DOI: 10.31359/2079-6242-2024-48-48
УДК 343.1

Н. В. Глинська, доктор юридичних наук, завідувачка відділом дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса, Національної академії правових наук України
ORCID ID: 0000-0001-5835-3798

Ю. С. Рєпіна, кандидат економічних наук, доцент, науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса, Національної академії правових наук України
ORCID ID: 0000-0002-3157-3181

РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ЯК МЕТОДОЛОГІЧНА ОСНОВА ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УКРАЇНІ: ДО ПРЕЗЕНТАЦІЇ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ (ЧАСТИНА 1. ТИПОЛОГІЗАЦІЯ РИЗИКІВ)*

Постановка проблеми. Обрання цифровізації кримінального провадження (далі – ЦКП) одним з основних векторів трансформації кримінальних процесуальних правовідносин повністю відповідає об'єктивній реальності та зумовлюється чисельністю позитивних очікувань для національної кримінальної юстиції після її запровадження. Останні – різнопланові, чи різноспрямовані, такі що є цінними як у контексті забезпечення гарантій справедливої процедури, зокрема, права доступу до правосуддя, прозорості, швидкості та оперативності, так і в контексті інтегрального публічного інтересу щодо підвищення ефективності діяльності суб'єктів кримінального провадження при вирішенні його завдань.

Разом із тим, як правило, кожне явище у цивілізованому суспільстві має дві сторони: позитивну і негативну. Ба більше, саме цифрові технології в яскравих кольорах здатні проілюструвати це твердження. З одного боку, їх масштабне впровадження в загальносоціальному форматі обіцяє якісний прогрес щодо усіх напрямів суспільного буття та звільнення людей від рутинної праці. А з другого, супутні цифровізації проблеми у разі її не контрольованості здатні звести нанівець увесь очікуваний позитивний ефект[2].

Беручи до уваги інтрузивний характер кримінального провадження, запровадження цифрових технологій у таку царину має бути контрольованим та виваженим з огляду на пов'язані із діджиталізацією потенційні чи імовірні негативні наслідки, приховані небезпеки для охоронюваних законом цінностей.

Відтак, доктринальний розгляд питань щодо ризиків реалізації норм кримінального процесуального права в перебігу ЦКП надасть теоретично

[1] *Примітка.* Стаття презентує результати дослідження, проведеного науковцями Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України в рамках фундаментальної теми «Теоретико-правові проблеми цифровізації кримінального провадження в Україні» (науковий керівник – Глинська Н. В.).

[2] Глинська Н. В. 'Ризик-орієнтований підхід до цифровізації кримінального провадження: окремі питання концептуалізації' *Теорія та практика протидії злочинності у сучасних умовах* : збірник тез Міжнародної науково-практичної конференції (3 листопада 2023 року) 58–67.

обґрунтовані пропозиції щодо оптимізації процесу ЦКП, а, отже, забезпечить розвиток кримінальної юстиції в Україні відповідно до вимог сучасності.

Висловлене зумовлює доцільність екстраполювання на процес ЦКП популярної у світі концепції ризик-орієнтованого підходу (далі – РОП) як засобу зниження ризику виникнення кризових явищ і розроблення державних програм у галузі ЦКП із запобігання небажаним подіям і їх ліквідації (далі – РОП ЦКП). Впровадження РОП ЦКП допоможе оцінити ризики, розробити й впровадити ефективні заходи з їх уникнення та мінімізації, а, отже, визначити й реалізувати пріоритетні напрями ЦКП.

Аналіз останніх досліджень і публікацій. Проблема цифровізації є предметом вивчення багатьох наук – як комп'ютерних, що є очевидним, так і суспільно-гуманітарних, предметні області яких відчувають на собі вплив новітніх технологій, а тому потребують відповідних змінюваній реальності досліджень. Так, окремі питання використання цифрових технологій під час кримінального провадження були предметом дослідження таких українських науковців, як: В. Білоус, В. Бірюков, В. Голубєв, М. Гуцалюк, О. Жученко, О. Капліна, М. Карчевський, О. Колотило, Є. Лук'янчиков, Т. Михальчук, А. Молдован, Т. Павлова, А. Рибченко, М. Смирнов, О. Торбас, В. Уваров, І. Хараберюш, В. Хахановський, С. Чернявський, Г. Чигрина, С. Шаренко та ін. Утім, нечисельними є монографічні дослідження, що присвячені саме проблематиці цифровізації у царині кримінального провадження. Серед них слід вказати на праці А. Столітнього, Д. Цехана, Д. Літвекича. На особливу увагу заслуговують останні монографічні дослідженні, зокрема, «Використання цифрової інформації в кримінальному процесуальному доказуванні» (А. Скрипник), «Права людини в умовах цифрової трансформації суспільства» (за редакцією Д. Лученка). Упровадженню сучасних технологій у судочинство присвячені монографічні роботи О. Бринцева, Н. Голубєвої, наукові статті П. Казакевич, Н. Кушакової-Костицької, В. Мильцевої, М. Смоковича та ін. Теоретико-прикладні питання використання новітніх технологій у національній судовій системі розглядались багатьма фахівцями, серед яких: Я. Берназюк, О. Кібенко, І. Міщенко, П. Пушкар та ін. Перспективам і особливостям застосування технологій штучного в кримінальному процесі присвячені наукові публікації таких науковців, як І. Басиста, О. Верхогляд-Герасименко, О. Капліна, І. Крицька, А. Туманянц, Ж. Удовенко та ін.

У XX ст. з'явилось нове поняття «суспільство ризику», пов'язане з ім'ям видатного німецького соціолога У. Бека та подальшими теоріями Н. Лумана, також німецького соціолога. Вивчення ризиків, ризик-орієнтованого підходу здебільшого цікавлять фахівців з економіки та управління, в тому числі державного. Водночас з'явились дослідження вітчизняних науковців-правників за напрямом вивчення юридичних ризиків у різних галузях права, зокрема, Д. Безубова, М. Великанової, І. Волосенко. Крім того, на ризиках у кримінальному провадженні акцентували увагу Л. Лобойко, С. Касапоглу, О. Шило.

Однак варто також зазначити, що незважаючи на чисельність наукових публікацій за тематикою ЦКП, наразі через відсутність інтегрованого науковоприкладного погляду на проблему, пов'язану із ЦКП, можна констатувати, що рівень вивчення проблеми ЦКП не відповідає запиту суспільства щодо концептуалізації цифрової трансформації кримінального провадження та створення доктринального підґрунтя майбутнім законодавчим ініціативам. Саме тому науковцями Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України було проведено дослідження, результати якого наводяться в цій науковій статті. Метою дослідження є розробка концептуальних засад для застосування РОП на процес ЦКП, що, з одного боку, стане методологічною основою при формуванні правової основи діджиталізації кримінального судочинства на сучасному етапі соціально-правового розвитку суспільства в Україні, а також й оцінки чинного кримінального процесуального законодавства з точки зору критерію уникнення та мінімізації супутніх ризиків ЦКП, а з другого, – дозволить спрямувати правозастосовну практику на ефективне керування ризиками ЦКП шляхом їх уникнення та мінімізації.

