

Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра кримінального та кримінально-процесуального права

Магістерська робота
освітній ступінь – магістр
на тему «**Цифровізація досудового розслідування та судового розгляду**
у кримінальному провадженні»
" Digitalization of Pre-Trial Investigation and Trial in Criminal
Proceedings"

Виконав: студент 2-го року навчання
Спеціальності 081 Право
Зверев Михайло Кирилович

Керівник Хавронюк М.І.
Професор, доктор юридичних наук

Рецензент _____
(прізвище та ініціали)

Магістерська робота захищена
з оцінкою _____

Секретар ЕК _____
« _____ » _____ 20 ____ р.

Київ – 2025

Декларація академічної доброчесності

Я, Зварев Михайло Кирилевич,
студент 2 року навчання магістерської
програми з спеціальністю "Право"
факультету правничих наук На ІКМН
підтверджую таке:

- написана мною магістерська
робота на тему: "Цифровізація
досудового розслідування та судового
розгляду у кримінальному провадженні".

Відповідає вимогам академічної
доброчесності та не містить порушень,
передбачених п. 3.1 Положення про ака-
демічну доброчесність здобувачів освіти
у На ІКМН, зі змістом якого я ознайом-
лений.

- Я заявляю, що надаю єдиного
перевірки електронна версія роботи є
ідеентичною її друкованій версії.

9.05.2025р.

ЗМ

ЗМІСТ

<u>ПЕРЕЛІК СКОРОЧЕНЬ</u>	4
<u>ВСТУП</u>	5
<u>РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ</u>	10
<u>1.1. Поняття цифровізації кримінального провадження</u>	10
<u>1.2. Правові основи цифровізації кримінального провадження в Україні</u>	20
<u>1.3. Міжнародний досвід цифровізації кримінального провадження</u>	29
<u>РОЗДІЛ 2. ЦИФРОВІ ТЕХНОЛОГІЇ У ДОСУДОВОМУ РОЗСЛІДУВАННІ</u>	37
<u>2.1. Впровадження цифрових технологій в органах досудового розслідування</u>	37
<u>2.2. Використання електронних доказів у кримінальному провадженні</u>	42
<u>2.3. Проблеми та перспективи цифровізації досудового розслідування</u> .	49
<u>РОЗДІЛ 3. ЦИФРОВІ ТЕХНОЛОГІЇ У СУДОВОМУ РОЗГЛЯДІ КРИМІНАЛЬНИХ СПРАВ</u>	57
<u>3.1. Перехід до електронного судочинства</u>	57
<u>3.2. Використання відеоконференцій та онлайн-слухань</u>	61
<u>3.3. Переваги та виклики цифровізації судового розгляду</u>	71
<u>ВИСНОВКИ</u>	78
<u>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</u>	84
<u>ДОДАТКИ</u>	96

ПЕРЕЛІК СКОРОЧЕНЬ

ЦКП - цифровізація кримінального провадження

КПК – Кримінальний процесуальний кодекс

КК – Кримінальний кодекс

ЄСІТС - Єдина судова інформаційно-телекомунікаційна система

ЄС – Європейський союз

КП – Кримінальне провадження

ЦТПК - Цифрова трансформація кримінального провадження

ЄРДР - Єдиний реєстр досудових розслідувань

ЄДРСР - Єдиний державний реєстр судових рішень

КРЕС - Консультативна рада європейських суддів

ЄСПЛ - Європейський суд з прав людини

ДБР – Державне бюро розслідування

ШІ – Штучний інтелект

ВСТУП

Сучасний етап розвитку правової системи України відзначається стрімким упровадженням цифрових технологій у сферу кримінального судочинства. Зокрема, цифровізація досудового розслідування та судового розгляду у кримінальному провадженні стала не лише ознакою технічного прогресу, а й ключовим інструментом підвищення ефективності, оперативності, прозорості та доступності правосуддя. В умовах воєнного стану, загрози безпеці держави, а також зростання злочинності потреба у швидкому реагуванні правоохоронної системи лише посилилася, що обумовлює актуальність наукового аналізу цифрових трансформацій у кримінальному провадженні.

Цифровізація кримінального процесу охоплює застосування електронного документообігу, цифрових доказів, відеоконференцій, автоматизованих інформаційних систем і штучного інтелекту, що формує нову якість правосуддя. Разом із тим така трансформація висуває низку викликів – зокрема правових, етичних та технічних. Ці зміни потребують глибокого наукового осмислення, з урахуванням як міжнародного досвіду, так і національної правової специфіки. Проте, попри зростання уваги наукової спільноти до проблематики цифровізації, окремі аспекти впровадження інноваційних технологій у сферу кримінального судочинства залишаються недостатньо дослідженими.

Наукова значущість теми полягає у необхідності визначення правових, організаційних та технічних умов, які забезпечують ефективне впровадження цифрових технологій у досудове розслідування та судовий розгляд. Окрім того, важливим є аналіз ризиків, пов'язаних із захистом персональних даних, недопущенням порушення прав людини та забезпеченням інституційної незалежності судової влади в умовах цифровізації.

Об’єкт дослідження – досудове розслідування та судовий розгляд у кримінальному провадженні.

Предмет дослідження - цифровізація досудового розслідування та судового розгляду у кримінальному провадженні

Мета дослідження – з’ясувати, як цифровізація змінює підходи до організації та реалізації досудового розслідування і судового розгляду у кримінальному процесі, а також оцінити переваги, ризики та правові наслідки цього процесу.

Завдання дослідження:

1. Розкрити поняття цифровізації кримінального провадження та її роль у модернізації кримінальної юстиції.
2. Проаналізувати правові засади цифровізації досудового розслідування та судового розгляду в Україні.
3. Вивчити міжнародний досвід цифрової трансформації кримінального правосуддя.
4. Дослідити практичне застосування цифрових технологій у діяльності правоохоронних органів і судів.
5. Виявити ключові переваги та ризики, пов’язані з цифровізацією кримінального провадження.
6. Надати пропозиції щодо вдосконалення правового регулювання цифрових процесів у кримінальній юстиції України.

Дослідницьке питання: *яким чином цифровізація впливає на ефективність, доступність і справедливість досудового розслідування та судового розгляду в межах кримінального провадження в Україні?*

Для досягнення поставленої мети дослідження та вирішення визначених завдань було використано комплекс загальнонаукових і спеціально-юридичних методів, які забезпечили всебічний аналіз явища цифровізації у сфері кримінального провадження. Зокрема:

- **діалектичний метод** застосовано як базовий для дослідження. Він дав змогу розглядати цифровізацію досудового розслідування та судового розгляду як динамічне явище, що розвивається відповідно до потреб сучасного суспільства та правової системи;
- **історико-правовий метод** дозволив дослідити еволюцію процесів цифровізації у кримінальному провадженні України, простежити етапи впровадження електронних технологій у досудове слідство й судову систему;
- **системно-структурний метод** використано для аналізу правової бази цифровізації кримінального процесу, а також для виявлення взаємозв'язку між різними елементами цифрових інструментів у рамках правозастосовної діяльності;
- **порівняльно-правовий метод** застосовано при дослідженні досвіду цифровізації кримінального провадження в інших державах та співставленні цього досвіду з українською практикою;
- **метод аналізу і синтезу** був використаний для вивчення наукових джерел, нормативних актів, судової практики та емпіричних даних щодо функціонування електронних систем у сфері кримінальної юстиції;
- **формально-юридичний метод** забезпечив вивчення та тлумачення правових норм, що регулюють цифрову трансформацію кримінального процесу.

Застосування цих методів у сукупності дало змогу глибоко проаналізувати науково-практичну проблему, обґрунтувати теоретичні положення дослідження та розробити практичні рекомендації щодо удосконалення цифрових інструментів у кримінальному судочинстві України.

Уперше на основі вітчизняного й міжнародного досвіду:

- уточнено поняття «цифровізація кримінального провадження» як системної інтеграції цифрових технологій у правозастосовну діяльність із урахуванням принципів ефективності, справедливості та прав людини;
- систематизовано правові, організаційні та технічні передумови цифровізації у кримінальному процесі України;
- виявлено проблеми правової невизначеності у використанні електронних доказів та штучного інтелекту в кримінальному судочинстві, запропоновано шляхи їх подолання;
- сформульовано авторські рекомендації щодо гармонізації національного законодавства з міжнародними стандартами у сфері цифрових правосудних практик, зокрема в умовах воєнного стану.

Результати дослідження мають практичну цінність для вдосконалення правозастосовної діяльності органів досудового розслідування, прокуратури та судів у частині впровадження електронного документообігу, відеоконференцій, використання електронних доказів та інших цифрових інструментів.

Практичне значення роботи проявляється у наступному:

- розроблені рекомендації можуть бути використані при підготовці проєктів змін до Кримінального процесуального кодексу України, зокрема щодо визначення статусу електронних доказів, вимог до цифрової фіксації процесуальних дій та захисту персональних даних;
- положення роботи можуть бути впроваджені в методичні матеріали для підвищення кваліфікації слідчих, прокурорів і суддів, а також в освітні програми юридичних факультетів;
- результати дослідження сприяють формуванню цифрової правової культури та усвідомлення ризиків, пов'язаних із автоматизацією правосуддя без належних запобіжників;

- напрацювання можуть бути використані для модернізації ЄРДР, ЄСІТС та інших державних цифрових систем, а також для формування вимог до їх кібербезпеки, прозорості та доступності.

Таким чином, робота має не лише теоретичну цінність, а й практичну спрямованість, що робить її релевантною сучасним викликам, які постають перед кримінальною юстицією в умовах цифрової трансформації держави.

Структура магістерської роботи складається зі вступу, основної частини, висновків, списку використаних джерел та літератури.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

1.1. Поняття цифровізації кримінального провадження

Поняття цифровізації кримінального провадження в Україні є одним із ключових напрямів сучасної трансформації правової системи, обумовленої потребами технологічного прогресу, глобалізацією та необхідністю підвищення ефективності правоохоронної діяльності. Цей процес охоплює впровадження цифрових технологій у всі етапи кримінального провадження – від реєстрації злочинів до судового розгляду та виконання рішень. В Україні цифровізація кримінального провадження розвивається в контексті загальносвітових тенденцій, але має специфічні риси, пов'язані з національним законодавством, інфраструктурними можливостями та соціокультурними факторами. Аналіз цієї проблематики вимагає звернення до українських наукових джерел, які висвітлюють теоретичні та практичні аспекти інтеграції цифрових інструментів у кримінальну юстицію.

«Діджиталізація», як термін, який увійшов в нашу мову лише декілька років тому, є транслітерацією англійського «digitalization» та, відповідно до словника, є зміною в усіх сферах суспільного життя, пов'язаною з використанням цифрових технологій. Слово є простою формою більш точного терміну «цифрова трансформація» та є проявом глобальної цифрової революції» [1].

«Діджиталізація, на відміну від діджитизації, розвертає нас не до певних документів та їх форми, а до людини, суспільства, держави. Якщо мова йде про популярну фразу «держава в телефоні», то це якраз і буде найпростіший варіант визначення діджиталізації. Отже «...цифровізація – явище більш складне та передбачає впровадження цифрових технологій в

усі сфери управлінської діяльності, але при цьому не замінює паперові носії, а, в основному, дублює їх» [2].

«Цифровізацію загалом можна визначити як процес впровадження цифрових технологій для вдосконалення життєдіяльності людини, суспільства і держави» [3].

«Цифрові трансформації (як результат цифровізації) – спричинені використанням цифрових технологій зміни в природі людини, її мисленні, життєдіяльності та управлінні» [3].

«Цифровізація означає комп'ютеризацію систем і робочих місць для більшої легкості та доступності» [4]. «Визначення цифрової трансформації надане в підзаконному нормативному акті: «Цифрова трансформація – діяльність, що має на меті використання цифрових технологій для вирішення традиційних проблем інноваційними способами»» [5]. «Крізь призму побудови бізнес-стратегій «Цифрова трансформація (англ. digital transformation)» визначається як «трансформація бізнесу шляхом перегляду бізнес-стратегії або цифрової стратегії, моделей, операцій, продуктів, маркетингового підходу, цілей тощо, шляхом прийняття цифрових технологій»»; [6] ««процес переходу до нових способів роботи і мислення з використанням цифрових, соціальних, мобільних і нових технологій та включає зміну мислення керівництва, заохочення інновацій і нових бізнес-моделей, оцифровку активів і ширше використання технологій для поліпшення досвіду співробітників, клієнтів, постачальників, партнерів і зацікавлених сторін» [7].

«Втім з огляду на етимологічну природу терміну „трансформація”, що говорить про якесь „перетворення”, перехід від старого до нового, зміну якості чогось тощо» [8].

«Цифровізацію загалом можна визначити як процес впровадження цифрових та інформаційно-комунікативних технологій для вдосконалення життєдіяльності людини, суспільства і держави. Необхідним результатом

цифровізації є цифрова трансформація, що означає спричинені використанням цифрових технологій зміни в природі людини, її мисленні, життєдіяльності та управлінні» [10, с. 61]. «Цифрова трансформація як закономірний результат цифровізації обумовлює перехід до нових способів роботи і мислення з використанням цифрових технологій, адаптацію того чи іншого різновиду діяльності до цифрових реалій. ЦКП – це багатоаспектне поняття, що в діяльнісному розумінні являє собою як процес розумного впровадження (розумне оснащення) цифрових та інформаційних технологій у кримінальну процесуальну форму, що супроводжується адаптацією кримінального провадження до специфіки цифрового середовища (цифрової інформації) та специфіки розслідування кіберзлочинів із дотриманням необхідного балансу між підвищенням ефективності розслідування та судового розгляду та забезпеченням прав та законних інтересів осіб в цій царині. Цифрова трансформація кримінального провадження (ЦТКП) – це закономірний результат процесу ЦКП, якісна визначеність якого характеризується певним рівнем перетворення кримінального провадження, обумовленим переходом до нових способів діяльності з використанням цифрових технологій, адаптацією до специфіки цифрового середовища (цифрової інформації). Звичайно сформульовані визначення є оперативними та потребують подальших наукових розвідок з метою дослідження їх різних аспектів. Супутником процесу ЦКП є формування релевантних цифрових компетентностей правозастосовників» [10, с. 62].

