доказовий тест. Перший компонент становить інформаційна обізнаність: чи мав суддя до ухвалення рішення відомості про фактичних організаторів, незаконність поданих документів, очікувану реєстраційну дію та кінцевого набувача активу. Другий компонент охоплює позапроцесуальну комунікацію: її учасників, зміст, періодичність і збіг у часі з ключовими подіями. Третій компонент полягає у нетиповій процесуальній поведінці, яка сама по собі може бути нейтральною, але набуває значення у поєднанні з іншими даними. Четвертий компонент відображає синхронізацію судового акта з реєстраційними, корпоративними та фінансовими операціями. П'ятий компонент характеризує мотив і вигоду, зокрема рух коштів, передавання майна, погашення зобов'язань або іншу винагороду.

Інформаційну обізнаність можуть підтверджувати метадані отримання і відкриття файлів, історія пошуку та доступу до матеріалів, електронне листування, записи хмарних сховищ, журнали судової інформаційної системи й відомості про накладення електронного підпису. Особливу доказову вагу може мати встановлення того, що до офіційного надходження процесуального документа на пристрої або в обліковому записі судді вже існував його проєкт чи відомості, доступні лише організаторам захоплення. Проте такий збіг потребує перевірки автора файла, часу його створення, маршруту передавання, факту відкриття та можливих альтернативних джерел походження. Без цієї перевірки технічний збіг текстів залишається припущенням, а не доказом усвідомлення спільної злочинної мети [5; 14].

Позапроцесуальна комунікація має оцінюватися за змістом і функцією, а не за самим фактом контакту. Наявність номера телефону, одноразове з'єднання, перебування осіб у спільній геолокації або листування з представником сторони можуть мати правомірне пояснення. Доказове значення виникає тоді, коли зміст повідомлень свідчить про обговорення бажаного результату, порядку дій, тексту майбутнього рішення або часу його реалізації, а цифрова хронологія узгоджується з подальшими процесуальними та реєстраційними подіями. Для запобігання хибному висновку слід

перевіряти належність облікового запису конкретній особі, можливість доступу третіх осіб, повноту діалогу, часові пояси, резервні копії та видалені фрагменти. Лише після цього комунікаційні дані можуть використовуватися для висновку про попередню домовленість.

Нетипова процесуальна поведінка не є самостійним доказом злочину. Прискорений розгляд клопотання, відступ від усталеної практики, вибір певного заходу забезпечення або порушення строку можуть бути наслідком помилки, перевантаження чи іншої незлочинної причини. Їх доказове значення виникає лише за підтвердженого зв'язку з зовнішньою комунікацією та подальшим результатом. Тому необхідно зіставляти цифрові журнали розподілу справи, час доступу до матеріалів, історію редагування проєкту рішення, послідовність процесуальних дій і момент внесення запису до державного реєстру. Синхронність цих подій може вказувати на координацію, але висновок про умисел повинен враховувати звичайний порядок роботи відповідного суду та можливі альтернативні пояснення [15].

Встановлення ролі судді потребує відмежування його внеску від дій інших співучасників. Цифрова хронологія має показати, яке саме повноваження було використане, який проміжний результат створено судовим актом, хто і в який спосіб реалізував цей результат та чи був він необхідною ланкою заволодіння майном. Якщо реєстраційна дія відбулася до ухвалення рішення, ґрунтувалася на іншому документі або могла бути здійснена незалежно від поведінки судді, причинний і функціональний зв'язок потребує додаткового обґрунтування. Навпаки, заздалегідь погоджений час оприлюднення рішення, негайний доступ до його електронної копії та синхронне внесення змін до реєстру можуть свідчити про виконання суддею визначеної ролі у спільному механізмі [1; 15].

Процесуальна придатність цифрових відомостей залежить від законного способу їх одержання. Кримінальний процесуальний кодекс України передбачає огляд, тимчасовий доступ до речей і документів, обшук, копіювання інформації з комп'ютерної системи, негласні слідчі (розшукові) дії та експертне дослідження [4]. Матеріали оперативно-розшукової діяльності та результати негласних слідчих (розшукових) дій можуть використовуватися у доказуванні лише за дотримання компетенції, підстав, порядку санкціонування, меж проведення та належного процесуального оформлення [10; 16]. Спосіб отримання повинен відповідати природі джерела та інтенсивності втручання. Доступ до персонального пристрою або приватного облікового запису судді не може підмінятися загальним дозволом на пошук будь-якої компрометувальної інформації.