Метою цієї публікації є презентація основних результатів, отриманих за підсумком проведеної наукової розвідки питання використання РОП як методологічної основи ЦКП (Частина 1 – «Висвітлення питання типологізації ризиків ЦКП як необхідної умови керування ними»). Тож перейдемо до демонстрації юридичній спільноті тих основних здобутків проведеного дослідження,

що на наш погляд, створюють методологічну основу для керування ризиками ЦКП на сучасному соціально-правовому етапі.

Виклад основного матеріалу. Перший блок таких результатів стосується типологізації ризиків ЦКП як неодмінної умови успішного керування ними.

За методологією РОП типологізація ризиків ЦКП та визначення факторів ризиків є вельми важливою, адже саме вплив на ці фактори чи їх врахування є необхідним засобом управління ризиками при прийнятті цифрових рішень.

Наголосимо, що метою процесу ЦКП є досягнення якісного результату у вигляді цифрової трансформації кримінального провадження (ЦТКП), що характеризується певним рівнем перетворення кримінальної процедури, зумовленим переходом до нових способів діяльності з використанням цифрових технологій, адаптацією до специфіки цифрового середовища (цифрової інформації). Причому ключовою характеристикою засобу отримання такого бажаного результату є реалізація процесу ЦКП у розумних межах – із дотриманням необхідного балансу між підвищенням ефективності розслідування й судового розгляду та забезпеченням прав і законних інтересів осіб у цій царині**.** Тож, ризики ЦКП – імовірні можливості небезпеки у вигляді отримання під час реалізації процесу ЦКП небажаних із точки зору досягнення зазначеної мети та виконання поточних завдань результатів у вигляді спричинення шкоди охоронюваним законам інтересам.

Потенційно ризикованою видається реалізація процесу ЦКП майже за всіма напрямами (векторами) ЦКП (як-от: перехід до електронного документообігу в царині кримінального провадження; запровадження єдиної інтегрованої (розумної) електронної системи органів кримінальної юстиції, поєднаної із загальнодержавними електронними реєстрами та базами даних (електронного кримінального провадження (ЕКП)); переведення процесуальної комунікації учасників кримінального провадження (створення єдиної цифрової платформи для комунікації) в електронну форму; розширення цифрового сегменту під час проведення слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій; використання (чи оперування) цифровою інформацією у доказуванні; розширення дистанційного правосуддя; використання технології штучного інтелекту в кримінальному провадженні), які відповідно виступають об'єктом ризику[1].

Стисло позначимо зміст основних якісних ризиків щодо кожного з виділених об'єктів.

1. ***При переведенні документообігу в царині кримінального провадження в електронну форму*** основними видами можливих негативних ефектів є блоки ризиків, пов'язані з: порушенням інформаційної безпеки електронного кримінального провадження (витік, втрата, пошкодження інформації, порушення її конфіденційності); створенням перешкод для ефективної реалізації прав учасників процесу (через недостатню цифрову компетентність та цифрову нерівність учасників процесу, належність учасників провадження до інклюзивної групи тощо); зайвим дублюванням процесуальних документів через гібридний документообіг, а тому додатковим навантаженням на органи кримінальної юстиції; додатковими процесуальними витратами часового ресурсу; втратою доказової сили документів, виготовлених в електронному вигляді через невизначеність закону щодо оригінальності документу; ін.

Із приводу створення перешкод для ефективної реалізації прав учасників процесу (через недостатню цифрову компетентність та цифрову нерівність учасників процесу, належність учасників провадження до інклюзивної групи тощо), про що ми вказували раніше в публікаціях, котрі передували цій роботі, зазначимо, що «пріоритетність цифрового формату має корелювати із гнучкістю щодо конкретного випадку, коли у конкретній правовій ситуації найбільш прийнятним та доцільним з урахуванням основного вектору цифровізації – прав та свобод учасників процесу – буде обрання саме паперового формату документування. Зміни до регламенту у зв'язку з цифровізацією судочинства, у тому числі актів і документів, мають бути внесені з дотриманням права на справедливий суд[2]».

Оскільки для теперішнього гібридного документообігу неминучою є процедура переведення письмових матеріалів кримінального провадження

[1] Глинська Н. В., Клепка Д. І. 'Цифровізація кримінального провадження: окремі аспекти концептуалізації (частина 1)' (2022) 43 Питання боротьби зі злочинністю 24–44 <http://pbz.nlu.edu.ua/issue/view/15815>

[2] Глинська Н. В. 'Правовий аспект запровадження режиму paperless в кримінальному провадженні України' (2023) 45 Питання боротьби зі злочинністю 86–96 < http://pbz.nlu.edu.ua/article/view/288509 >

в електронний формат (оцифрування матеріалів провадження), слід окремо враховувати можливі негативні правові наслідки, зокрема, у вигляді втрати юридичної сили оцифрованих документів, порушення права на захист через об'єктивні складності передання всіх суттєвих рис матеріальних об'єктів –речових доказів та ін. Такі ризики виникають як через технічні причини (погана якість, відсутність необхідних пристроїв), так і через недостатню правову визначеність, зокрема, у частині оригінальності цифрових копій, об'єктивних складнощів оцифрування матеріальних об'єктів.

У контексті зайвого дублювання електронних документів паперовими не можна відкладати, по-перше, визначення в законі порядку конвертації процесуальних документів з однієї форми в іншу (зокрема, у законі мають бути прямо передбачені випадки, коли електронний процесуальний документ повинен бути роздрукований і приєднаний до паперового кримінального провадження, тощо), який попередить невиправдане дублювання електронних процесуальних документів на паперових носіях; а по-друге, перегляд на стратегічному рівні доцільності дублювання фіксації певних процесуальних дій у паперовому протоколі.

2. ***При запровадженні єдиної інтегрованої (розумної) електронної системи органів кримінальної юстиції, поєднаної із загальнодержавними електронними реєстрами та базами даних, – електронного кримінального провадження (ЕКП))*** – основними видами можливих негативних правових ефектів є блоки ризиків, пов'язані із порушенням інформаційної безпеки електронного кримінального провадження (витік, втрата, пошкодження інформації, порушення її конфіденційності).