«Воєнний стан незворотно вплинув на життя нашої країни, у тому числі спричинив зростання злочинності. Це своєю чергою призвело до необхідності розробки більш ефективних методів розслідування кримінальних правопорушень. Цифровізація кримінального процесу стає одним з ключових елементів, які сприяють підвищенню удосконаленню

діяльності правоохоронних органів та забезпечує їх здатність ефективно реагувати на злочинні дії в умовах війни» [11, с. 32].

Сутність цифровізації кримінального провадження полягає у заміні традиційних паперових процедур електронними аналогами, автоматизації процесів збору, зберігання та обробки даних, а також у використанні штучного інтелекту, блокчейну, хмарних технологій для підвищення прозорості, швидкості та об'єктивності правосуддя.

На думку О.В. Петришина, цифровізація в правовій сфері не обмежується технічними інноваціями, а передбачає системну зміну парадигми функціонування інститутів держави, що вимагає переосмислення принципів законності, презумпції невинуватості та права на захист у нових умовах [12].

З огляду на вищевикладене, ми пропонуємо таке визначення. ***Цифровізація кримінального провадження*** – це впровадження та використання цифрових технологій на всіх етапах досудового розслідування, судового розгляду та виконання судових рішень з метою підвищення ефективності, прозорості, оперативності та безпеки кримінального процесу. Вона включає застосування електронного документообігу, цифрових доказів, відеоконференцій, автоматизованих інформаційних систем, баз даних та інших ІТ-рішень у діяльності правоохоронних і судових органів.

Водночас, як зазначають науковці, ключовим викликом залишається збереження балансу між ефективністю технологій і гарантіями прав людини, особливо у контексті ризиків несанкціонованого доступу до даних або маніпуляцій цифровими доказами [13].

Початок інституційних змін у сфері цифровізації кримінального провадження в Україні пов'язаний із прийняттям Кримінального процесуального кодексу 2012 року, який уперше легалізував використання електронних документів у доказовій базі [14]. Проте справжній поштовх до

трансформації відбувся після 2017 року, коли було ухвалено Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (у редакції від 1 грудня 2022 року цей Закон має назву «Про електронну ідентифікацію та електронні довірчі послуги») [15], що закріпив правові підстави для електронного підпису та ідентифікації. Це дозволило розпочати створення єдиних реєстрів, таких як Єдиний реєстр досудових розслідувань (ЄРДР), який став основним інструментом фіксації інформації про злочини. За даними дослідження Т. О. Савченко, впровадження ЄРДР зменшило час реєстрації заяв про злочини з 3–5 днів до кількох годин, що свідчить про позитивний вплив цифровізації на оперативність реагування правоохоронних органів [16].

Важливим кроком стало створення Системи електронного суду, яка дозволила учасникам процесу подавати клопотання, ознайомлюватися з матеріалами справ та отримувати повідомлення в онлайн-режимі. Ця система сприяла зменшенню корупційних ризиків, пов'язаних із «втратою» паперових документів, а також забезпечила більш рівний доступ до правосуддя для громадян із віддалених регіонів. Однак, ефективність електронного суду обмежена технічними проблемами, такими як недостатня інтеграція з іншими державними базами даних або відсутність єдиних стандартів шифрування, що створює загрозу конфіденційності інформації.

Окрему увагу в наукових дослідженнях приділено цифровізації доказової діяльності. Зокрема, вчені з Національної академії правових наук України (як, наприклад, Ю. П. Битяк) акцентують на тому, що використання відеозаписів, електронних листувань, даних з GPS-трекерів або соціальних мереж потребує чітких критеріїв допустимості та перевірки достовірності [13].

Пандемія COVID-19 стала каталізатором прискорення цифровізації. За даними Офіційного веб-порталу Судової влади України, кількість

онлайн-засідань у кримінальних справах зросла на 70%, що, з одного боку, підтвердило життєздатність електронних інструментів, а з іншого – виявило низку проблем [17]. Багато суддів та слідчих, особливо у сільській місцевості, не володіли навичками роботи з відеоконференцзв'язком, що призводило до порушень процесуальних строків. Крім того, нерівний доступ до інтернету в різних регіонах обмежував можливості учасників процесу, особливо потерпілих із малозабезпечених верств населення.

Однією з найбільш дискусійних тем у науковому середовищі є використання штучного інтелекту у кримінальному провадженні.

Алгоритми ШІ вже застосовуються для аналізу великих масивів даних з метою виявлення кореляцій між злочинами, прогнозування рецидивів або оцінки ризиків у діяльності підозрюваних. Водночас, науковці попереджають про небезпеку упередженості алгоритмів, навчених на історичних даних, які можуть відтворити структурні нерівності. Наприклад, експеримент, проведений Інститутом інформаційних технологій і права НАН України у 2022 році, показав, що система, розроблена для оцінки ймовірності втечі підозрюваних, частіше рекомендувала запобіжні заходи для осіб із сільських районів, що корелювало з їхнім нижчим соціально-економічним статусом. Це свідчить про необхідність суворого регулювання та аудиту алгоритмів, що використовуються в правовій сфері [13].

Важливим аспектом цифровізації є захист персональних даних, особливо у контексті євроінтеграційних прагнень України. Впровадження Загального регламенту щодо захисту даних (GDPR) як еталону вплинуло на українське законодавство, зокрема на Закон «Про захист персональних даних» 2010 року [18]. Проте, у кримінальному провадженні доступ до даних часто суперечить принципам мінімізації та обмеженості мети. Наприклад, правоохоронці отримують доступ до геолокаційних даних мобільних операторів без чітких процедур обґрунтування необхідності, що

створює ризик масового стеження. Це, на думку науковця, потребує удосконалення механізмів судового контролю.

Цифровізація сучасного правосуддя має безпосередній та багатогранний вплив на реалізацію й гарантування права особи на належний захист у кримінальному провадженні. З одного боку, впровадження електронних інструментів - таких як онлайн-доступ до баз даних судових рішень, функціональні електронні кабінети для адвокатів, спеціалізовані платформи для дистанційного подання процесуальних документів, а також можливість отримання правових консультацій через інтернет - значно спрощує доступ до правової допомоги. Це особливо важливо для тих осіб, які проживають у віддалених або малозабезпечених регіонах, де фізична присутність адвоката або поїздка до суду є ускладненою. У результаті цифрові сервіси сприяють підвищенню ефективності правового захисту, зменшенню часових і фінансових витрат, а також розширенню кола осіб, які можуть скористатися своїм правом на правову допомогу.

Водночас цифровізація створює й нові виклики, пов'язані з технічною складністю та нерівним доступом до цифрових інструментів серед правників. Особливо це стосується роботи з цифровими доказами - аудіозаписами, відеофайлами, метаданими, зашифрованими файлами та іншими складними цифровими форматами, що все частіше використовуються в рамках кримінального процесу.

Адвокати, які не мають достатнього рівня цифрової компетентності або навичок роботи з подібними матеріалами, можуть не лише витрачати більше часу на ознайомлення з доказами, але й не до кінця розуміти їх зміст або юридичну значущість. Згідно з дослідженням, проведеним Асоціацією адвокатів України у 2021 році, лише 35% адвокатів, які здійснюють захист у кримінальних справах, систематично використовують електронні платформи у своїй практиці. Більшість респондентів або не володіють

відповідними технічними навичками, або мають недовіру до надійності електронних систем, вважаючи їх вразливими до збоїв або втрати даних. Як наслідок, це може негативно впливати на ефективність реалізації права підозрюваного чи обвинуваченого на захист, адже адвокат не використовує всі доступні інструменти для забезпечення належної правової позиції (Офіційний веб-портал Національної асоціації адвокатів України).

Окремої уваги заслуговує питання кібербезпеки в умовах цифрового правосуддя. З кожним роком зростає кількість кібератак на державні інформаційні системи, і правова сфера не є винятком. Особливо актуальною ця проблема стала у 2024–2025 роках, коли зафіксовано серйозні атаки на Єдиний реєстр досудових розслідувань (ЄРДР), що поставило під загрозу збереження та конфіденційність даних у кримінальних провадженнях. Витоки або знищення інформації в таких реєстрах можуть мати фатальні наслідки для правосуддя. У відповідь на це, деякі науковці та експерти пропонують застосовувати блокчейн-технології як інструмент забезпечення незмінності цифрових записів у кримінальних справах. Такі технології дозволяють зафіксувати кожну зміну у справі з неможливістю її редагування заднім числом, що суттєво підвищує рівень довіри до електронних доказів. Однак реалізація таких рішень вимагає значних інвестицій в оновлення інфраструктури, технічного переоснащення органів досудового розслідування, судів та адвокатури. Крім того, наразі відсутній уніфікований стандарт кібербезпеки, обов'язковий для всіх учасників кримінального провадження, що ускладнює ефективну координацію дій щодо захисту інформації, особливо в міжвідомчій взаємодії. Це створює прогалини в безпеці, якими можуть скористатися зловмисники або треті сторони. [13].

Соціокультурні чинники також відіграють роль у цифровізації. Ми впевнені, що довіра громадян до електронних систем залишається низькою через страх перед технічними збоями або несанкціонованим використанням даних.

У контексті міжнародного досвіду, Україна демонструє активність у впровадженні рекомендацій Європейського Союзу щодо цифровізації юстиції, особливо в межах реалізації Угоди про асоціацію між Україною та ЄС. Така інтеграція передбачає адаптацію національного законодавства і практик до європейських стандартів цифрового правосуддя. Зокрема, ініціатива «Цифрова Європа» забезпечує фінансування розробки і впровадження інноваційних електронних систем, спрямованих на модернізацію судової інфраструктури. Одним із результатів цього процесу стало створення в Україні платформи «Єдина судова інформаційно-телекомунікаційна система» (ЄСІТС), яка забезпечує електронний документообіг, доступ до матеріалів справи та електронне листування між учасниками судового процесу.

Однак повна імплементація європейських цифрових стандартів стикається з низкою перешкод, головним чином адміністративного та фінансового характеру. Наприклад, впровадження обов'язкової двофакторної аутентифікації для безпечного доступу до системи електронного суду відбувалося частково і з затримками, зумовленими браком бюджетних коштів для придбання відповідного обладнання та програмного забезпечення. Бюрократична інертність і фрагментованість процесів впровадження нових рішень часто гальмують розвиток цифрових систем, створюючи розрив між теоретичними зобов'язаннями та практичною реалізацією.

Перспективи цифровізації кримінального провадження в Україні безпосередньо пов'язані з упровадженням сучасних технологій, що вже активно використовуються в низці європейських країн. Ідеться, зокрема, про впровадження алгоритмів машинного навчання для аналізу великого масиву судових рішень, побудову розподілених реєстрів (на зразок блокчейн) для відстеження руху речових доказів, а також використання систем відеоспостереження з вбудованими модулями розпізнавання облич.

Такі інновації можуть підвищити ефективність слідчих дій і забезпечити об'єктивність доказування. Водночас чинний Кримінальний процесуальний кодекс України наразі не містить спеціальних норм, які регулювали б використання результатів роботи нейронних мереж, біометричних сканерів або інших інтелектуальних технологій. Це створює прогалини в правовому регулюванні і ставить під сумнів допустимість таких доказів у суді, зокрема з огляду на дотримання процесуальних гарантій і прав людини.

Важливим стратегічним напрямом розвитку цифрового правосуддя в Україні є створення єдиного міжвідомчого інформаційного простору. Йдеться про інтеграцію даних з таких ключових джерел, як ЄРДР, система електронного суду, бази митних органів, податкової служби, Національної поліції, а також інших органів виконавчої влади. Наявність єдиного цифрового середовища дозволить забезпечити безперервний обмін інформацією, уникнути дублювання даних та помилок, підвищити швидкість розгляду справ, а також забезпечити прозорість процедур. За оцінками провідних експертів, повноцінна реалізація цього проекту може зайняти щонайменше 5–7 років, враховуючи обсяг роботи та необхідність значних фінансових інвестицій у технічну інфраструктуру, кіберзахист і навчання персоналу. Попри це, вже сьогодні в Україні впроваджуються окремі елементи цифрової взаємодії між установами, наприклад, системи електронних міжвідомчих запитів, які дозволяють оперативно отримувати потрібну інформацію з суміжних органів.

Критичним чинником успішної цифрової трансформації юстиції є якісна підготовка кадрів, здатних ефективно працювати в нових умовах. Вищі юридичні навчальні заклади, а також установи післядипломної освіти - зокрема, Національна школа суддів України - вже інтегрують до своїх освітніх програм курси з цифрової юриспруденції, електронного документообігу, кібербезпеки та інші актуальні теми. Це свідчить про зростання розуміння важливості формування нових компетенцій у суддів,

прокурорів, адвокатів, слідчих. Особливо перспективним напрямом є впровадження віртуальних симуляторів і спеціалізованих платформ для моделювання реальних ситуацій, де фахівці можуть відпрацьовувати навички роботи з електронними доказами, електронними процесуальними документами, а також взаємодії в межах цифрового процесу. Такий підхід сприятиме не лише підвищенню кваліфікації окремих фахівців, але й формуванню нової цифрової культури у сфері правосуддя загалом.

1.2. Правові основи цифровізації кримінального провадження в Україні

Обговорення впровадження електронного кримінального провадження (ЕКП) стало активним після ухвалення нового Кримінального процесуального кодексу України (КПК) у 2012 році.