Допустимість необхідно відрізняти від достовірності. Навіть законно одержані дані не підтверджують конкретної обставини, якщо не встановлено їх походження, автентичність і цілісність [14]. У протоколі слід фіксувати технічні характеристики джерела, спосіб доступу, послідовність копіювання, назви та розміри файлів, часові мітки, метадані, використане програмне забезпечення і контрольні геш-значення. Первинна копія повинна зберігатися незмінною, а дослідження проводитися на робочій копії. Сторони захисту мають відкриватися не лише вибрані повідомлення чи знімки екрана, а й матеріали, необхідні для перевірки повноти контексту, способу атрибуції, незмінності даних і безперервності їх збереження.

Спеціальний порядок повідомлення судді про підозру вимагає, щоб цифрові відомості утворювали конкретну й узгоджену сукупність, яка об'єктивно пов'язує особу з визначеним кримінальним правопорушенням [7; 9; 12]. Недостатньо послатися на незаконність рішення та додати окремі факти комунікації. Обґрунтована підозра має пояснювати, які дані підтверджують обізнаність судді, у чому полягала його роль, яким був зв'язок між процесуальною дією і заволодінням майном та чому відхиляються правдоподібні незлочинні пояснення. Для обвинувального вирoku така модель повинна бути підтверджена допустимими і достовірними доказами поза розумним сумнівом, а не лише високою ймовірністю узгодженої поведінки.

Отже, доказування умислу та ролі судді у рейдерському захопленні доцільно будувати на п'яти взаємопов'язаних компонентах: інформаційній обізнаності; позапроцесуальній комунікації; нетиповій процесуальній поведінці; синхронізації судових, реєстраційних і фінансових подій; мотиві або вигоді. Жоден із них не має наперед установленної сили. Висновок про умислу співучасть є обґрунтованим лише тоді, коли цифрові дані отримано законно, підтверджено їх походження та незмінність, забезпечено змагальну перевірку, виключено обґрунтовані альтернативні пояснення і встановлено конкретний функціональний внесок судді у заволодіння майном. Такий підхід одночасно підвищує ефективність розслідування рейдерства та захищає незалежність правосуддя від необґрунтованого кримінального переслідування.

Список використаних джерел

1. Кальман О. Г., Погорєцький М. А. Рейдерство: причини та заходи протидії. *Вісник Запорізького юридичного інституту Дніпропетровського державного університету внутрішніх справ*. 2009. № 3. С. 150–160.
2. Конституція України від 28 черв. 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
3. Кримінальний кодекс України: Кодекс України від 5 квіт. 2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