Оскільки невіддаленою у часі перспективою є повне перенесення процесуальної комунікації учасників провадження у кіберпростір на базі відповідних інформаційних систем та ситуація, коли основний сегмент доказового фонду кримінального провадження складатиме цифрова інформація, то забезпечення інформаційної та кібербезпеки кримінального провадження стає пріоритетним напрямом науково-технічної діяльності. Він вимагає істотної уваги та зусиль як з боку держави, так і безпосередньо з боку органів кримінальної юстиції. Отже, активного дискурсу набуває потреба в комплексному забезпеченні інформаційної безпеки електронного кримінального провадження – стану захищеності інформаційного середовища електронного кримінального провадження (апаратного і програмного сегментів та суб'єктів кримінального провадження), що забезпечує його функціонування, формування, використання і розвиток для ефективного виконання завдань кримінального провадження (далі – ІБЕКП).

Для ідентифікації ризиків інформаційної безпеки кримінального провадження (далі – ІБКП) необхідно враховувати загальні спектри інтересів інформаційної безпеки (далі – ІБ), які можна поділити на такі категорії, як порушення цілісності, конфіденційності, доступності та спостереженості – важливих аспектів якості процесуальної інформації.

Звичайно, управління ризиками ІБКП має відбуватись насамперед на державному рівні у контексті реалізації державної політики ІБ. Інакше кажучи, управління більшістю ризиків ІБКП знаходиться за межами царини кримінальних процесуальних відносин. Утім, існує коло чинників порушення ІБКП, що знаходяться вже в орбіті кримінальних процесуальних відносин та можуть бути керованими в процесі реалізації РОП ЦКП. Зокрема, поміж технічних причин та можливих кібератак, порушенням ІБКП може бути протиправне втручання в роботу ЕКП учасників провадження, що матиме наслідок – витік, втрату, підробку (фальсифікацію, внесення незаконних змін) матеріалів кримінального провадження; неконтрольоване зберігання цифрової інформації тощо.

Зауважимо, що потенційні наслідки порушення ІБКП є вагомими для всіх охоронюваних законом інтересів. Йдеться про створення перепон для: ефективного розслідування (зокрема, витік інформації про проведення обшуку – зрив проведення слідчої дії), безпеки учасників провадження (розголошення інформації щодо особи свідка, який перебуває під захистом, персональних даних), реалізації завдання повного та об'єктивного розслідування через необ'єктивну інформацію. Фальсифікація матеріалів кримінального провадження може призвести до незаконних обмежень прав і свобод учасників провадження (незаконних затримань, застосування запобіжних заходів та інших заходів забезпечення кримінального провадження, а також інших порушень прав учасників провадження). Як влучно наголошують Б. Щур та І. Басиста, «судовий процес, в основі якого ле-

жать інформаційні технології, має бути особливо захищеним, бо може бути «зруйнований»[1].

3. ***Ризики використання цифрової інформації у доказуванні (збиранні, закріпленні та зберіганні).*** Збирання та зберігання цифрової інформації (перспективних доказів) у кримінальному провадженні є вкрай чутливим до можливих ризиків порушення ІБ *(«безпекові» ризики у контексті цифрового доказування*), наслідками чого може стати втрата, пошкодження та маніпуляції з цифровими даними, «ризик зникнення цих даних (через припинення функціонування відповідного цифрового сховища, в якому вони розміщені; припинення доступу до цього цифрового сховища; видалення цих даних особою, яка має на це право, або алгоритмом, який має на це дозвіл, чи з технічних причин, наприклад, внаслідок дії шкідливого коду або апаратною збою) та ризик зміни цих даних із тих самих причин[2]».

Поміж позначених «безпекових» ризиків перед цариною кримінального провадження постають виклики, пов'язані з: можливою недостовірністю цифрової інформації (діпфейки, спотворення цифрової інформації); порушенням цілісності (автентичності) цифрового доказу; втратою (знищенням) доказової інформації; втратою доказового значення зібраної цифрової інформації через недотримання/порушення кримінальної процедури її збирання, фіксації, зокрема, через непропорційне втручання в права та свободи особи під час збирання даних у кіберпросторі (*ризик недопустимості використання зібраної цифрової інформації у доказуванні*); неправильною оцінкою цифрової інформації (зокрема, «латентної» цифрової інформації – інформації, що недоступна для безпосереднього представлення та дослідження під час судового розгляду; в ході її збирання та вивчення необхідно залучити експерта та провести експертизи (в тому числі з метою виявлення знищеної інформації, встановлення фактів несанкціонованого доступу до неї, її зміни, спотворення тощо).

Як відомо, цифрова інформація є надто вразливою через те, що може бути легко змінена чи знищена. При цьому ризики надійного зберігання електронних доказів здебільшого зводяться не лише до факторів технічного характеру (наприклад, енергозалежність пристроїв (у випадку розрядження пристрою або недостатньої за обсягом пам'яті система накладає (записує) нову інформацію на місце попередньої, що може призвести до знищення доказів); комп'ютерна пам'ять може бути пошкоджена або знищена під впливом фізичних факторів (високий рівень вологості, висока температура) та електромагнітних хвиль тощо)), а й до можливих протиправних дій, спрямованих на знищення чи спотворення цифрової інформації. Тож гарантії надійності збереження електронної інформації полягають не лише у площині високої якості технологій, а й у заданні нормативного алгоритму такого зберігання, зокрема, архівації інформації, фіксації ланцюга збереження доказу у відповідному протоколі (фіксування покрокового шляху огляду, збереження та архівації цифрової інформації із мережі Інтернет тощо). З огляду на це слушною є думка науковців про «необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів справи. Зокрема, на рівні з традиційними правилами поводження із документами, необхідно враховувати технічні особливості збирання, зберігання та використання інформації[3]».

4. Блок ризиків, пов'язаних із ***переведенням процесуальної комунікації учасників кримінального провадження в електронну форму***. Основними очікуваними позитивними ефектами переведення процесуальної комунікації учасників провадження в digital-площину, зокрема, онлайн-ініціювання кримінального провадження, дистанційного ознайомлення з матеріалами провадження, – ефективний доступ до правосуддя, ефективний доступ сторони захисту до матеріалів провадження, оперативність судово-контрольних проваджень тощо.

---

[1] Щур Б. В., Басиста І. В. 'Судове провадження у режимі відеоконференції та трансляція з іншого приміщення, у тому числі, яке знаходиться поза межами приміщення суду: окремі підходи до розуміння та проблеми реалізації' (2022) 29 (3) Вісник Національної академії правових наук України 242–267.

[2] Пашковський М. І. 'Використання Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних під час досудового розслідування колабораціонізму: аналіз судової практики' *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму* : матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 лип. 2023 р.) 168–172.

[3] Хижняк Є. С. 'Особливості огляду електронних документів під час розслідування кримінальних правопорушень' (2017) 4 (58) Держава та регіони 80–85.