Головною метою впровадження ЕКП була потреба зменшити можливості для зловживань, підробок і впливу людського фактора на неупередженість розслідування. Також важливу роль у цій ініціативі відігравала потреба у скороченні витрат часу, ресурсів і коштів усіх сторін кримінального процесу.

КПК 2012 року передбачав лише обмежене використання цифрових технологій у кримінальному судочинстві через слабкий розвиток тодішніх інформаційно-телекомунікаційних систем. Проте вже у тому ж році розпочалась цифрова трансформація: було створено Єдиний реєстр досудових розслідувань (ЄРДР) і запроваджено Автоматизовану систему документообігу суду (АСДС), яка згодом – у 2017 році – стала частиною Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС).

Наступним етапом стало налагодження взаємодії між цими системами, що стало можливим завдяки запуску інформаційно-телекомунікаційної системи досудового розслідування під назвою «іКейс».

У 2018 році Антикорупційна ініціатива Європейського Союзу в Україні (EUACI) розпочала вивчення технічної реалізації цього проєкту, а вже з 2019 року почала безпосередню розробку програмного забезпечення. У 2020 році систему іКейс передали на баланс НАБУ, після чого її почали тестувати в межах пілотного проєкту.

Публічна презентація системи відбулася у квітні 2020 року під час вебконференції за участі Комітету Верховної Ради з питань правоохоронної діяльності, Офісу Генпрокурора, НАБУ та Антикорупційної ініціативи ЄС. У грудні 2021 року до КПК були внесені відповідні зміни, а НАБУ, Офіс Генпрокурора, ВАКС та Рада суддів України видали спільний наказ, яким офіційно впровадили систему «іКейс» у досудовому розслідуванні. Як зазначено у пояснювальній записці до змін, основною метою є відмова від паперової форми документів на етапах досудового розслідування і розгляду справ у суді.

Це стало відправною точкою для нової цифрової ери в українській системі кримінального судочинства. 16 грудня 2021 року НАБУ і САП зафіксували перше кримінальне провадження в новій системі.

Втім, через початок повномасштабного вторгнення Росії у 2022 році розвиток системи тимчасово призупинився – аж до літа того ж року.

Наразі «іКейс» продовжує активно розвиватися, а кількість проваджень, внесених до системи, постійно зростає.

З квітня 2024 року в системі з'явилася можливість подавати до ВАКС клопотання про проведення обшуків та тимчасовий доступ до речей і документів.

Попри значні досягнення, реалізація всього потенціалу системи ще триває. Її повноцінна робота залежить від організаційної та правової готовності ключових органів – НАБУ, САП і ВАКС.

Кабінетом Міністрів України 17 січня 2018 р. №67-р було ухвалено розпорядження «Про схвалення Концепції розвитку цифрової економіки та

суспільства України на 2018–2020 роки». «Згідно з цією концепцією «Цифровізація» – це насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливорює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір. Основною метою цифровізації є досягнення цифрової трансформації існуючих та створенні нових галузей економіки, а також трансформації сфер життєдіяльності у нові більш ефективні та сучасні» [20].

Концептуальним документом, який належить до адміністративно-правових засад організації та діяльності прокуратури в Україні, є Стратегія розвитку прокуратури на 2021–2023 роки, затверджена Наказом Генерального прокурора від 16 жовтня 2020 року № 489 [21].

«А. Столітнім розроблено технічний твір «Інформаційно-аналітична система обробки заздалегідь згенерованих баз Єдиного реєстру досудових розслідувань за допомогою готових наборів Excel (з ілюстраціями)», що передбачає можливість шляхом обробки попередньо сформованих і збережених баз даних Реєстру генерувати дані за більш ніж 30 видами порушень кримінального процесуального законодавства та по суті є елементом електронного процесуального контролю. А. Столітній запропонував інтегрувати вказану систему до ЄРДР шляхом перенесення її логічних виражень і форм до розділу «Аналітика та статистика», що дозволяє частково автоматизувати процесуальну діяльність уповноважених суб'єктів щодо своєчасного виявлення й усунення порушень процесуальної процедури, допущеної під час досудового розслідування» [22, с. 29]. «У межах чинної моделі фіксації даних в електронній системі (заповнення цифрових контурів, електронні каталоги альтернативного вибору даних, система відміток) наявні передумови електронного процесуального контролю, оскільки за допомогою інструментів аналітики ЄРДР суб'єкти процесуального контролю мають можливість оперативно виявляти випадки

процесуальних порушень під час закінчення досудового розслідування» [22, с. 29]. «За допомогою ЄРДР можна відстежувати закриті кримінальні провадження, а за допомогою розробленого ним технічного твору – звужувати пошук рішень, які потребують перевірки та процесуального реагування, оскільки, наприклад, серед 532 277 закритих кримінальних проваджень було визначено 662 (0,12%), у яких потенційно наявні порушення процесуальної процедури, що вдосконалює процесуальну діяльність прокурора на вказаному етапі [22, с. 29–30]. 15 грудня 2021 року введено в дію прийнятий 1 червня 2021 року Закон «Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування»» [29].

«Вказаним Законом внесено зміни до Кримінального процесуального кодексу України, зокрема КПК України доповнено ст. 106-1 такого змісту: «Інформаційно-телекомунікаційна система досудового розслідування – це система, яка забезпечує створення, збирання, зберігання, пошук, оброблення і передачу матеріалів та інформації (відомостей) у кримінальному провадженні. Порядок функціонування інформаційно-телекомунікаційної системи досудового розслідування визначається положенням, яке затверджується спільно Офісом Генерального прокурора, органом, у складі якого функціонує орган досудового розслідування, а також органом, що затверджує положення про систему, яка функціонує у суді відповідно до ст. 35 цього Кодексу. Інформаційно-телекомунікаційна система досудового розслідування взаємодіє з Єдиним реєстром досудових розслідувань та системою, яка функціонує в суді відповідно до статті 35 цього Кодексу, а також може взаємодіяти з іншими інформаційними, інформаційно-телекомунікаційними системами у випадках, передбачених законом»» [29].

«Крім того, передбачено, що «слідчий, дізнавач, прокурор, слідчий суддя, суд, а також захисник (за його згодою) використовують, а інші учасники кримінального провадження можуть використовувати інформаційно-телекомунікаційну систему досудового розслідування під час реалізації своїх повноважень, прав та інтересів, передбачених цим Кодексом, за умов та в порядку, що визначені положенням про таку систему. У разі використання зазначеної у цій статті системи дослідження матеріалів досудового розслідування, наявних у такій системі, може здійснюватися з використанням доступу до них через цю систему. Матеріали досудового розслідування, що містяться в інформаційно-телекомунікаційній системі досудового розслідування, передаються, їх копії чи примірники надаються в електронній формі, а за рішенням слідчого, дізнавача, прокурора, слідчого судді, суду, які їх передають чи надають, – у паперовій формі»» [29].

«Важливим є доповнення Розділу XI «Перехідні положення» КПК України п. 20-6 такого змісту: «У разі відсутності інтеграції системи, яка функціонує у суді відповідно до ст. 35 цього Кодексу, з інформаційно-телекомунікаційною системою досудового розслідування слідчий, дізнавач, прокурор подає до суду матеріали в паперовій формі та в електронній формі з використанням кваліфікованого електронного підпису»» [29]. «Слід відзначити, що Вища рада правосуддя 17 серпня 2021 р. відповідно до вимог законодавства затвердила Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи. До початку функціонування Єдиної судової інформаційно-телекомунікаційної системи законодавством передбачено створення та функціонування окремих підсистем (модулів) цієї інформаційно-телекомунікаційної системи (ІТС), тобто поетапне введення в дію усієї ІТС, яка буде забезпечувати діяльність судової влади. Прийняте Положення визначає застосовні терміни і поняття. Передбачено порядок функціонування у судах та в органах правосуддя окремих підсистем

(модулів) ЄСІТС. Такими підсистемами є «Електронний кабінет», «Електронний суд», а також функціонування відеоконференцзв'язку як окремої підсистеми. Визначено порядок вчинення процесуальних дій в електронній формі з використанням вказаних підсистем ЄСІТС. Урегульовано особливості використання у судах та органах правосуддя програмного забезпечення у перехідний період до початку функціонування ЄСІТС у повному її складі підсистем або ж модулів» [28].

Згідно зі ст. 26 Закону України «Про правовий режим воєнного стану» «скорочення чи прискорення будь-яких форм судочинства в умовах воєнного стану забороняється [30]. При цьому чинний кримінальний процесуальний закон закріплює принцип розумності строків як одну з основоположних засад кримінального провадження (ст. 28 КПК), а також передбачає, що кожен має право, щоб обвинувачення щодо нього у найкоротший строк або стало предметом судового розгляду, або щоб відповідне кримінальне провадження щодо нього було закрито (ст. 21 КПК). Тож введення воєнного стану не скасовує високих темпоральних та якісних стандартів до результату кримінального судочинства, втім вимагає особливих інструментів, що дозволили б судді відправляти правосуддя, перебуваючи вдома чи у іншому безпечному місці. Зазначене питання окреслено у нещодавно оприлюдненому Міністерством юстиції України «Оперативному моніторингу: правосуддя в умовах війни»» [31, с. 27-28], «у якому звернуто увагу на те, що існує проблема, пов'язана із необхідністю перегляду нормативно-правового регулювання питання запровадження судами у період воєнного або надзвичайного стану особливого режиму роботи суду, дистанційної форми роботи, у тому числі розгляду справ в режимі відеоконференції поза межами приміщення суду (зали засідань) суддею, з використанням власних технічних засобів, участі у судовому засіданні суддів та/або секретаря судового засідання дистанційно у режимі

відеоконференції, особливостей підписання судових рішень та процесуальних документів» [32].

«Консультативна рада європейських суддів у своєму свіжому Висновку № 26 (2023) від 1 грудня 2023 року «Рухаючись вперед: використання асистивних технологій у судочинстві» [33] не лише позначила позитивні ефекти диджиталізації царини правосуддя, але й надала перелік ризиків, які неодмінно супроводжують переваги використання асистивних, тобто допоміжних технологій, під час здійснення правосуддя. Зокрема, КРЕС застерігає від того, що технологія не повинна використовуватися для прогнозування рішення окремого судді, а також зауважує, що технології не повинні знеохочувати або перешкоджати критичному мисленню суддів. Що більше, у документі наголошується на існуванні загрози для інституційної незалежності судової влади, оскільки процес ухвалення рішень може опинитися у руках тих, хто розробляє інструменти обробки даних» [35].

«Варто пригадати, що новелою КПК України є право суду обґрунтовувати судові рішення показаннями, наданими слідчому, прокурору, або посилатися на них, у порядку отримання показань, визначеного ст. 615 цього Кодексу. А відповідно до ч. 11 ст. 615 КПК України показання, отримані під час допиту свідка, потерпілого, у тому числі одночасного допиту двох чи більше вже допитаних осіб, у кримінальному провадженні, що здійснюється в умовах воєнного стану, можуть бути використані як докази в суді виключно у випадку, якщо хід і результати такого допиту фіксувалися за допомогою доступних технічних засобів відеофіксації. Власне, у цій частині сучасний КПК повернувся до моделі КПК 1960 року, де протоколи допитів свідків на слідстві дуже часто замінювали собою їх показання, надані суду наживо. Адже норма кримінального процесуального закону про те, що суд може обґрунтовувати свої висновки лише на показаннях, які він безпосередньо сприймав під час судового засідання або які були отримані в порядку, передбаченому ст. 225

«Допит під час досудового розслідування в судовому засіданні» КПК України, – це одне з найвагоміших надбань КПК України 2012 року» [36]

На нашу думку, правові основи цифровізації кримінального провадження мають охоплювати широкий спектр питань, включаючи електронний документообіг, електронні докази, засоби цифрового зв'язку, автоматизацію процесів та захист прав учасників провадження у цифровому середовищі.

Одним із важливих напрямів цифровізації є впровадження електронного документообігу в кримінальному провадженні. З огляду на те, що велика частина матеріалів справи складається з документів, їх цифрова форма дозволяє значно пришвидшити обмін інформацією між учасниками процесу, слідчими, прокурорами та судами. У цьому контексті важливе значення має Закон України «Про електронні документи та електронний документообіг» [37], який закріплює юридичну силу електронного документа та визначає вимоги до його створення, зберігання та обігу. Одним із ключових елементів цього процесу є електронний підпис, який гарантує автентичність і цілісність електронного документа. Використання кваліфікованого електронного підпису в кримінальному провадженні вже зараз дозволяє подавати клопотання, заяви, скарги та інші процесуальні документи в електронній формі, однак необхідно забезпечити їх повсюдне впровадження на практиці.

Іншою важливою складовою процесу цифровізації кримінального провадження є можливість здійснення окремих процесуальних дій у дистанційному режимі, зокрема шляхом використання відеоконференцзв'язку. Така практика відкриває нові можливості для оперативного реагування на процесуальні потреби та скорочення часу розгляду справ. Водночас реалізація цього підходу можлива лише за умови належного технічного забезпечення з боку судових установ, органів досудового розслідування та інших учасників провадження. Важливим є не

лише наявність техніки та програмного забезпечення, але й стабільний захищений канал зв'язку, можливість ідентифікації учасників, фіксація ходу засідання.

Окрім технічних аспектів, не менш значущими є вимоги щодо дотримання процесуальних гарантій, зокрема права на захист, доступу до матеріалів справи, забезпечення конфіденційного спілкування обвинуваченого з адвокатом та права бути почутим у справедливому судовому процесі. Усі ці гарантії повинні залишатися безумовними навіть у разі дистанційної форми участі у провадженні.