4. Кримінальний процесуальний кодекс України: Кодекс України від 13 квіт. 2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
5. Погорецький М. А. Цифрові (електронні) докази та цифрова (електронна) форма доказів: розмежування понять і його значення для кримінального процесуального доказування. *Аналітично-порівняльне правознавство*. 2026. № 1. Ч. 3. С. 115–125. DOI: <https://doi.org/10.24144/2788-6018.2026.01.3.18>
6. Погорецький М. А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. *Аналітично-порівняльне правознавство*. 2025. № 5. Ч. 3. С. 239–256. DOI: <https://doi.org/10.24144/2788-6018.2025.05.3.37>. URL: https://app-journal.in.ua/wp-content/uploads/2025/10/APP_05_2025_part-3-2.pdf
7. Погорецький М. А., Гринюк В. О. Повідомлення судді про підозру: проблемні питання правового регулювання, теорії та практики. *Вісник кримінального судочинства*. 2018. № 2. С. 58–71. URL: <https://vkslaw.com.ua/index.php/journal/article/view/272/244>
8. Погорецький М. А., Гриценко І. С. Судова влада в Україні: до визначення поняття. *Право і суспільство*. 2012. № 2. С. 23–27. URL: http://nbuv.gov.ua/UJRN/Pis_2012_2_8
9. Погорецький М. А., Польовий О. Л., Яновська О. Г. Гарантії суддівської незалежності при притягненні суддів до юридичної відповідальності : монографія. Київ : ВД «Дакор», 2014. 308 с. URL: <https://ir.library.knu.ua/handle/15071834/8488>
10. Погорецький М. А., Старенький О. С. Негласні слідчі (розшукові) дії як засоби отримання доказів: окремі проблемні питання. *Право України*. 2018. № 8. С. 85–106. URL: http://nbuv.gov.ua/UJRN/prukr_2018_8_9
11. Погорецький М. А., Шеломенцев В. П. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.
12. Про судоустрій і статус суддів: Закон України від 2 черв. 2016 р. № 1402-VIII. URL: <https://zakon.rada.gov.ua/laws/show/1402-19#Text>
13. Рішення Конституційного Суду України від 11.06.2020 № 7-р/2020 у справі щодо відповідності Конституції України (конституційності) статті 375 Кримінального кодексу України. URL: <https://zakon.rada.gov.ua/laws/show/v007p710-20#Text>
14. Романюк В. В., Абламський С. Ю. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека*. 2024. № 2 (93). С. 140–150. DOI: <https://doi.org/10.32631/pb.2024.2.13>
15. Сергєєва Д. Б. Розслідування рейдерських захоплень у системі кримінальних правопорушень проти власності: процесуальні та криміналістичні проблеми. *Вісник кримінального судочинства*. 2026. № 1. С. 217–246. DOI: <https://doi.org/10.59835/2413-5372.2026.1/217-246>
16. Шумило М. Є., Погорецький М. А. Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах: теоретичний та практичний аспекти. *Вісник Луганського інституту внутрішніх справ*. Луганськ : РВВ ЛІВС, 2001. Вип. 3. С. 199–209.

Співак Марина Вікторівна, професор кафедри адміністративного права та процесу НАВС, доктор політичних наук, професор

СИСТЕМНА ЕРОЗІЯ ПРАВ ЛЮДИНИ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ: НОВІ ЗАВДАННЯ ДЛЯ ПРАВООХОРОННОГО СЕКТОРУ

Російська агресія проти України поставила перед вітчизняною системою архітектури безпеки безпрецедентний виклик – необхідність жорсткого захисту суверенітету та одночасного збереження демократичного правопорядку. В умовах воєнного стану особливої актуальності набуває дослідження явища «системна ерозія прав людини» – процесу поступового, часто латентного, звуження й деградації фундаментальних юридичних гарантій під приводом безпекової доцільності. Ключова роль у забезпеченні цього балансу належить правоохоронним органам, які безпосередньо комунікують із громадянським суспільством та реалізують державний примус. Вираз «системна ерозія прав людини» (systemic erosion of human rights) можна знайти у звітах міжнародних організацій, де описується поступовий занепад правових стандартів під тиском війни, авторитаризму чи відсутності реформ.

У 2023 році Комісар Ради Європи з прав людини Дуня Міятович, досліджуючи феномен ерозії прав людини в Україні, наголошувала, що цей процес характеризується не лише кількісним зростанням порушень, а й поступовим запереченням самої легітимності правових стандартів. У контексті національної безпеки України, ерозія проявляється у «звиканні» правоохоронної системи до ігнорування процесуальних гарантій (ст. 3, 5, 6 Конвенції про захист прав людини і основоположних свобод (далі – ЄКПЛ) під впливом воєнного стану. Як зазначається у європейських безпекових звітах, нехтування принципами верховенства права державними суб'єктами веде до деградації демократичних інститутів, що, зрештою, послаблює внутрішню стійкість держави перед зовнішніми загрозами» [1].

У 2025 році осмислення природи ерозії прав людини у сучасній безпековій архітектурі Європи відображено у доповіді Комісара Ради Європи з прав людини М. О'Флаєрти. Згідно з європейським підходом, ерозія правових стандартів сьогодні полягає не лише у суто технічних процесуальних порушеннях, а у небезпечній готовності політичних та безпекових еліт частково відмовлятися від