Наразі зроблено лише точкові кроки в цьому напряму[1], тому поки що ми не маємо можливості оцінити реалізацію цього вектору на практиці. Втім, у контексті прогнозування зазначимо, що поміж ризиків суто безпекового характеру, правова стратегія переведення процесуальної комунікації в електронну форму має враховувати та упереджувати чи мінімізувати небажані правові наслідки. Зокрема такі, як зниження ефективності чи взагалі унеможливлення реалізації права особи на доступ до правосуддя та захист. Ризики для доступу до правосуддя виникають через неналежний рівень прозорості та непослідовність алгоритмізації порядку користування онлайн платформами для звернення з заявами про вчинене кримінальне правопорушення), а для захисту – через відсутність чіткого нормативного алгоритму процесуальної комунікації сторони захисту із особами, що ведуть провадження, цифрову некомпетентність учасників провадження та відсутність альтернативних форм комунікації.

5. ***Розширення цифрового сегменту під час проведення слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій.***

Даний вектор ЦКП передбачає *певну процесуальну адаптацію кримінальної процедури до цифрового середовища* як об'єкта чи предмета вчинення кримінальних правопорушень. І в цьому сенсі необхідно здійснити оцінку відповідності наявних процесуальних механізмів документування та розслідування кримінальних правопорушень, вчинених у кіберпросторі чи із використанням цифрових даних, на предмет їх ефективності. Результатом такої аналітичної діяльності має стати певна нормативна та праксеологічна «корекція» кримінальної процесуальної діяльності. Така адаптація має відбуватися з урахуванням як блоку ризиків, пов'язаних із непропорційним втручанням в права та свободи особи (зокрема, права на приватність), порушенням права на рівність, презумпцією невинуватості *під час «цифрового розслідування»*[2], так і блоку ризиків, пов'язаних із нівелюванням доказового значення зібраної інформації через недотримання належної правової процедури.

6. Блок ризиків, пов'язаний із ***дистанційною формою проведення окремих процесуальних дій чи судового розгляду.*** У тенденції розширення можливостей проведення процесуальних дій у режимі відеоконференції слід убачити технічні ризики, що, перш за все, пов'язані із неналежною якістю дистанційного зв'язку, та/чи порушенням ІБКП під час його використання, а, по друге, самі такі дії складають блок негативних правових наслідків, обумовлених специфікою реалізації кожної із них в онлайн режимі (є різними в залежності від характеру дистанційної процедури).

Зазначений напрям ЦКП є не лише формою осучаснення кримінальної процедури, адже він насамперед спрямований й на підвищення ефективності реалізації права особи на справедливий судовий розгляд. Утім, за певних обставин зазначена цінність, що заважає розширенню дистанційності у кримінальному провадженні, може опинитися під загрозою.

Зауважимо, що наслідки технічних недоліків у конкретному провадженні безпосередньо можуть

[1] *Примітка.* Зокрема, 1 грудня 2023 року зроблено крок до переведення процесуальної комунікації сторони обвинувачення зі слідчими суддями в системі антикорупційних органів. ВАКС розпочав експлуатацію інформаційно-телекомунікаційної системи досудового розслідування (іКейс) та прийматиме клопотання про дозвіл на проведення обшуку житла чи іншого володіння особи від детективів НАБУ та прокурорів САП в електронному форматі. Як обіцяють розробники іКейс, після закінчення тестування системи, налагодження процесів інтеграції та обміну даними, побудови захищених каналів зв'язку та розбудови технічних спроможностей, між НАБУ, САП та ВАКС матеріалами кримінальних проваджень у зазначеній категорії клопотань можна буде обмінюватися за декілька секунд. Це значно зекономить ресурси, зокрема, час, матеріально-технічні потреби для обробки та зберігання документів. Надалі триває розвиток та вдосконалення системи іКейс, аби в найближчій перспективі сторона захисту змогла долучитися до технічної можливості роботи з електронними матеріалами кримінального провадження на всіх етапах його здійснення.

[2] *Примітка.* Під «цифровим досудовим розслідуванням» (ЦДР) авторами розуміється досудове розслідування, пов'язане зі збирання, фіксацією, зберіганням, оцінкою та використанням інформації в електронному (цифровому) форматі. ЦДР зумовлює низку особливостей та викликів у кримінальній процесуальній діяльності: широкий спектр цифрових доказів, таких як електронні листи, текстові повідомлення, записи телефонних розмов, дані з GPS-навігаторів, відеозаписи, зображення, аудіофайли, дані із соціальних мереж тощо; використання спеціальних технічних засобів, програмного забезпечення та методів для збирання й аналізу цифрових доказів; необхідність спеціальних знань у сфері інформаційних технологій та цифрової криміналістики. Важливою проблемою ЦДР є забезпечення кібербезпеки та захисту цифрових доказів від фальсифікації, знищення або несанкціонованого доступу, дотримання законності та прав людини під час збирання і використання цифрових доказів. Розслідування цифрових злочинів часто потребує міжнародного співробітництва, адже цифрові докази можуть бути розміщені на серверах у різних країнах світу. З огляду на те, що ЦДР є потужним інструментом для розслідування та запобігання злочинам у сучасному цифровому світі, для його ефективного та правомірного використання необхідно вирішити низку викликів, пов'язаних із забезпеченням законності, дотриманням прав людини та міжнародним співробітництвом.

призвести до визнання порушення статті 6 ЄКПЛ[1]. З урахуванням того, що *ризики порушення основних вимог справедливої процедури через застосовування режиму ВКЗ* докладно розглянуті нами у контексті формування стратегії розвитку дистанційного провадження, на цих сторінках лише наведемо їх приблизний перелік. До основних ризиків порушення вимог справедливої процедури через застосовування режиму ВКЗ належать, зокрема: зниження ефективності реалізації права на захист (через відсутність конфіденційного спілкування із захисником, труднощі у залученні перекладачів, позбавлення можливості оскарження результатів дистанційного доказування тощо); ризики недотримання принципу рівності сторін (зокрема, через труднощі проведення дистанційного перехресного допиту); перешкоджання повноті та всебічності дослідження обставин справи сторонами та судом (зокрема, через відсутність повноцінного особистого сприйняття судом показань обвинуваченого, свідків, потерпілого чи експертів та можливості спостереження за невербальними сигналами з метою виявлення фактів стороннього впливу на дистанційних учасників Із боку третіх осіб (під час дачі показань існує ризик неправильної оцінки свідчень судом та як наслідок – прийняття несправедливого рішення); недотримання принципу безпосередності при дистанційному доказуванні (через об'єктивну ускладненість проведення дистанційного судового огляду матеріальних об'єктів – речових доказів); недостовірної ідентифікації особи учасника провадження та автентичності інформації, що надається сторонами в електронному вигляді для дослідження у ході дистанційного кримінального провадження та ін.

Попередньо наголосимо на необхідності подальшого просування у бік розширення дистанційного правосуддя, зокрема, за векторами спрощення вимог до локації учасників конференції та допущення використання ними власних технічних засобів, з огляду на його беззаперечні переваги у контексті оперативності, процесуальної економії та усунення ризиків втрати важливих доказів у справі[2].