Цифровізація правосуддя також охоплює важливу сферу — використання електронних доказів у кримінальному провадженні. Згідно з чинним законодавством, зокрема положеннями Кримінального процесуального кодексу України, електронні носії інформації можуть виступати як джерела доказів у справі. Проте на практиці виникають численні проблеми щодо визнання таких доказів належними та допустимими. Основною причиною є відсутність чіткого законодавчого визначення поняття «електронний доказ», а також неурегульованість процедур його фіксації, отримання, збереження, перевірки на достовірність та подальшої оцінки в межах кримінального провадження. У результаті це створює невизначеність як для органів досудового розслідування, так і для суду, що негативно впливає на якість і передбачуваність судових рішень. У міжнародній практиці подібні проблеми вирішуються через розробку спеціальних техніко-юридичних стандартів, які встановлюють чіткі вимоги до форми, змісту та способу обробки електронних доказів. Українському законодавству варто орієнтуватися на такі підходи й поступово імплементувати єдину методологію поводження з цифровими доказами, забезпечуючи їхню автентичність, цілісність і юридичну надійність.

Ще одним перспективним і динамічним напрямом цифровізації є автоматизація окремих процесів у кримінальному провадженні, що значно розширює функціональні можливості слідчих, прокурорів, суддів і адвокатів. Ідеться не лише про зберігання кримінальних справ у цифровому форматі чи можливість участі в засіданні через інтернет, але й про запровадження складних інтелектуальних систем, здатних обробляти великі обсяги інформації, виявляти схеми правопорушень, будувати прогностичні моделі, ідентифікувати ризики. Наприклад, застосування технологій на базі штучного інтелекту може використовуватись для аналізу масивів телефонних з'єднань, встановлення взаємозв'язків між підозрюваними, виявлення шахрайських дій або навіть для оцінки ймовірності втечі чи повторного правопорушення. Такі інструменти потенційно здатні суттєво посилити ефективність кримінальної юстиції, скоротити навантаження на слідчих та суддів, а також підвищити точність прийняття рішень.

Водночас будь-яке використання алгоритмічних рішень у сфері правосуддя повинно супроводжуватись жорстким контролем і правовим регулюванням. Зокрема, має бути забезпечене дотримання принципу презумпції невинуватості, заборони дискримінації, прозорості алгоритмів і права особи на оскарження результатів, що базуються на роботі таких технологій. Без цих запобіжників існує ризик підміни людської правової оцінки механічними висновками систем, що суперечить засадам справедливого правосуддя.

1.3. Міжнародний досвід цифровізації кримінального провадження

У контексті глобалізації та інтеграції Європейського Союзу досвід європейських країн у сфері цифровізації кримінального правосуддя стає особливо актуальним, оскільки поєднує інноваційні підходи, правові стандарти та етичні виклики. Нижче нами розглядаються ключові аспекти

цифровізації кримінального правосуддя, такі як використання штучного інтелекту (ШІ), аналіз великих даних, автоматизація процесів розслідування, електронні суди та міжнародна співпраця, з посиланням на дослідження європейських науковців та практиків. Аналіз базується на наукових працях, опублікованих у таких виданнях, як *European Journal of Criminology*, *Computer Law & Security Review*, а також на офіційних документах ЄС, зокрема директивах та звітах Європейської комісії.

Однією з найважливіших тенденцій останніх років є інтеграція штучного інтелекту в кримінальне правосуддя. Дослідження, проведені німецькими та британськими вченими [38], показують, що алгоритми ШІ використовуються для прогнозування злочинності, аналізу ризиків рецидиву та оптимізації розподілу ресурсів поліції.

Наприклад, у Нідерландах система *SyRI* (System Risk Indication) [39], розроблена для виявлення шахрайства у сфері соціального забезпечення, стала предметом гострої суспільної дискусії через порушення приватності, що призвело до її заборони судом у 2020 році. Цей випадок підкреслює необхідність балансу між технологічним прогресом і захистом прав людини, про що пише М. Hildebrandt у своїй роботі «Law for Computing Scientists» [38, 39, 43].

У Франції, згідно з дослідженнями Institut Montaigne (2021), алгоритми, що аналізують дані з камер спостереження та соціальних мереж, допомагають ідентифікувати потенційні загрози тероризму, але водночас викликають занепокоєння через ризик дискримінації окремих груп населення. Європейський підхід до регулювання ШІ, відображений у проекті «Акта про штучний інтелект» (2023) [40], намагається запобігти таким ризикам, вимагають прозорості алгоритмів та забороняючи використання технологій масового спостереження в публічних просторах, крім виняткових випадків.

Великі дані (big data) також відіграють ключову роль у цифровізації кримінального правосуддя. Згідно з дослідженнями європейських науковців [41, 42], поліція та органи прокуратури все частіше використовують аналітику даних для виявлення злочинних схем, особливо в сферах відмивання грошей, торгівлі людьми та кіберзлочинності.

У Великій Британії система *PredPol* (Predictive Policing) [43], заснована на історичних даних про злочини, дозволяє прогнозувати «гарячі точки» злочинності. Проте критики, такі як E. Ferguson [39], вказують на те, що подібні системи можуть посилювати структурні упередження, оскільки історичні дані часто відображають дискримінаційні практики минулого.

У скандинавських країнах, зокрема в Данії та Швеції, акцент робиться на аналізі даних для запобігання злочинам, а не покарання, що відповідає концепції «превентивного правосуддя». Наприклад, данська програма *SSP* (Schools, Social Services, Police) використовує дані зі шкіл і соціальних служб для раннього втручання у ситуації, що загрожують криміналізацією неповнолітніх. Такий підхід, як зазначає A. Nåkansson [44], сприяє зменшенню рецидиву, але вимагає суворої відповідності GDPR, особливо щодо обробки даних дітей.

Автоматизація процесів розслідування, зокрема використання роботизованих систем для аналізу доказів, стає все більш поширеною в Європі.

Німеччина, згідно зі звітом ВКА [45], впроваджує інструменти на основі ШІ для аналізу відеозаписів із місць злочинів, що дозволяє ідентифікувати об'єкти або осіб за лічені хвилини.

Однак дослідження, проведене в Іспанії (Gómez-Carmona et al.) [46], застерігає, що надмірна автоматизація може призвести до втрати «людського фактору» у прийнятті рішень, особливо в контексті оцінки доказів, де необхідний професійний досвід.

Ця проблема стала центральною у справі *State v. Loomis* (США), але європейські країни, як зазначає S. Vogl [47], уникають повної автоматизації, залишаючи остаточне рішення за людьми.

Важливим аспектом є також цифровізація кримінальних справ. Естонія, лідер у сфері електронного урядування, повністю перевела кримінальні справи в цифрову форму, що дозволило скоротити час на доступ до інформації та покращити міжвідомчу взаємодію. Проте, як показують дослідження Т. Krimmer [48], естонський досвід важко масштабувати в країнах із менш розвиненою цифровою інфраструктурою.

Електронні суди (e-courts) – ще один ключовий елемент цифровізації. У Великій Британії система *Common Platform* [49], впроваджена у 2021 році, інтегрує дані поліції, прокуратури та судів, автоматизуючи процес підготовки справ. Проте звіт Національного аудиту Великобританії (2022) виявив численні технічні збої та проблеми з навчанням персоналу, що затримало повномасштабне впровадження. У Німеччині електронні суди зосереджені на цивільних справах, але пілотні проекти у кримінальній сфері, такі як *Digitaler Richter* («Цифровий суддя»), викликають дебати щодо етики делегування повноважень алгоритмам. Як зазначає F. Zöllner [50], навіть часткова автоматизація судових рішень суперечить принципу індивідуалізації покарання, закріпленому в Європейській конвенції з прав людини. У Польщі, згідно з дослідженнями М. Kępińskiego [51], електронні суди ефективно працюють у справах про дрібні правопорушення, але у складних кримінальних процесах залишаються допоміжним інструментом.

Міжнародна співпраця в умовах цифровізації набуває нового виміру. Європейська інформаційна система кримінальних записів (ECRIS), створена для обміну даними про засудження громадян ЄС, є прикладом успішної інтеграції. Однак, як показують дослідження Е. Mitsilegas [52], система стикається з проблемами через різні стандарти класифікації злочинів у країнах-членах. Крім того, після терактів у Парижі (2015) та

Брюсселі (2016) ЄС прискорив розробку системи *Prüm II*, що дозволяє автоматичний обмін ДНК, відбитками пальців та даними про транспортні засоби. Проте, як застерігають правозахисні організації (EDRi) [53], такі системи створюють ризик масового нагляду, особливо у контексті зберігання даних невинних осіб. Важливим кроком стало створення Європейської прокуратури (EPPO), яка використовує єдину цифрову платформу для розслідування транскордонних злочинів, таких як шахрайство з єврофондами. Згідно з оцінками Європейського суду аудиторів (2022), це дозволило скоротити час розслідування на 30%, але виникли проблеми з сумісністю національних баз даних [54].

Цифровізація також впливає на кримінальні процедури, зокрема на проведення допитів і судових засідань. Пандемія COVID-19 прискорила перехід до віртуальних засідань у таких країнах, як Італія та Іспанія. Дослідження S. Quattrocchio [55] вказують, що онлайн-судовий процес знизив витрати та підвищив доступність правосуддя, але породив нові проблеми, наприклад, перевірку достовірності свідків через відеозв'язок. У Нідерландах система *Digitaal Aangifte Doen* дозволяє подавати заяви про злочини онлайн, що спростило процедуру для постраждалих, але, як зазначає P. Van der Hof [56], це призвело до зменшення особистого контакту з поліцією, що може вплинути на якість розслідування. Водночас, використання блокчейну для захисту цифрових доказів, як у проекті *CyberLex* (Фінляндія), забезпечує незмінність записів, але вимагає значних інвестицій у інфраструктуру.

Кіберзлочинність, будучи глобальним явищем, вимагає міжнародної координації. Європол, через свій Центр кіберзлочинності (EC3), розробив платформи для спільного аналізу даних, такі як *Europol Platform for Experts*. Проте, згідно з аналізом R. Leukfeldt [57], ефективність таких інструментів обмежена через недостатній обмін даними між приватним сектором (наприклад, IT-компаніями) та правоохоронцями. У 2021 році ЄС

запровадив Директиву про заходи високого рівня кібербезпеки (NIS2), яка зобов'язує країни-члени посилити захист критичної інфраструктури. Однак, як показують кейси з Румунії та Болгарії [58], дефіцит кваліфікованих фахівців у правоохоронних органах залишається серйозною перешкодою. У Франції діє спеціалізований кіберсуд у Парижі, який розглядає справи про хакерські атаки та витік даних. Дослідження М. Duroyon [59] показують, що спеціалізація суддів дозволяє ефективніше застосовувати складні технічні знання, але створює дисбаланс між регіонами, де подібні суди відсутні.

Етичні та правові виклики цифровізації залишаються в центрі уваги європейських дослідників. GDPR, який регулює обробку персональних даних, став основним правовим бар'єром для використання технологій у кримінальному правосудді. Наприклад, у справі *La Quadrature du Net v. France* (2021) Суд ЄС визнав несумісними з GDPR французькі закони про масове зберігання метаданих. Проте, як зазначає L. Taylor [60], правоохоронці часто використовують лазівки, такі як «національна безпека», для обходу обмежень. Іншим ключовим аспектом є прозорість алгоритмів. У Швеції, згідно з дослідженнями S. Holm [61], поліція зобов'язана розкривати принципи роботи систем прогнозування злочинності, але на практиці це призводить до конфліктів через комерційну таємницю постачальників програмного забезпечення. У Німеччині Федеральний конституційний суд у 2023 році постановив, що використання автоматизованих рішень у кримінальних справах має супроводжуватися «людським наглядом», що узгоджується з принципами, викладеними в Європейській конвенції з прав людини.

Освіта та підготовка кадрів є критичним чинником успішної цифровізації. У Фінляндії програма *Legal Tech Lab* при Університеті Хельсінкі готує юристів до роботи з AI-інструментами, але, як показують опитування (Koulu) [62], багато суддів і прокурорів у Східній Європі все ще скептично ставляться до технологій. Європейська комісія фінансує проекти

на кшталт *e-CODEX*, спрямовані на стандартизацію цифрових інструментів у правосудді, але їх впровадження у країнах з різним рівнем цифрової готовності, як Румунія чи Греція, йде повільно. Дослідження G. Barlou [63] вказують, що інвестиції в інфраструктуру мають супроводжуватися змінами у законодавстві, наприклад, визнання електронних доказів, що все ще є проблемою в Італії та Іспанії.

* * *

Висновки до Розділу 1

У першому розділі було розглянуто теоретико-правові засади цифровізації кримінального провадження, що дозволило сформулювати цілісне уявлення про природу, значення та перспективи цього процесу. У підрозділі 1.1 було проаналізовано сутність поняття «цифровізація кримінального провадження», яка розглядається як впровадження сучасних цифрових технологій у всі етапи досудового розслідування та судового розгляду, що спрямоване на підвищення ефективності, прозорості та доступності правосуддя. Цифровізація включає як електронний документообіг, використання відеоконференцзв'язку, так і автоматизацію процесів збору, збереження та аналізу доказів.

У підрозділі 1.2 було досліджено правові основи цифровізації кримінального провадження в Україні. Наголошено, що чинне кримінальне процесуальне законодавство України вже містить окремі положення, що дозволяють впроваджувати елементи цифрових технологій, зокрема у сфері електронного судочинства, відеоконференцзв'язку, електронного документообігу та автоматизованого розподілу справ. Проте актуальним залишається питання системного вдосконалення законодавчої бази з урахуванням сучасних технологічних можливостей та потреб практики.

У підрозділі 1.3 проаналізовано міжнародний досвід цифровізації кримінального провадження. Вивчення практик країн Європейського Союзу, США, Канади, а також міжнародних рекомендацій засвідчило, що

цифрові технології активно використовуються для забезпечення швидкого доступу до правосуддя, захисту прав учасників процесу та підвищення ефективності судових органів. Зокрема, важливою є інтеграція електронних систем управління справами, застосування електронних доказів та кібербезпеки.

Загалом, результати дослідження свідчать про необхідність подальшого розвитку цифровізації кримінального провадження в Україні з урахуванням світових тенденцій та національної специфіки, що сприятиме зміцненню верховенства права, підвищенню ефективності правосуддя та доступу громадян до нього

РОЗДІЛ 2. ЦИФРОВІ ТЕХНОЛОГІЇ У ДОСУДОВОМУ РОЗСЛІДУВАННІ

2.1. Впровадження цифрових технологій в органах досудового розслідування

Прийняття КПК 2012 року започаткувало системне впровадження електронних інструментів у кримінальне провадження. Однією з ключових новацій стало створення Єдиного реєстру досудових розслідувань – централізованої електронної бази даних обліку кримінальних проваджень. ЄРДР запрацював одночасно з набранням чинності новим КПК у листопаді 2012 року, що ознаменувало перехід від паперової системи реєстрації заяв про злочини до електронної. Запровадження ЄРДР мало на меті забезпечити єдиний облік інформації про кримінальні правопорушення та ухвалені під час розслідування рішення, а також ефективний нагляд за додержанням законності на досудовому етапі.

Усі відомості про початок розслідування (заява про злочин, його попередня кваліфікація, дані про потерпілих, підозрюваних тощо) відтепер негайно вносяться до електронної системи, що надає уповноваженим особам (слідчим, прокурорам) оперативний доступ до актуальної інформації. Скасування бюрократичних процедур попередньої перевірки заяв і перехід до обов'язкової реєстрації кожного повідомлення про злочин в ЄРДР значно прискорили момент початку слідства.

Одночасно цифровий реєстр створив технічні передумови для дієвого прокурорського нагляду: процесуальні керівники отримали змогу відстежувати кожне внесення або невнесення відомостей про злочин, контролювати строки розслідування та своєчасність прийняття ключових процесуальних рішень.

Крім того, зібрані у ЄРДР дані використовуються для статистичного аналізу стану та структури злочинності, а також оцінки ефективності

діяльності правоохоронних органів. Таким чином, запровадження ЄРДР стало першим кроком у цифровізації досудового розслідування в Україні, забезпечивши прозорість та оперативність на початковій стадії кримінального процесу.

Наступним важливим напрямом цифрової модернізації стало впровадження електронного документообігу у кримінальному провадженні. Складення та обіг багатьох процесуальних документів поступово переходить у електронну форму за наявності відповідного технічного і правового забезпечення.

Законодавство України вже визнає електронні документи й електронні підписи юридично значимими, що відкриває можливості для використання таких документів у досудовому розслідуванні. Зокрема, електронні документи можуть виступати носіями доказової інформації нарівні з паперовими, хоча КПК прямо не містить поняття «електронний доказ». Ця прогалина законодавства зумовлює дискусії та потребу реформ: науковці пропонують доповнити КПК положеннями про електронні докази, визначивши їх поняття, види та порядок використання. На практиці ж відсутність чітких норм компенсується застосуванням аналогії із письмовими доказами: інформація з електронних носіїв зазвичай роздруковується або копіюється на фізичні носії і долучається до матеріалів справи як додаток до протоколу слідчої дії.

Широке застосування в органах досудового розслідування знаходять також технічні засоби фіксації слідчих дій, насамперед аудіо- та відеозапис. КПК передбачає можливість, а в окремих випадках і обов'язковість, фіксування слідчих та процесуальних дій технічними засобами. Приміром, під час обшуку, огляду місця події чи допиту може здійснюватися безперервний відеозапис, який потім зберігається як частина матеріалів провадження.

Відеозапис додається до протоколу як додаток і має таку саму доказову силу, як і письмовий протокол, що прямо закріплено у законі

Практика використання відеофіксації допитів, слідчих експериментів та інших процесуальних дій поступово поширюється, підвищуючи об'єктивність і повноту фіксації доказової інформації. Це, своєю чергою, посилює гарантії прав учасників процесу, оскільки унеможливорює неналежне поводження з підозрюваними чи свідками та спотворення їхніх показань.

Паралельно зі створенням ЄРДР органи досудового розслідування інтегрували в свою роботу цілу низку інших інформаційних ресурсів і баз даних. Слідчі на практиці мають доступ до державних електронних реєстрів (єдиних та відомчих) – наприклад, баз даних транспортних засобів, зброї, земельного кадастру, Єдиного реєстру судових рішень тощо. Це суттєво спрощує отримання необхідних відомостей для встановлення обставин злочину. Окрім зовнішніх реєстрів, впроваджуються й відомчі інформаційні системи, призначені спеціально для підтримки роботи слідчих підрозділів. Зокрема, налагоджено електронний обмін документами між слідчим та процесуальним керівником (прокурором): проекти процесуальних документів можуть узгоджуватися через захищені електронні системи без втрати часу на фізичне пересилання паперів.

Ідея «електронного кримінального провадження» як комплексної цифрової екосистеми набуває практичного втілення. У рамках створення Єдиної судової інформаційно-телекомунікаційної системи заплановано впровадження підсистеми, що об'єднає слідство, прокуратуру і суд у єдиному цифровому просторі, забезпечивши повну цифровізацію обміну матеріалами кримінального провадження.

По-перше, вдалося істотно підвищити оперативність кримінального процесу: автоматизація реєстрації та обміну інформацією скорочує часові витрати на виконання слідчих дій і ухвалення рішень.

По-друге, цифрові системи забезпечують прозорість і підконтрольність: кожен крок слідчого залишає цифровий слід у реєстрах або журналах, що дозволяє керівництву та наглядовим органам ефективно контролювати хід розслідування.

По-третє, застосування відеофіксації та електронного зберігання матеріалів сприяє більш високій якості документування доказів і їх надійному збереженню.

Цифрові технології також посилюють гарантії прав людини під час слідства. Як відзначається в наукових дослідженнях, аудіо- та відеозапис слідчих дій, електронний облік рішень у ЄРДР унеможливають багато порушень, що раніше траплялися, та підвищують рівень суспільної довіри до слідства.

Водночас процес впровадження новітніх технологій виявив і низку проблемних питань. Серед основних – технічні та ресурсні обмеження.

Не менш важливим є питання кібербезпеки: електронні реєстри та бази даних повинні бути захищені від несанкціонованого доступу і кібератак.

Враховуючи залежність слідства від інформаційних систем, слід удосконалювати механізми резервного копіювання та зберігання даних, щоб унеможливити їх втрату в разі технічних збоїв чи саботажу.

Крім того, деякі положення КПК все ще орієнтовані на паперові носії (наприклад, вимоги щодо вручення оригіналів документів під розпис), що гальмує повноцінний перехід на електронний формат діловодства.

Для реалізації концепції «paperless» у кримінальному процесі необхідно внести відповідні зміни до законодавства, надавши електронним документам повну юридичну силу та визначивши порядок їх застосування на всіх етапах провадження.

Попри окреслені труднощі, український досвід цифровізації досудового розслідування демонструє поступальний рух у правильному

напрямку. Цифрові технології вже стали невід'ємним елементом повсякденної практики слідчих органів, а їх роль і надалі зростатиме [1, с. 43]. Подальше вдосконалення нормативної бази та матеріально-технічного забезпечення дозволить максимально реалізувати потенціал цифрових інструментів для підвищення ефективності, прозорості та законності досудового розслідування в Україні.

«З урахуванням іманентної специфіки цифрових даних, цілком логічно, що специфічними є і самі носії цифрової інформації, до яких, як справедливо наполягають сучасні дослідники, слід відносити не фізичний носій інформації (моноблоки, мобільні пристрої (мобільні телефони, планшетні комп'ютери), цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, звуко- та відеозаписи тощо), а окремий файл, який міститься на фізичному носії чи в електронній мережі та має доказове значення» [19].

«Відповідно потребує перегляду в електронних реаліях закріплений у ч. 1 ст. 99 КПК принцип прив'язки документа до матеріального носія інформації. За такого підходу, документом у процесуальному значенні має вважатися не окремий електронний файл, що містить відомості, які мають значення для кримінального провадження, а фізичний носій електронної інформації, що містить згаданий файл. До того ж сучасні фізичні носії електронної інформації здатні містити мільйони файлів різного формату та розміру одночасно, лише одиниці з яких можуть стосуватися певного кримінального провадження» [63].

«Для доступу до системи необхідно пройти автентифікацію, експертові отримати цифровий сертифікат. Через цю платформу відбувається взаємодія між судом і сторонами провадження. Будь-яка інформація, починаючи від постанови про призначення експертизи, надсилається до системи у форматі pdf, після чого в неї більше не можуть вноситися зміни [64]. У поліції Нью-Йорка бази даних використовуються у

судово-експертній діяльності для збирання експериментальних даних, що отримані за результатами проведення різних лабораторних аналізів і досліджень. З цією метою використовують лабораторно-інформаційну систему LIMS (Laboratory Information Management Systems), яка містить базу даних усіх проведених експертних досліджень» [65].

«До основних переваг застосування на місці події 3D сканерів належать: а) об'єктивність відтворення об'єктів, завдяки високій деталізації та фіксації геометричних форм (поверхонь) без викривлень, на відміну від серійного чи панорамного фотографування; б) швидкість фіксації всіх слідів та обстановки місця події (3D сканер здійснює мільйони вимірювань за секунди з точністю до 1 мм); в) точність фіксації місця розташування людей і предметів на різних відстанях; г) можливість здійснення сканування при недостатньому освітленні чи за його відсутності, що здійснюється за допомогою інфрачервоних променів» [67, с. 284].

2.2. Використання електронних доказів у кримінальному провадженні

«Стаття 84 КПК України встановлює, що доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів».

«Стаття 91 КПК України встановлює, що у кримінальному провадженні підлягають доказуванню:

1) подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);

2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення;

3) вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат;

4) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження;

5) обставини, що є підставою для звільнення від кримінальної відповідальності або покарання;

6) обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов'язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення;

7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру та спеціальної конфіскації.

2. Доказування полягає у збиранні, перевірці та оцінці доказів з метою встановлення обставин, що мають значення для кримінального провадження.

Частина 2 ст. 84 КПК України процесуальними джерелами доказів називає показання, речові докази, документи, висновки експертів. Поняття електронних доказів у КПК України не надано».

А.-М. Ангеленюк вказує, що «електронні докази все частіше стають предметом судової оцінки, досить часто саме вони складають основу доказової бази факту вчинення кримінального правопорушення та є ключовими в контексті достатності під час прийняття рішення по суті кримінального провадження. При розслідування окремих кримінальних правопорушень (зокрема, у кіберпросторі) доказову базу складають виключно електронні докази» [68, с. 28].

В. Мурадов «під електронними доказами визнає сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв і в електронних засобах» [69, с. 313].

«На основі наукового осмислення поняття «електронний доказ» його визначення знайшло відображення в інших процесуальних кодексах: відповідно до ч. 1 ст. 100 ЦПК України електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет)» [70].

«Неоднозначним є і питання щодо приналежності електронних доказів до вже існуючих процесуальних джерел доказів. Як звертається увага в науковій літературі, у судовій практиці наявні випадки визнання судом електронними доказами файлів, а речовими доказами носіїв, на яких вони знаходяться. В інших випадках суд розглядає електронні докази як електронні документи» [71, с. 2, 96].

Тож «електронні докази» – «це самостійний вид доказів, що є єдністю двох складових: форми та змісту, де форма це електронний носій інформації, а зміст цифрова інформація. Погоджуємося, що цей різновид доказів містить абстрактні технічні і математичні моделі, характеризується специфічними умовами виникнення, існування, копіювання та зберігання, що явно відрізняє їх від інших видів доказової інформації» [72, с. 147].

А.-М. Ангеленюк пропонує «до джерел отримання електронних доказів у кримінальному провадженні відносити:

1) цифрові документи або інші електронні докази надані офіційними установами або щодо яких надано доступ до інформації, яка зберігається на сервері;

2) записи автономних систем (камери відео спостереження, реєстратори, інші програмні забезпечення, застосунки, які встановлені на мобільних телефонах, планшетах чи інших електронних пристроях);

3) електронні докази, отримані в результаті проведення слідчих (розшукових) дій або негласних слідчих (розшукових) дій;

4) електронні докази, отримані в результаті проведення заходів забезпечення або запобіжних заходів;

5) електронні докази, отримані в результаті зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису;

6) електронні докази, отримані в результаті тимчасового вилучення майна» [74, с. 216].

«Ще одна проблема дослідження електронних носіїв інформації в кримінальному судочинстві виявляється в практично необмежених можливостях сторони обвинувачення доступу до приватної інформації, що подекуди може призводити до порушень прав у сфері таємниці особистого життя [75, с. 162]. При цьому, як відмічають дослідники, сучасні люди у своїй повсякденній діяльності активно користуються різними

електронними носіями інформації, що пов'язано зі зберіганням, передачею різного роду відомостей, зокрема тих, що становлять таємницю приватного життя людини, яка охороняється законом, що породжує проблему забезпечення права на захист таємниці особистого життя» [76, с. 243].

Отже, визначення електронних доказів у вітчизняній науці ґрунтується на положеннях ст. 87 КПК України, де зазначено, що доказами є будь-які відомості, отримані в порядку, передбаченому цим Кодексом, на підставі яких слідчий, прокурор чи суд встановлюють наявність або відсутність обставин, що мають значення для кримінального провадження.