7. ***Блок ризиків при застосуванні технологій штучного інтелекту (далі – ШІ)*** в кримінальному судочинстві, який наразі видається найбільш ризикованим з усіх напрямів ЦКП. Незважаючи на вигоди, які надає використання ШІ у кримінальній юстиції, водночас виявляються потенційні ризики: (1) непрозорість прийняття рішень, (2) різні типи дискримінації, (3) втручання в приватне життя, (4) виклики для захисту (а) персональних даних, (б) людської гідності та (в) свободи слова й інформації. Вони посилюються в секторі правоохоронних органів і кримінального судочинства, оскільки здатні вплинути на презумпцію невинуватості, основні права на свободу особи та особисту недоторканність, а також на ефективний засіб правового захисту та справедливий суд[3].

У квітні 2021 р. Європейська комісія вперше запропонувала нормативне регулювання ШІ в ЄС, яким передбачається ранжувати технології ШІ за рівнем ризику (неприйнятний, високий, обмежений тощо) залежно від забезпечення відповіднос-

[1] *Примітка.* Адже у контексті гарантування права особи на ефективний захист особа має право не лише бути присутнім, а й також слухати та стежити за процесом. Такі права випливають із самого поняття змагальності, а так само можуть бути виведені з гарантій, що містяться в підпунктах (c), (d) і (e) пункту 3 статті 6 (Стенфорд проти Сполученого Королівства, § 26). Відповідно погана акустика в залі суду та проблеми зі слухом можуть стати причиною порушення статті 6 (§ 29) (Посібник щодо статті 6 Європейської конвенції з прав людини. 2021, § 154 [European Commission for the efficiency of Justice (2021) Guidelines on videoconferencing in judicial proceedings : Document adopt. by the CEPEJ at its 36th plenary meeting (16 and 17 June 2021), p. 28. Retrieved from https://www.echr.coe.int/documents/ guide_art_6_criminal_eng.pdf]. Отже, при використанні відеозв'язку під час провадження необхідно забезпечити технічно безперешкодну можливість заявнику стежити за провадженням та бути заслуханим, і, як зазначалося раніше, також ефективну та конфіденційну комунікацію з адвокатом без свідків (Marcello Viola проти Італії, §§ 63–67; Asciutto проти Італії, §§ 62–73; Sakhnovskiy проти Росії [ВП], § 98).

[2] *Примітка*. Підтвердженням реалізації цієї стратегії є довгоочікуване для кримінальної процедури унормування можливості учасників процесу приймати участь у провадженні дистанційно з використанням власних технічних засобів. Так, 14 березня 2024 р. Президентом України підписано Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-комунікаційної системи (ЄСІКС) № 3604-IX. Зазначеним Законом передбачено, зокрема, можливість участі адвоката, свідка чи потерпілого в судовому засіданні поза приміщенням суду з телефону чи планшету, хоча такий формат може бути застосовний у разі введення воєнного стану або під час карантину, встановленого Кабінетом Міністрів України.

[3] European Parliament (2021). Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters : Resolution of 6 October 2021 (2020/2016(INI)). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021IP0405

ті систем ШІ критеріям: безпечності, прозорості, доступності для відстеження, недискримінаційності, екологічної чистоти, контрольованості людьми[1].

Щодо джерел (факторів) ризиків ЦКП

Якісна характеристика ризику була б не повною без врахування джерел (факторів) ризику – певних явищ, предметів, процесів, що зумовлюють існування ризиків, є їх причинами та в управлінській літературі визнаються як одна з ключових компонент складу ризику. Адже управління ризиками суб'єктом як на правотворчому, так і правозастосовному рівні має враховувати об'єктивні можливості впливу певної системи заходів (правових, організаційних, технічних) на ті обставини, що зумовлюють виникнення ризиків ЦКП, з метою мінімізації їх впливу (зокрема, у спосіб встановлення чи зміцнення необхідних нормативних компенсаторних механізмів).

Фактори чи джерела ризиків за своєю функціональною структурою та природою є різнорідними та різнорівневими, мають об'єктивний та суб'єктивний характер. *Внутрішніми об'єктивними факторами* чи джерелами ризику ЦКП є сукупність явищ правового, технічного й організаційного характеру, що безпосередньо стосуються тих чи інших напрямів ЦКП або «знаходяться в межах самої системи, що є об'єктом ризику, і зумовлюють виникнення стану ризику»[2]. До них, зокрема, слід віднести недосконаліть правового регулювання процесу ЦКП (невідповідність кримінального процесуального законодавства правовим стандартам), неузгодженість (різницю) судової практики, відсутність належної інтеграції інформаційних систем, а, отже, неналежний рівень процесуальної комунікації, непрозорість технологій ШІ, інклюзивність певної категорії громадян; різний інтелектуально-освітній рівень користувачів судової системи та ін.

Окремим фактором, котрий, на жаль, залишається актуальним, є неналежна *якість кримінального процесуального законодавства*.

У свою чергу, до *внутрішніх суб'єктивних факторів* ризику ЦКП можна віднести недостатність кадрів, які здатні працювати із цифровими комп'ютерними технологіями (неналежна цифрова компетентність правозастосувачів), низьку якість прийнятих процесуальних цифрових рішень у конкретному провадженні, невиконання або неналежне виконання процесуальних обов'язків (зокрема, поверхневий аналіз фактичної ситуації кримінального провадження, в якому застосовуються цифрові технології, неналежна фіксація цифрових слідчих дій тощо).

Зовнішні фактори ризиків ЦКП *прямої дії* зводяться до сукупності явищ економічного, соціального, технологічного характеру. До них у контексті їх прямого впливу на ефективність ЦКП можна віднести, зокрема, економіко-соціальний розвиток, у тому числі рівень життя та освіченості населення, науково-технологічній розвиток, який визначає якість, поширеність та доступність цифрових технологій, політику ІБ тощо.

На нашу думку, більшістю ризиків ЦКП можна керувати лише на загальнодержавному управлінському рівні, за межами системи кримінального провадження. Саме такою виглядає об'єктивна реальність. Добре продумана, грамотна, із чітким та послідовним механізмом реалізації державна політика у напрямі цифровізації суспільства із визначеним пріоритетом інноваційного розвитку відіграє важливу роль у процесах зменшення масштабів викликів, з якими стикаються суб'єкти управління ризиками ЦКП.

У розвиток тематики ***типологізації ризиків ЦКП*** також зазначимо, що в юридичній літературі запропоновані класифікації ризиків за низкою інших критеріїв за: сферою виникнення; причинами виникнення; галузями права; видами виникнення; можливістю передбачення; суспільними відносинами виникнення тощо.

З урахуванням практичної спрямованості (керування ризиками ЦКП) недостатньо визначити лише якісні характеристики ризику. Незважаючи на те, що кількісні методи обмежено можуть бути застосовані в правовому дослідженні, втім, це не позбавляє сенсу здійснювати ***певну градацію ризиків за їх якісно-кількісним рівнем.***

Кількісною характеристикою небезпеки є квантифікація небезпек, яка визначає ступінь небезпеки або ризик. Нескінченно малий («нульовий») ризик свідчить про відсутність реальної

[1] EU AI Act: First Regulation on Artificial Intelligence / European Parliament website [News. Updated: 14-06-2023–14:06]. URL: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[2] Великанова М. М. 'Поняття та структурні елементи ризику: цивільно-правовий аспект' (2017) 45 Університетські наукові записки 76–86 < https://journals.indexcopernicus.com/api/file/viewByFileId/427972 >

небезпеки в системі, і навпаки: чим вищий ризик, тим вища реальність впливу небезпеки. Величина ризику визначається як відношення кількості подій із небажаними наслідками до максимально можливого їх числа за конкретний період часу[1]. Залежно від кількісної характеристики ризик можна розглядати за ступенем його припустимості: ризик, яким *можна нехтувати*, *допустимий, гранично допустимий, надмірний*. Однак досягти нульового рівня ризику, тобто абсолютної безпеки, на практиці неможливо.

Як інструмент ранжування та візуалізації ризиків із визначенням категорій наслідків і їх правдоподібності застосовується матриця ризиків[2]. Найпростіший варіант матриці ризиків використовує п'ятибальну шкалу 5х5 оцінки впливу (Таблиця 1) та правдоподібності (імовірності) цих ризиків. Так само є можливим використовувати матрицю 3х3 для меншої деталізації (наприклад, саме такою матрицею ризиків послуговується Державна судова адміністрація України для оцінки ризиків[3]). Наразі матриця ризиків є одним із найпоширеніших інструментів оцінювання ризику[4].

У правовій сфері застосування математичних методів і розрахунків зазвичай виявляється досить складним, а частіше й зовсім неможливим. Водночас це не позбавляє практичного сенсу наведення інструментів ранжування й аналізу ризиків, навпаки, націлює на пошук нових підходів до оцінки ризиків ЦКП.

Наприклад, перспективи використання ШІ в кримінальному судочинстві, які наразі широко дискутуються у науковому середовищі, мають узгоджуватися із ризиками для прав людини і засад кримінального провадження. Тому, якщо після аналізу й оцінювання ризику використання ШІ у кримінальному провадженні, наприклад, при застосуванні слідчим суддею, судом запобіжних заходів, рівень ризику для прав і свобод підозрюваного, обвинуваченого є недопустимим, забороняється застосовувати ШІ. Саме такий шлях регулювання ШІ із застосуванням ризик-орієнтованого підходу обрав ЄС в Законі про штучний інтелект[5], ініціатором якого виступила Європейська комісія[6]. Зазначений акт є яскравим прикладом ранжування ризиків та містить ризик-орієнтований підхід, за яким визначаються чотири рівні ризику для систем ШІ (неприйнятний, високий, обмежений, мінімальний/нульовий ризик), та встановлює суворі зобов'язання для їх використання. Критерієм для зарахування технології ШІ до певної категорії за рівнем ризику є її вплив на безпеку та гарантію прав людей і бізнеса.

У контексті практики розрахунку ризиків у кримінальному провадженні також доречно звернути увагу на існування системи оцінки ризиків при збиранні цифрової інформації, зокрема, з відкритих джерел. Як зазначає О. О. Торбас, джерело та фактична інформація повинні бути оцінені незалежно один від одного, тому вкрай важливо, щоб особа, яка заповнює звіт, добре знала систему оцінювання[7]. Управлінням ООН з наркотиків та злочинності розроблено посібник з аналітики «Кримінальна розвідка»[8], в якому для оцінка джерел та даних використовуються системи «4х4» і «6х6», що пропонуються науковцем до застосування:

---

[1] Див., напр.: Піскунова Л. Е., Прилипко В. А., Зубок Т. О. *Безпека життєдіяльності: підручник* (Академія, 2012) 224

[2] ДСТУ IEC/ISO 31010:2013 у Додатку В «Методи загального оцінювання ризику» містить п. В.29 «Матриця наслідків/імовірностей», у якому надається загальний огляд цього методу, його застосування, вхідних даних, процесу, вихідних даних, переваг та обмеженостей [ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику». URL: https://zakon.isu.net.ua/sites/default/files/normdocs/iso_31010.pdf].

[3] Додатки до Інструкції з організації та здійснення внутрішнього контролю в Державній судовій адміністрації України. URL: https://dsa.court.gov.ua/userfiles/media/ new_folder_for_uploads/dsa/dod_1_5_N284.pdf

[4] *Примітка.* На основі показників правдоподібності і впливу вона наочно демонструє рівень ризику. Більшість матриць ризиків має три області: область низької імовірності (зелена), яка вказує на те, що ризик події недостатньо високий або що вона достатньо контролюється; висока ймовірність (червона) – подія вимагає використання великої / більшої кількості зусиль для її зниження та середня, інша назва – ALARP (жовта), яка знаходиться між цими двома областями та зазвичай вважається, що будь-яка подія, котра потрапляє в цю область, є такою, яку слід відстежувати, але із мінімальним контролем.

[5] Artificial Intelligence Act: MEPs adopt landmark law : Press Releases 13-03-2024–12:25 URLhttps://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

[6] AI Act / An official website of the European Union. URL: ttps://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[7] Торбас О. О. *OSINT при розслідуванні кримінальних правопорушень : підручник*: (Видавництво «Юридика», 2024) 14.

[8] *United Nations Office on Drugs and Crime. Criminal Intelligence. Manual for Analysts. United Nations,* (April 2011) 96 <https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf>

Таблиця 1.

МАТРИЦЯ РИЗИКІВ ЦКП

ВПЛИВ	ПРАВДОПОДІБНІСТЬ					
		Майже неможливо	Малоймовірно	Середня	Можливо	Дуже можливо
	Дуже високий					
	Високий					
	Середній					
	Низький					
	Відсутній					

КАТЕГОРІЇ: Високий ризик; Середній ризик; Низький ризик

СИСТЕМА ОЦІНКИ 4x4

Таблиця 2.

ОЦІНКА ДЖЕРЕЛА

A	– жодних сумнівів щодо автентичності, достовірності, правдивості джерела; – попередні приклади повної надійності
B	– джерело, з якого була отримана інформація, в більшості випадків було надійним
C	– джерело, з якого була отримана інформація, в більшості випадків було ненадійним
X	– надійність джерела оцінити неможливо

Таблиця 3.

ОЦІНКА ІНФОРМАЦІЇ

1	– немає сумнівів у точності інформації
2	– інформація особисто відома джерелу, з якого вона отримується, але не відома аналітику, який її отримує; – логічна сама по собі; – узгоджується з іншою наявною інформацією
3	– інформація особисто джерелу невідома, але підтверджується іншою інформацією
4	– інформація особисто джерелу не відома та не може бути незалежно підтверджена

СИСТЕМА ОЦІНКИ 6x6

Таблиця 4.