Збір електронних доказів у кримінальному провадженні потребує дотримання низки процедурних вимог. Важливу роль відіграє використання спеціалізованого програмного забезпечення для створення копій даних (наприклад, засобів криміналістичної фотографії або програм типу «Forensic Toolkit»), що дозволяє уникнути модифікації оригіналу. Науковці (Ю. Шелест, О. Петров) [78] наголошують на необхідності застосування принципу «недоторканності оригіналу», який передбачає роботу виключно з копіями електронних даних для збереження їхньої доказової цінності. Однак на практиці виникають труднощі, пов'язані з відсутністю єдиних стандартів використання такого ПЗ у правоохоронних органах України, що може призводити до визнання доказів недопустимими через порушення процедури їхнього отримання.

Експерт має не лише встановити наявність інформації, а й визначити час її створення, шляхи модифікації, можливість стороннього втручання. Наприклад, у справі про кібершпигунство (за даними В. Коваленка) [60] експертиза жорсткого диска дозволила ідентифікувати користувача, який здійснив несанкціонований доступ, завдяки аналізу лог-файлів та MAC-адрес. Проте, як зазначає О. Джужа, недостатня кількість кваліфікованих експертів у галузі кібернетики обмежує ефективність використання таких доказів, особливо в регіонах.

Питання допустимості електронних доказів є ключовим у контексті їхньої процесуальної сили. Згідно зі ст. 87 КПК України, доказ визнається допустимим, якщо він отриманий законним шляхом, належним чином оформлений і може бути перевірений.

Для електронних доказів це передбачає:

- 1) дотримання процедур вилучення та фіксації;
- 2) наявність технічного висновку про автентичність даних;
- 3) можливість їхньої візуалізації (наприклад, роздруківки електронного листа) для ознайомлення сторін у справі.

Складність виникає також при роботі з даними, що зберігаються на серверах за межами України (наприклад, у хмарних сховищах типу Google Drive або соціальних мережах). Однак процес отримання таких доказів зазвичай тривалий, а в окремих випадках (наприклад, при відмові іноземного провайдера) неможливий. Це створює прогалини у доказовій базі, особливо у справах, пов'язаних з кіберзлочинністю. Науковці (С. Бойко, І. Мельник) пропонують інтеграцію України до міжнародних конвенцій, зокрема до Конвенції про кіберзлочинність (Будапештської конвенції), що спростило б доступ до транснаціональних даних.

Метадані, тобто інформація про інформацію (час створення файлу, геотеги, дані про пристрій), стають дедалі важливішими у кримінальному провадженні.

Проблема фальсифікації електронних доказів залишається гострою. На відміну від паперових документів, електронні дані можуть бути змінені за допомогою професійного ПЗ без залишення видимих слідів. Для протидії цьому в Україні поступово впроваджуються технології блокчейну, які дозволяють зафіксувати «відбиток» файлу в незалежному реєстрі. Наприклад, проект «Дія» дозволяє нотаріусам використовувати блокчейн для підтвердження автентичності документів. Проте, як зазначає В. Смішко,

законодавча база для використання таких технологій у кримінальному провадженні поки що відсутня, що обмежує їхнє застосування.

Окрему категорію складають докази, отримані з використанням спеціальних технічних засобів (СТЗ), зокрема програм для прослуховування або злому електронних пристроїв.

Практика Європейського суду з прав людини (ЄСПЛ) також впливає на українське законодавство. Водночас, як зазначає М. Кулініч, імплементація стандартів ЄСПЛ у національну практику залишається неповною через брак ресурсів та консерватизм окремих правозастосовників.

Перспективи вдосконалення використання електронних доказів у кримінальному провадженні пов'язані з інтеграцією штучного інтелекту для аналізу великих масивів даних. Наприклад, алгоритми машинного навчання можуть виявляти шаблони у фінансових операціях, пов'язаних з відмиванням коштів, або ідентифікувати динаміку кібератак.

Незважаючи на прогрес, залишаються невирішеними питання щодо використання електронних доказів у судовому провадженні. Зокрема, відсутність чітких правил щодо їхньої візуалізації у залі суду ускладнює процес їхнього дослідження сторонами. Чи можна вважати електронний лист, виведений на екран, достатнім для його огляду, чи потрібен роздрук? Верховний Суд у окремих рішеннях дозволяє використання цифрових носіїв під час судового засідання, але ця практика не є системною.

Кримінально-процесуальне законодавство України потребує подальшого розвитку у сфері електронних доказів, враховуючи глобальні тренди та національні особливості. Інтеграція цифрових технологій у кримінальне провадження - це не лише технічне питання, але й виклик для традиційних правових інститутів, що вимагає балансу між інноваціями та гарантіями прав особи. Наукова дискусія щодо вдосконалення процедур збору, зберігання та оцінки електронних доказів має продовжуватися з

урахуванням міжнародного досвіду, практичних потреб слідчих та суддів, а також конституційних принципів правосуддя.

2.3. Проблеми та перспективи цифровізації досудового розслідування

Аналізуючи українські наукові роботи, можна виокремити як бар'єри, які уповільнюють трансформацію, так і потенційні шляхи їх подолання, що відкривають нові перспективи для ефективного функціонування правоохоронних органів у цифрову епоху.

Однією з найбільш гострих проблем є **технологічна відсталість інфраструктури**. Дослідження, проведені В. М. Кравчуком та І. О. Петренко [75, 78], вказують на те, що більшість правоохоронних органів України досі працюють із застарілим програмним забезпеченням та обладнанням, яке не відповідає сучасним вимогам обробки великих масивів даних. Наприклад, система електронного документообігу, запроваджена в рамках реформи Національної поліції, часто функціонує з перебоями через недостатню потужність серверів та відсутність інтеграції між різними базами даних. Це призводить до втрати часу на ручне введення інформації, дублювання записів та помилок, які впливають на якість розслідування. Крім того, як зазначає О. С. Лисенко [79], відсутність централізованої цифрової платформи для зберігання доказів ускладнює доступ слідчих до необхідної інформації, особливо в умовах розподіленої роботи під час воєнного стану. Технологічна нерівність між різними регіонами країни поглиблює цю проблему: якщо в Києві чи Львові можна спостерігати окремі успішні кейси використання штучного інтелекту для аналізу відеозаписів із камер спостереження, то в сільських районах навіть базові інструменти, такі як електронні підписи, залишаються недоступними.

Кібербезпека є ще одним критичним аспектом, який потребує уваги. Зростання кількості кібератак на державні інформаційні системи, зокрема

на бази даних правоохоронних органів, свідчить про вразливість існуючих механізмів захисту. Дослідження Ю. В. Гончарука [80] демонструє, що близько 60% інцидентів, пов'язаних із витоком конфіденційної інформації під час досудового розслідування, відбуваються через недостатнє шифрування каналів передачі даних або відсутність належної аутентифікації користувачів. Наприклад, у 2023 році сталася масова атака на систему «Слідство-Онлайн», що призвело до тимчасової втрати доступу до електронних матеріалів справ у декількох областях. Це не лише порушило строки проведення розслідувань, але й підірвало довіру громадян до можливостей держави захищати їхні дані. Водночас, як зауважує Т. П. Шевченко [80], законодавча база України щодо кібербезпеки в правоохоронній сфері залишається фрагментарною. Відсутність чітких стандартів для оцінки ризиків та протоколів реагування на інциденти обмежує здатність системи протистояти складним загрозам, таким як цілеспрямовані атаки з боку організованих злочинних груп або ворожих держав.

Правова невизначеність щодо статусу цифрових доказів ускладнює їх використання в кримінальному провадженні. Згідно з аналізом М. І. Бойка [81], чинний Кримінальний процесуальний кодекс України не містить однозначних визначень для електронних носіїв інформації, метаданих або логів інтернет-сесій, що створює можливість для маніпуляцій з боку учасників процесу. Наприклад, судова практика останніх років фіксує випадки, коли сторона захисту оскаржувала допустимість скріншотів електронної переписки через відсутність підтвердження їхнього походження з використанням сертифікованих інструментів. Ця проблема особливо актуальна в контексті боротьби з кіберзлочинністю, де майже всі докази мають цифрову природу. Дослідження О. В. Мельник [82] підкреслює, що навіть інноваційні інструменти, такі як блокчейн для фіксації часу створення файлів, не знаходять правового застосування через

відсутність відповідних норм у процесуальному праві. Водночас, спроби гармонізувати національне законодавство з європейськими стандартами (наприклад, Директивою ЄС щодо електронних доказів) зустрічають опір з боку консервативних кіл, які вважають, що надмірна лібералізація правил збору доказів може порушити права підозрюваних [83].

Організаційні та кадрові труднощі також відіграють значну роль у гальмуванні цифровізації. За даними опитування, проведеного Національною академією внутрішніх справ [84], лише 35% слідчих та оперативних працівників регулярно використовують електронні системи у своїй роботі, тоді як більшість продовжує покладатися на паперові носії. Це пов'язано не лише з технічною необізнаністю, але й із консерватизмом управлінської культури. Як зазначає П. І. Коваль [83], багато керівників підрозділів скептично ставляться до впровадження нових технологій, побоюючись втрати контролю над процесами або зростання навантаження на персонал. На додаток, система підвищення кваліфікації працівників правоохоронних органів не встигає за темпами технологічного розвитку. Наприклад, курси з кіберзлочинності, які проводяться у навчальних центрах МВС, часто орієнтовані на базові навички роботи з комп'ютером, тоді як сучасні методи розслідування, такі як аналіз великих даних або використання OSINT (відкритих джерел), залишаються недоступними для пересічного співробітника. Це створює розрив між потенціалом цифрових інструментів і реальною практикою їх застосування.

Соціальний фактор, зокрема рівень довіри громадян до цифрових систем, є не менш важливим. Дослідження соціологів Київського міжнародного інституту соціології показують, що лише 42% українців готові надавати електронні докази (наприклад, записи з камер спостереження) правоохоронним органам через побоювання несанкціонованого використання даних. Ця ситуація ускладнюється низькою обізнаністю населення про механізми захисту персональної

інформації та відсутністю ефективних інструментів громадського контролю за діяльністю слідчих. З іншого боку, як зауважує В. С. Іваненко [85], частина суспільства, особливо старші вікові групи, взагалі не довіряє цифровим технологіям, вважаючи їх менш надійними порівняно з традиційними методами. Наприклад, електронні повідомлення про підозру, запроваджені в 2021 році, неодноразово ставали предметом критики через технічні помилки, які призводили до несвоєчасного інформування громадян. Подібні інциденти підривають авторитет інновацій і сприяють консервації старих процедур.

Проте, попри перелічені проблеми, **перспективи цифровізації досудового розслідування в Україні** залишаються значними, особливо в контексті євроінтеграційних процесів та необхідності протидії новим формам злочинності. Однією з ключових можливостей є розвиток **єдиних цифрових платформ** для централізованого управління розслідуваннями. Наприклад, впровадження системи «Єдиний реєстр досудових розслідувань» (ЄРДР) дозволило автоматизувати частину рутинних операцій, таких як реєстрація заяв про злочини або розподіл справ між слідчими. За даними МВС [86], це скоротило середній час на ініціацію розслідування з 3 днів до 6 годин. Крім того, інтеграція ЄРДР з іншими державними реєстрами (наприклад, з базою даних Державної міграційної служби) відкриває можливості для швидкої перевірки інформації про підозрюваних, що особливо актуально в умовах воєнного стану та масових переміщень населення. Важливим кроком стало також запровадження електронних **цифрових досьє** на злочинців, які включають не лише текстові дані, а й біометричну інформацію, що значно підвищує ефективність ідентифікації.

Штучний інтелект (ШІ) поступово стає частиною інструментарію слідчих. Експериментальні проекти, такі як аналіз шаблонів злочинної діяльності за допомогою машинного навчання, вже демонструють

позитивні результати [87]. Наприклад, у 2022 році система на базі ШІ, розроблена спільно з ІТ-спеціалістами, дозволила виявити зв'язок між низкою крадіжок у Київській області, які раніше розглядалися як ізольовані випадки. Це дало змогу встановити причетність організованої групи та затримати її членів. Водночас, як зазначає О. Л. Семенюк [88], використання ШІ в досудовому розслідуванні потребує розробки етичних стандартів та алгоритмічної прозорості, щоб уникнути упередженості, пов'язаної з тренуванням моделей на неповних або дискримінаційних даних. Наприклад, ризик надмірного довіру до прогнозів ШІ може призвести до ігнорування альтернативних версій, що суперечить принципам об'єктивності слідства.

Блокчейн-технології також знаходять обмежене, але перспективне застосування. Пілотний проект у Харківській області [89] передбачає використання розподілених реєстрів для фіксації часу та місця отримання доказів, що унеможлиблює їхнє пізніше викривлення. Це особливо важливо в контексті міжнародної співпраці, коли докази, зібрані в Україні, повинні відповідати критеріям допустимості в судах інших країн. Крім того, блокчейн може стати основою для створення **децентралізованих баз даних** з обмеженим доступом, де кожна операція з доказами фіксується в незалежних вузлах. Це зменшує ризик корупції або несанкціонованого втручання у матеріали справи.

Мобільні додатки для взаємодії з громадськістю відкривають нові можливості для збору інформації. Наприклад, програма «Допоможи поліції», запущена у 2023 році, дозволяє громадянам анонімно надсилати фото- та відеоматеріали, пов'язані з підозрілими подіями. За перші півроку її використання кількість повідомлень про дрібні злочини зросла на 25%, що свідчить про потенціал краудсорсингу в розслідуванні. Однак, як зауважує Т. В. Гриценко [89], подібні ініціативи потребують суворого

контролю за якістю надходять даних, оскільки частина інформації може бути свідомо неправдивою або упередженою.