НАДІЙНІСТЬ ДЖЕРЕЛА

A Повністю надійне	– жодних сумнівів щодо автентичності, достовірності, правдивості джерела; – попередні приклади повної надійності
B Зазвичай надійне	– певні сумніви щодо автентичності, достовірності, правдивості чи компетентності джерела (одне з перелічених); – попередні приклади відносної надійності
C Відносно надійне	– сумніви щодо автентичності, достовірності, правдивості чи компетентності джерела (два і більше перелічених); – попередні приклади періодичної надійності
D Зазвичай ненадійне	– явні сумніви щодо автентичності, достовірності, правдивості чи компетентності джерела; – попередні прикладі нерегулярної надійності
E Ненадійне	– впевненість у відсутності автентичності, достовірності, правдивості чи компетентності джерела; – приклади ненадійності
F	– неможливо оцінити

Таблиця 5.

ОЦІНКА ІНФОРМАЦІЇ

1 Підтверджено	– підтверджено іншими незалежними джерелами; – логічна сама по собі; – узгоджується з іншою інформацією
2 Вірогідно правда	– не була підтверджена незалежними джерелами; – логічна сама по собі; – узгоджується з іншою інформацією
3 Ймовірно	– не була підтверджена; – логічна сама по собі; – дещо узгоджується з іншою інформацією
4 Сумнівно правда правда	– не була підтверджена; – нелогічна; – сумнівна на момент отримання, хоча потенційно може бути правдивою
5 Неправдоподібно	– підтверджується протилежна інформація; – нелогічна сама по собі; – суперечить іншій інформації
6	– неможливо оцінити або/та не може бути незалежно підтверджена

Таким чином, аналізуючи джерело та інформацію, аналітики (котрими в орбіті кримінальної процедури виступають дізнавач, слідчий, прокурор, слідчий суддя та суд – *прим. авт. – Н. Г. та Ю. Р.*) присвоюють їм відповідні оцінки, а не описують власні роздуми щодо достовірності джерела чи правдивості інформації. Наприклад, оцінка А2 за системою «6х6» вказує на те, що така інформація фактично без застережень може використовуватися в розслідуванні, в той самий час оцінка С3 за системою «4х4» вимагає вкрай критичного ставлення до такої інформації[1].

Наведені матриці оцінки джерел та інформації (за фактичної наявності елементів вибірковості у збиранні доказів у справі) є важливим стратегічним інструментом для забезпечення судової перспективи здобутих доказів і попередження чи зниження ризиків, пов'язаних із можливою недостовірністю цифрової інформації.

Висновки. Підсумовуючи викладене, зазначимо, що метою виявлення вже вказаних та інших подібних ризиків не є намір гальмування процесу ЦКП, який, на наш погляд, виступає неминучим майбутнім, в якому буде розвиватися наше суспільство. Навпаки, ідентифікація можливих ризиків на кожному з виділених векторів ЦПК є необхідною умовою для системного управління такими ризиками як на правотворчому, так й правозастосовному рівнях. Інакше кажучи, потрібно розуміти, з якими загрозами ми маємо справу, та відповідно до їх змісту та рівня обирати надійні засоби їх убезпечення. Сприйняття ризику як об'єктивного супутника процесу ЦПК переводить правозастосувача у площину керування ним. Тож сам факт імовірної небезпеки не є червоним світлом для ЦКП, а вимагає системного підходу до управління такими небезпеками як під час стратегічної діяльності правозастосувача, так й під час тактичного правозастосування. У противному разі системна невирішеність цих питань може призвести до неефективності та уповільнення темпів розвитку ЦКП, реалізації «реакційної», а не стратегічної кримінальної процесуальної політики. Саме тому заслуговують на увагу запропоновані нами концептуальні засади для застосування ризик-орієнтованого підходу до процесу цифровізації кримінального провадження.

При цьому необхідність типологізації ризиків ЦКП зумовлюється пошуком засобу зниження ризику виникнення кризових явищ, що викликає необхідність розробки державних програм у галузі ЦКП із запобігання небажаним подіям та їх ліквідації. У свою чергу, подальше впровадження РОП ЦКП із метою оцінки ризиків, розробки й впровадження ефективних заходів з їх уникнення та мінімізації здатне допомогти визначити й реалізувати пріоритетні напрями ЦКП, що відповідатиме інтересам українського суспільства.

[1] Торбас О О 14–16.

REFERENCE

List of legal documents

Legislations

1. Artificial Intelligence Act: MEPs adopt landmark law : Press Releases [13-03-2024–12:25]. URL: https://www.europarl.europa.eu/news/en/press-room/202403 08IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (in English)
2. AI Act / An official website of the European Union. URL: ttps://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (in English)
3. European Commission for the efficiency of Justice (2021). Guidelines on videoconferencing in judicial proceedings : Document adopt. by the CEPEJ at its 36th plenary meeting (16 and 17 June 2021), p. 28. URL: https://www.echr.coe.int/documents/ guide_art_6_criminal_eng.pdf (in English)
4. European Parliament (2021). Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters : Resolution of 6 October 2021 (2020/2016(INI)). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021IP0405 (in English)
5. Dodatky do instruktsii z organizatsii ta zdiisnennia vnutrishnoho kontroliu v Derzhavnii cudovii admbnisratsii Ukrainu [Appendices to the Instructions on the organization and implementation of internal control in the State Judicial Administration of Ukraine] URL: https://dsa.court.gov.ua/userfiles/media/ new_folder_for_uploads/dsa/dod_1_5_N284.pdf (in Ukrainian)
6. DSTU IEC/ISO 31010:2013 «Keruvannia ryzykom. Metody zahalnoho otsinyuvannia rysyku» [SSTU IEC/ISO 31010:2013 «Management of risk. Methods of general risk assessment»] URL: https://zakon.isu.net.ua/sites/default/files/normdocs/ iso_31010.pdf (in Ukrainian)

Bibliography

Authored books

1. Piskunova L. Ye., Prylypko V. A., Zubok T. O. *Bezpeka zhyttieliialnosti : pidruchnyk* [Life safety: a textbook] (Akademiia, 2012) 224 (in Ukrainian)
2. Torbas O. O. *OSINT pry rozsliduvanni kruminalnyh pravoporushen : pidruchnyk* [OSINT in the investigation of criminal offenses: a textbook] (Yurydyka, 2024) 180 (in Ukrainian)

Non-authored books

3. *United Nations Office on Drugs and Crime. Criminal Intelligence. Manual for Analysts. United Nations* (April 2011) 96 < https://www.unodc.org/documents/ orga nized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf > (in English)