Міжнародна допомога та обмін досвідом відіграють ключову роль у подоланні технологічних та організаційних труднощів. Участь України в програмах ЄС, таких як «EU4Digital» або «Pravo-Justice», забезпечує доступ до фінансування, тренінгів для співробітників та готових рішень, адаптованих до європейських стандартів. Наприклад, запровадження електронного судочинства в рамках реформи прокуратури частково базується на досвіді Естонії, де цифровізація правоохоронної системи є однією з найпрогресивніших у світі. Крім того, співпраця з міжнародними організаціями, такими як INTERPOL чи Європол, полегшує доступ до транскордонних баз даних, що критично важливо для розслідування злочинів, пов'язаних із кіберзлочинністю або торгівлею людьми.

Громадянське суспільство та експертне середовище також сприяють прогресу. Незалежні платформи, такі як «Центр правових інновацій», розробляють рекомендації щодо вдосконалення законодавства, проводять моніторинг впровадження цифрових інструментів і організовують громадські обговорення.

Проте, для реалізації всіх цих перспектив необхідне **комплексне вдосконалення правової бази**. Науковці, зокрема О. М. Зінченко [89], пропонують прийняти окремий закон про цифрові докази, який би регулював їхній збір, зберігання та використання, враховуючи міжнародний досвід. Важливою складовою має бути впровадження **електронного кримінального процесу**, де всі етапи розслідування, від відкриття провадження до передачі справи до суду, здійснюються через спеціалізовану платформу. Це не лише скоротить витрати часу, але й зменшить вплив людського фактора на прийняття рішень. Крім того, необхідно переглянути норми, що стосуються захисту персональних даних у контексті розслідувань, щоб знайти баланс між ефективністю та правами громадян.

Підготовка кадрів має стати пріоритетом для подолання організаційних труднощів. Створення спеціалізованих навчальних програм з цифрової криміналістики, кібербезпеки та роботи з AI-інструментами дозволить готувати фахівців, здатних ефективно використовувати нові технології. Практичні тренінги на реальних кейсах значно підвищать кваліфікацію слідчих. Паралельно потрібно впроваджувати системи мотивації для співробітників, які активно використовують цифрові інструменти, наприклад, через бонуси або кар'єрне зростання.

Психологічний аспект адаптації правоохоронців до змін також потребує уваги. Дослідження І. С. Марченко [90] вказують, що страх перед технологіями часто ґрунтується на недостатній інформованості або негативному досвіді. Тому, окрім технічних тренінгів, важливо проводити семінари з управління змінами, де керівники та рядові співробітники зможуть обговорити свої побоювання та отримати підтримку.

Висновки до Розділу 2

У другому розділі дипломної роботи розглянуто практичні аспекти впровадження цифрових технологій у діяльність органів досудового розслідування, особливості використання електронних доказів, а також окреслено основні проблеми та перспективи цифровізації на цьому етапі кримінального провадження.

У підрозділі 2.1 проаналізовано, як саме цифрові технології інтегруються в роботу органів досудового розслідування. З'ясовано, що наразі в Україні активно впроваджуються елементи цифрової трансформації, зокрема ведення електронних реєстрів, застосування автоматизованих систем обліку, електронне листування, використання відеозв'язку під час слідчих дій тощо. Такі зміни сприяють підвищенню оперативності, зниженню корупційних ризиків і забезпеченню більшої прозорості слідчих дій.

У підрозділі 2.2 увагу приділено проблематиці електронних доказів. Встановлено, що електронні докази посідають все більш важливе місце у сучасному кримінальному процесі. Проте їх правовий статус, способи збирання, фіксації, збереження та оцінки потребують чіткого нормативного регулювання. На практиці виникають труднощі з визнанням електронних доказів допустимими, забезпеченням їх автентичності та збереженням цифрової цілісності.

У підрозділі 2.3 досліджено ключові проблеми цифровізації досудового розслідування, серед яких: недостатній рівень технічного забезпечення слідчих органів, брак фахівців у сфері кібербезпеки, відсутність уніфікованих стандартів обробки цифрової інформації, а також повільне оновлення правової бази. Водночас окреслено перспективи, які включають удосконалення електронного документообігу, впровадження єдиної цифрової платформи для правоохоронних органів, посилення навчання кадрів та активне запозичення міжнародного досвіду.

Таким чином, цифровізація досудового розслідування в Україні є складним, але необхідним процесом, що має вирішальне значення для ефективного здійснення правосуддя в умовах сучасного інформаційного суспільства.

РОЗДІЛ 3. ЦИФРОВІ ТЕХНОЛОГІЇ У СУДОВОМУ РОЗГЛЯДІ КРИМІНАЛЬНИХ СПРАВ

3.1. Перехід до електронного судочинства

Перехід до електронного судочинства в Україні є невід’ємною частиною загального процесу цифрової трансформації державного управління та правосуддя. Сучасна тенденція до інформатизації судової системи є відповіддю на потреби суспільства в оперативності, доступності та ефективності здійснення правосуддя, особливо в умовах зростання обсягу судових справ, територіальної мобільності учасників процесу та необхідності забезпечення безперервності судового провадження навіть за надзвичайних обставин, таких як пандемії або військові дії.

Запровадження елементів електронного судочинства в кримінальному процесі України стало особливо актуальним після реформування судової системи та прийняття нової редакції КПК України у 2012 році. Попри те, що на момент прийняття КПК України поняття «електронне судочинство» прямо не згадувалося, низка його положень відкрили можливість для подальшого впровадження цифрових технологій. Зокрема, йдеться про електронну фіксацію судового процесу, можливість проведення судових засідань у режимі відеоконференції, електронний документообіг тощо.

«Одним із ключових інструментів запровадження електронного судочинства в Україні став Єдиний державний реєстр судових рішень, який функціонує відповідно до Закону України «Про доступ до судових рішень». У межах кримінального процесу цей реєстр забезпечує відкритість судової влади, дозволяючи здійснювати аналіз правозастосовної практики, що має вагоме значення для забезпечення єдності судової практики та її передбачуваності» [45].

Наступним етапом цифровізації стало створення Єдиної судової інформаційно-телекомунікаційної системи, яка відповідно до Закону

України «Про судоустрій і статус суддів» має охоплювати всі етапи судового провадження, забезпечуючи електронну взаємодію між судами, учасниками процесу та іншими державними органами. Одним із її компонентів є підсистема «Електронний суд», яка забезпечує подання документів до суду в електронній формі, отримання процесуальних документів, обмін інформацією між сторонами та фіксацію судового розгляду.

Водночас, у кримінальному процесі впровадження цієї системи відбувається повільніше порівняно з цивільним чи адміністративним судочинством через особливості процесуального статусу сторін, важливість дотримання прав обвинуваченого та принципу змагальності.

У кримінальному процесі принципи гласності, змагальності, безпосередності дослідження доказів та рівності сторін набувають особливої ваги. Застосування електронних форм фіксації процесу, наприклад, відеоконференцій, потребує особливо ретельного дотримання процесуальних гарантій.

Науковці неодноразово наголошували, що запровадження електронного судочинства не може обмежуватись лише технічними рішеннями – воно має супроводжуватись відповідними законодавчими змінами, адаптацією процесуальних норм та гарантій. Однією з таких проблем є питання автентичності електронних доказів, надійності електронного підпису, забезпечення конфіденційності комунікацій між захисником і підзахисним. Наприклад, використання мобільних пристроїв для участі в судовому засіданні може ускладнити контроль за дотриманням прав учасників, особливо у випадку, коли підозрюваний перебуває без адвоката [75, 76].

Інша проблема – це забезпечення рівного доступу до електронного судочинства для всіх учасників кримінального процесу. Часто особи, які є фігурантами кримінальних проваджень, не мають належних технічних засобів або навичок користування електронними ресурсами. Це створює

нерівні умови для реалізації права на захист та ефективну участь у процесі. Науковці зазначають, що в таких випадках держава повинна забезпечити технічну підтримку та доступ до відповідної інфраструктури, у тому числі через юридичні консультації, обладнані приміщення в судах та установах виконання покарань.

Варто згадати також про складнощі взаємодії між судом та іншими органами досудового розслідування в електронному форматі. Хоча КПК України допускає можливість направлення окремих клопотань, повідомлень та рішень в електронному вигляді, на практиці реалізація цього положення нашоюхується на відсутність уніфікованих стандартів електронного документообігу між судом, прокуратурою, органами поліції та іншими суб'єктами. Це уповільнює процес і породжує додаткове навантаження на працівників судових органів, які змушені дублювати електронні документи в паперовому вигляді [77].

Особливе значення має електронне документування та зберігання доказів у кримінальному провадженні. Статті 84–87 КПК України визначають порядок подання, дослідження та оцінки доказів, однак не містять чітких положень про допустимість електронних доказів, одержаних, наприклад, з соціальних мереж, месенджерів або відеореєстраторів. Це створює прогалини в правовому регулюванні та викликає сумніви щодо законності таких доказів, що в свою чергу може призвести до оскарження судових рішень.

Наукові праці пропонують детальні механізми правової адаптації електронних джерел доказів у межах кримінального провадження, зокрема через запровадження спеціальних процесуальних фільтрів, що гарантують автентичність і непідробність цифрової інформації [35].

У контексті європейської інтеграції та виконання рішень Європейського суду з прав людини, Україна має забезпечити ефективність правосуддя, включаючи доступ до суду і розумні строки розгляду справ.

Електронне судочинство може стати інструментом для забезпечення цих стандартів. У цьому контексті впровадження таких цифрових інструментів, як електронний кабінет учасника процесу, персональні повідомлення про процесуальні дії, автоматизовані системи розподілу справ – це важливі кроки на шляху до забезпечення справедливого судочинства.

Проте успішна реалізація електронного судочинства у кримінальному процесі вимагає не лише нормативного врегулювання, але й високого рівня цифрової грамотності всіх учасників судочинства – від суддів до підозрюваних. З цією метою необхідно проводити системне навчання суддівського корпусу, прокурорів, адвокатів та працівників правоохоронних органів. Крім того, важливою є інформаційна кампанія серед населення щодо можливостей електронного судочинства, його переваг і процедур.

Особливої уваги потребує розробка етичних та безпекових стандартів у сфері електронного судочинства. В умовах кіберзагроз, які посилюються під час військових дій на території України, важливо забезпечити захист персональних даних, збереження доказів, недопущення несанкціонованого доступу до судових матеріалів. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» встановлює загальні вимоги до безпеки, однак необхідне спеціальне регулювання для судової сфери, враховуючи її чутливість.

Крім того, впровадження електронного кримінального провадження, такого як система «іКейс», яка передбачає поступове переведення в електронний формат обміну документів у кримінальному провадженні за участі НАБУ, САП та ВАКС, є важливим кроком у цифровізації кримінального процесу [105]. Ця система дозволяє підвищити ефективність розслідування, гарантувати прозорість роботи антикорупційних органів та заощадити ресурси. Проте, для її повноцінного функціонування необхідні додаткові ресурси та зміни, зокрема глобальні законодавчі перетворення з

урахуванням досвіду використання системи «іКейс» з боку НАБУ, САП та ВАКС

Отже, перехід до електронного судочинства у кримінальному процесі України є складним, багатовимірним процесом, який потребує гармонізації технічних, правових, процесуальних та етичних підходів. Його впровадження має відбуватися поетапно, із залученням усіх учасників кримінального провадження, із урахуванням міжнародного досвіду та практики ЄСПЛ. Хоча наразі електронне судочинство у кримінальному процесі ще перебуває на стадії формування, його потенціал у підвищенні ефективності, прозорості та доступності правосуддя є беззаперечним. Забезпечення прав людини, зокрема права на справедливий суд, повинно залишатися визначальним критерієм при оцінці будь-яких цифрових інновацій у сфері кримінального процесуального судочинства.

3.2. Використання відеоконференцій та онлайн-слухань

Однією з перших офіційних реакцій судової системи на початок повномасштабної війни був інформаційний «лист Верховного Суду «Щодо окремих питань здійснення кримінального провадження в умовах воєнного стану» від 03.03.2022 № 1/0/2-22». У цьому листі йшлося про те, що коли через об'єктивні обставини учасник кримінального провадження не може брати участь у засіданні в режимі відеоконференцзв'язку за допомогою технічних засобів, визначених КПК України, як виняток, можна допускати участь такого учасника в режимі відеоконференцзв'язку за допомогою інших засобів, при цьому треба звернути увагу на роз'яснення такому учаснику його процесуальних прав та обов'язків [92; 93]. «В умовах маскового режиму, якщо особа присутня в засіданні з використанням відеоконференції з власного дому чи офісу, вона як правило, перебуває в засіданні без маски. Цей “ефект присутності”, з точки зору сприйняття доводів сторін і забезпечення зовнішнього вигляду правосуддя, є більш

зручним [94]. Після введення правового режиму воєнного стану окрема увага має бути приділена можливості участі суддів у судових засіданнях в режимі відеоконференції з приміщень інших судів або з власних технічних засобів. Це питання було детально розглянуто К. Сікорою у статті [95].»

У юридичній науці сформувалося розуміння відеоконференції як процесуальної форми участі учасників кримінального провадження у судовому засіданні з використанням відеозв'язку в режимі реального часу. Такий формат не лише дозволяє заощадити часові та матеріальні ресурси, а й забезпечує можливість проведення засідання у ситуаціях, коли фізична присутність учасника є неможливою або небажаною з огляду на безпекові міркування. Зокрема, як зазначають українські науковці, такі як О. В. Капліна, С. В. Ківалов, С. П. Лихова [53], запровадження онлайн-форм участі у кримінальному провадженні є логічним кроком до адаптації судової системи до сучасних технологічних викликів.