Journal aticles

4. Hlynska N. V., Klepka D. I. 'Tsyfrovizatciia kruminalnoho provadzhennia: okremi aspekty kontseptualizatsii (chastyna 1)' [Digitalization of criminal proceedings: certain aspects of conceptualization (part 1) (2022) 43 Pytannia borotbu zi zlochynnistiu 24–44 < http://pbz.nlu.edu.ua/issue/view/15815 > (in Ukrainian)
5. Hlynska N. V. 'Pravovyi aspekt zaprovadzhennia rezhymu paperless v kryminalnomu provadzhenni Ukrainy' [The legal aspect of the introduction of the paperless regime in the criminal proceedings of Ukraine] (2023) 45 Pytannia borotbu zi zlochynnistiu 86–96 < http://pbz.nlu.edu.ua/article/view/288509 > (in Ukrainian)
6. Shchur B. V., Basysta I. V. 'Sudove provadzhennia u rezhymi videokonferentsii ta transliatsii z inshoho prymishchennia, u tomu chysli, yake znakhodytsia poza mezhamy prumishchennia sudu : okremi pidkhody do rozuminnia ta problemy realizatsii' [Court proceedings in videoconference mode and broadcasting from another premises, including one located outside the court premises: separate approaches to understanding and problems of implementation] (2022) 29 (3) Visnyk Natsionalnoii akademii pravovykh nauk Urkainy 242–267 (in Ukrainian)
7. Khyzhniak Ye. S. 'Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen' [Peculiarities of inspection of electronic documents during investigation of criminal offenses] (2017) 4 (58) Derzhava ta rehiony 80–85. (in Ukrainian)
8. Velykanova M. M. 'Ponyattya ta strukturni elementy ryzyku: tsyvilno-pravovyi aspect' (2017) 45 Universytetski naukovi zapysky 76–86 < https://journals.indexcopernicus.com/ api/file/viewByFileId/427972 > (in Ukrainian)

Conference paper

9. Hlynska N. V. 'Ryzyk-oriientovanyi pidkhid do tsyfrovizatsii kryminalnoho provadzhennia : okremi pytannia kontseptualistsii' [Risk-based approach to digitalization of criminal proceedings: separate issues of conceptualization] *Teoriia ta praktyka protydii zlochynnosti u suchasnykc umovakh* : zbirnyk tez Mizhnarodnoi naukovo-praktychnoi konferentsii (m. Lviv, 03 lystop. 2023 r.) 58–67 (in Ukrainian)
10 Pashkovkyi M. I. 'Vykorystannia Protokolu Berkli z vedenia rozsliduvan z vykorystanniam vidkrytykh tsyfrovykh dannykh pid chas dosudovoho rozsliduvannia kolabortsionizmu : analiz suduvoi praktyky' [Using the Berkeley

Protocol for investigating open digital data in pretrial collaborative investigations: a case study] *Aktualni pytannia kryminalno-pravovoi kvalifikatsii, dokumentuvannia ta rozslidyvannia* : materialy Vseukr. nauk.-prakt. konf. (m. Odesa, 21 lyp. 2023 r.) 168–172. (in Ukrainian)

Websites

11. 'EU AI Act: First Regulation on Artificial Intelligence' (European Parliament website 14.06.2023) <https://www.europarl.europa.eu/ news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> (in English)

Глинська Н. В., Рєпіна Ю. С.

Ризик-орієнтований підхід як методологічна основа цифровізації кримінального провадження в Україні: до презентації результатів дослідження (Частина 1. Типологізація ризиків)

Стаття присвячена презентації основних результатів, отриманих за підсумком проведеної наукової розвідки питання використання ризик-орієнтованого підходу як методологічної основи цифровізації кримінального провадження в Україні щодо висвітлення питання типологізації ризиків цифровізації кримінального провадження як необхідної умови керування ними.

Беручи до уваги інтрузивний характер кримінального провадження, запровадження цифрових технологій у таку царину має бути контрольованим та виваженим з огляду на пов'язані із діджиталізацією потенційні чи ймовірні негативні наслідки, приховані небезпеки для охоронюваних законом цінностей. Відтак, доктринальний розгляд питань щодо ризиків реалізації норм кримінального процесуального права в перебігу цифровізації кримінального провадження надасть теоретично обґрунтовані пропозиції щодо оптимізації процесу цифровізації кримінального провадження, а, отже, забезпечить розвиток кримінальної юстиції в Україні відповідно до вимог сучасності.

Це зумовлює доцільність екстраполювання на процес цифровізації кримінального провадження популярної у світі концепції ризик-орієнтованого підходу як засобу зниження ризику виникнення кризових явищ, а так само доцільність розробки державних програм у галузі цифровізації кримінального провадження із запобігання небажаним подіям і їх ліквідації. Впровадження ризик-орієнтованого підходу цифровізації кримінального провадження допоможе оцінити ризики, розробити й впровадити ефективні заходи з їх уникнення та мінімізації, а, отже, й визначити та реалізувати пріоритетні напрями цифровізації кримінального провадження.

Ключові слова: *кримінальна юстиція, електроне кримінальне провадження, цифровізація, штучний інтелект, ризик, ризик-орієнтований підхід.*

Hlynska N. V., Riepina Yu. S.

Risk-based Approach as a Methodological Basis for Digitalization of Criminal Proceedings in Ukraine: to the Presentation of Research Results (Part 1. Typology of Risks)

The article is devoted to the presentation of the main results obtained as a result of the scientific research on the use of a risk-based approach as a methodological basis for the digitalisation of criminal proceedings in relation to digitalisation of criminal proceedings, with the aim of highlighting the issue of the typology of risks in the digitalization of criminal proceedings as a prerequisite for their management. Given the intrusive nature of criminal proceedings, the introduction of digital technologies in this area should be controlled and balanced, taking into account the potential or probable negative consequences associated with digitalisation and hidden dangers to the legally protected values. Therefore, a doctrinal consideration of the risks of introducing criminal procedure norms in the course of digitalization of criminal procedure will allow to provide theoretically grounded proposals for optimizing the process of digitalisation of criminal proceedings and thereby ensure the development of criminal justice in Ukraine in accordance with modern requirements.

This determines the expediency of extrapolating to the process of digitalization of criminal proceedings the concept of a risk-oriented approach popular in the world as a means of reducing the risk of crisis phenomena, as well as the expediency of developing state programs in the field of digitalization of criminal proceedings to prevent unwanted events and eliminate them.The introduction of a risk-based approach to the digitalization of criminal proceedings will help to assess risks, develop and implement effective measures to prevent and minimize them, and therefore identify and implement priority areas for the digitalization of criminal proceedings.

Keywords: *criminal justice, electronic criminal proceedings, digitalization, artificial intelligence, risk, risk-based approach.*

Стаття надійшла до редакції:22.09.2024 р.
Прийнята до друку: 20.11.2024 р.