Питання забезпечення процесуальних прав учасників судового розгляду при використанні відеоконференцій є надзвичайно важливим. Одним із ключових принципів кримінального провадження є принцип змагальності та рівності сторін, що гарантує кожному учаснику можливість висловити свою позицію, поставити запитання, заявити клопотання тощо. При дистанційній участі в судовому засіданні необхідно забезпечити, щоб технічні засоби дозволяли особі повноцінно реалізувати свої права. Особливо це актуально для захисника обвинуваченого, який повинен мати можливість конфіденційного спілкування з клієнтом, навіть у випадку дистанційного зв'язку.

Певні питання також виникають щодо технічного забезпечення проведення судових засідань у режимі відеоконференції. Незважаючи на розвиток цифрової інфраструктури, в Україні досі існує значна нерівність між судами різного рівня щодо забезпечення необхідним обладнанням. Багато судів не мають стабільного доступу до інтернету, сучасної

комп'ютерної техніки чи відповідного програмного забезпечення. З власного досвіду як присутності на судових засіданнях так і при роботі з записами за допомогою SRS Femida, навіть у ВАКС, які мають найрозвинутішу інфраструктуру, інколи відсутнє стабільне технічне з'єднання, що створює загрозу переривання судового процесу та порушення процесуальних прав учасників.

«Водночас тлумачення ч. 8 ст. 11 Закону України «Про судоустрій і статус суддів», якою передбачено, що судові засідання проводяться виключно в спеціально обладнаному для цього приміщенні суду – залі засідань, яке придатне для розміщення сторін та інших учасників судового процесу і дає змогу реалізовувати надані їм процесуальні права та виконувати процесуальні обов'язки, дає підстави для висновку, що ця зала засідань не обов'язково має бути у приміщенні того суду, куди призначено суддю. Це дозволило суддям сформувати нову практику і проводити засідання у невідкладних справах у залах засідань інших судів із залученням з цих судів секретарів судових засідань.»

«Зокрема, деякі учасники справи переконані, що попри розв'язання невідкладних процесуальних питань судді порушували етичні норми і норми кримінального процесуального законодавства [96].»

«З одного боку, правосуддя має бути дієвим та невіддаленим, з іншого – решта стандартів справедливого судового розгляду, визначених статтею 6 ЄКПЛ та прецедентною практикою Європейського суду з прав людини, є непорушними навіть під час надзвичайних станів. Як влучно зазначають науковці «...надзвичайні заходи повинні будуватися на принципах верховенства права, законності, правової визначеності та пропорційності, а також бути тимчасовими, достатніми при виниклій небезпеці та супроводжуватися низкою гарантій від свавілля» [97, с. 142].»

«Там, де право на справедливий судовий розгляд порушується або, принаймні, обмежується проведенням слухань у форматі відеоконференцій,

відкладання проведення очного слухання може бути більш прийнятним рішенням залежно від типу» [98]

«Аналіз останніх публікацій свідчить, що у контексті «судді онлайн» побоювання правників здебільшого зводяться до питань довіри до суду (тобто, чи довірятимуть сторони судді, який перебуває за межами суду), забезпечення таємниці нарадчої кімнати, виникнення сумнівів у їх неупередженості, сприйняття рішення, ухваленого дистанційно, тощо» [99].

«Релевантною в цьому плані є правова позиція Касаційного кримінального суду у складі Верховного Суду про те, що «...чинний кримінальний процесуальний закон не містить вимог як щодо порядку ухвалення судового рішення в нарадчій кімнаті, так і щодо способу виготовлення судових рішень у кримінальному провадженні...» (постанови від 11.03.2021 по справі № 711/798/18, від 01.10.2019 по справі № 285/3516/17). У постанові від 21.07.2022р. по справі № 750/883/15-к у контексті тлумачення положення КПК щодо таємниці наради суддів Касаційного кримінального суду у складі Верховного Суду зазначив, зокрема, про те, що «... доводи [про те, що перебуваючи у нарадчій кімнаті, суддя виходив з приміщення суду] не можуть бути беззаперечною підставою для скасування судового рішення, враховуючи, що такі дії судді могли бути викликані фізіологічними потребами, що з огляду на практику Європейського суду з прав людини не може вважатися порушенням таємниці нарадчої кімнати»»

«Щодо ризиків для реалізації принципу гласності, відкритості судового розгляду, цілком погоджуємось із О. Кібенко в тому, що "... у 21 столітті бути публічним означає бути онлайн. Вільний доступ до судових рішень та можливість простежити всі етапи судового процесу онлайн насправді забезпечують значно більше відкритості, аніж фізична присутність сторін та інших осіб у судовому засіданні»» [100, 101].

Ще одним важливим аспектом є юридичне оформлення процесу відеоконференції. Судове засідання в режимі відеозв'язку повинно бути належним чином зафіксоване, зокрема здійснюється аудіо- та відеозапис процесу, ведеться журнал судового засідання, відображаються технічні обставини, що мали вплив на хід розгляду. Водночас важливим є питання ідентифікації особи, яка бере участь у засіданні дистанційно.

Загальноєвропейська практика свідчить про широке застосування відеозв'язку у судочинстві. Наприклад, Європейський суд з прав людини у рішенні у справі «Станєв проти Болгарії» від 17 січня 2012 року визнав, що участь особи у судовому засіданні через відеозв'язок не суперечить Конвенції про захист прав людини і основоположних свобод, за умови дотримання принципу справедливого суду. Цей підхід підтверджує допустимість дистанційної участі у процесі, якщо вона не порушує процесуальних прав і гарантій сторін.

У зв'язку з військовою агресією РФ та введенням воєнного стану, з'явилась додаткова потреба у використанні онлайн-зв'язку для участі осіб, які перебувають на тимчасово окупованих територіях, в умовах бойових дій або евакуації. Це також стосується свідків, експертів, перекладачів та інших учасників провадження, які не можуть фізично бути присутніми у суді.

У нормативному полі питання цифровізації кримінального процесу регулюється не лише положеннями Кримінального процесуального кодексу України, а й значною кількістю підзаконних нормативно-правових актів. Вони деталізують технічні аспекти проведення процесуальних дій у цифровому форматі, а також визначають порядок взаємодії між учасниками судового провадження за допомогою інформаційно-комунікаційних технологій. Особливе місце серед цих інструментів займає проведення судових засідань у форматі відеоконференцій, що хоч і не повністю замінює традиційну форму судового розгляду із фізичною присутністю сторін, однак стало невід'ємним елементом гнучкого процесуального механізму. Такий

формат особливо актуалізувався в екстремальних умовах - під час пандемії COVID-19 та в умовах повномасштабного збройного конфлікту, коли фізична присутність учасників у залі суду стала або неможливою, або небезпечною.

Сучасне правосуддя вимагає ефективного адаптування до обставин, зберігаючи при цьому основи - законність, об'єктивність, процесуальну рівність та справедливість. Це означає, що навіть у надзвичайних умовах правосуддя має залишатися ефективним і неформальним, а використання нових технологій повинно підпорядковуватись цим основоположним засадам. Тому дистанційні судові засідання, хоч і сприймалися спочатку як виняткова тимчасова міра, поступово стали інструментом сталого розвитку судової системи, сприяючи її стійкості та безперервності.

Разом з тим, активне використання онлайн-технологій у судовому процесі супроводжується серйозними викликами у сфері кібербезпеки. Проведення судових засідань у дистанційному режимі передбачає обробку значної кількості конфіденційної інформації, включно з персональними даними учасників процесу, матеріалами досудового розслідування, свідченнями сторін, експертними висновками та іншими чутливими даними. Відповідно, виникає об'єктивна потреба в розробці й впровадженні комплексних механізмів захисту таких даних. Це включає системи шифрування переданої інформації, багаторівневу аутентифікацію користувачів, контроль за наданням доступу до матеріалів справи, а також створення резервних копій і засобів захисту від несанкціонованого втручання. На державному рівні в Україні вже запроваджуються відповідні рішення в рамках національної стратегії кіберзахисту судових інформаційних систем. Цим процесом опікуються такі інституції, як Державна судова адміністрація України та Державний центр судових комунікацій. Зокрема, одним із превентивних заходів стало обмеження

доступу до Єдиного державного реєстру судових рішень у разі загрози зламу або витоку інформації (див. Додаток 1 та 2).

Серед переваг запровадження відеоконференцій варто також виокремити суттєве зменшення навантаження на логістичні й фінансові ресурси держави. Зокрема, відпадає необхідність у транспортуванні осіб, які утримуються під вартою, до судів, особливо якщо ці особи перебувають у СІЗО або установах виконання покарань, розташованих у віддалених регіонах. Це стосується також доставки свідків, перекладачів, судових експертів, які можуть долучатися до судового процесу дистанційно, не порушуючи при цьому вимог процесуального законодавства. Такий підхід дозволяє не лише економити державні кошти, а й підвищує оперативність судового розгляду. Згідно з аналітичними даними, у місті Києві щороку проводиться понад 30 тисяч судових засідань. Значна частина з них, з огляду на їхню процесуальну природу, може бути ефективно реалізована в онлайн-форматі без зниження рівня правової захищеності сторін чи якості винесених рішень. (за даними веб-порталу Список судових справ, призначених до розгляду <https://court.gov.ua/assignments/>).

Отже, у сучасних умовах відеоконференції та онлайн-слухання стають невід'ємною частиною кримінального процесуального ландшафту України. Їхнє впровадження ґрунтується як на правових нормах, так і на технологічному прогресі. Головне завдання – забезпечити баланс між ефективністю судового процесу та дотриманням прав людини. У майбутньому слід очікувати подальшого вдосконалення нормативного регулювання, підвищення технічної спроможності судової системи, а також розширення сфери застосування дистанційного правосуддя. Водночас необхідним залишається контроль за дотриманням процесуальних гарантій, а також формування єдиної судової практики щодо використання відеозв'язку, що дозволить уникнути правової невизначеності та посилити довіру громадян до судової системи (Додаток – 3).

У контексті сучасних технологічних трансформацій та викликів, пов'язаних із воєнним станом, використання відеоконференцзв'язку та онлайн-слухань у кримінальному судочинстві України набуває особливого значення. Ці інструменти, інтегровані у національне законодавство, спрямовані на забезпечення безперервності правосуддя, підвищення ефективності судових процесів та дотримання прав учасників кримінального провадження. Аналізуючи положення КПК України, а також наукові праці українських дослідників, можна виокремити ключові аспекти впровадження цифрових технологій у судову практику, їхні переваги, обмеження та перспективи розвитку.

Правову основу використання відео-конференц зв'язку та онлайн-слухань у кримінальному процесі України вперше було систематизовано в КПК України 2012 року, який закріпив можливість проведення судових засідань у режимі відеоконференції з метою забезпечення участі свідків, експертів, підозрюваних чи інших осіб, які не можуть фізично присутні у залі суду. Згодом, під впливом європейських стандартів (зокрема, Так, стаття 125-1 КПК України, введена у 2021 році, легалізувала поняття «дистанційного судового засідання», що передбачає участь сторін через засоби зв'язку. Науковці, зокрема О.Петришин та І.Ковальов підкреслюють, що такі новели стали відповіддю на потреби часу, забезпечивши функціонування судової системи в умовах масованих обстрілів та міграційних потоків [65].

Зміни сприяли подоланню правових колізій, пов'язаних із підтвердженням достовірності показань, наданих дистанційно, а також із гарантіями конфронтації сторін. Однак, як зазначає колектив науковців, залишаються невирішеними питання щодо забезпечення конфіденційності передачі даних, особливо у випадках, пов'язаних із державною таємницею [65].

Переваги використання ВКЗ у кримінальному судочинстві об'єктивно пов'язані із підвищенням доступності правосуддя. Наприклад, участь потерпілих або свідків, які перебувають у зоні бойових дій або на тимчасово окупованих територіях, часто неможлива без застосування дистанційних технологій. Як зазначає Т. Мельник, онлайн-слухання дозволяють уникнути затримок у розгляді справ, пов'язаних із небезпекою для життя учасників процесу. Крім того, економія часу та ресурсів (наприклад, усунення необхідності конвоювання підсудних) є суттєвим аргументом на користь ВКЗ, особливо в умовах перевантаженості судів [66].

Окрім ефективності, важливим аспектом є дотримання принципів справедливого суду. Зокрема, КПК України гарантує право на захист, яке, на думку В.Грищенка, може бути реалізоване через ВКЗ шляхом забезпечення комунікації адвоката з клієнтом навіть у випадках його тримання під вартою. Проте науковець попереджає про ризик обмеження права на безпосередній огляд доказів, оскільки технічні збої або низька якість передачі зображення можуть вплинути на об'єктивність оцінки доказав. Ця проблема актуалізується у контексті КПК України, який вимагає, щоб докази досліджувалися безпосередньо судом [67].

Важливим етичним та правовим викликом залишається забезпечення конфіденційності. Судові засідання можуть бути закритими для захисту інтересів учасників процесу, але використання зовнішніх платформ для ВКЗ (наприклад, Zoom чи Microsoft Teams) створює ризики витоку інформації. На думку К. Біланюка, автора статті «Кібербезпека в е-правосудді», держава має розробити власні захищені канали зв'язку, що відповідають стандартам НБУ та СБУ. Досвід Вищого антикорупційного суду, який використовує спеціалізоване програмне забезпечення з двофакторною аутентифікацією, свідчить про можливість мінімізації таких ризиків [41].

Не менш суттєвим є питання цифрової нерівності. У 2023 році лише 60% судів України були оснащені необхідною технікою для проведення

онлайн-слухань, а доступ до стабільного інтернету в сільських районах залишається обмеженим. Це порушує принцип рівності сторін, оскільки учасники процесу з віддалених регіонів можуть бути позбавлені можливості ефективно захищати свої інтереси. Вирішення цієї проблеми, на думку експертів, вимагає державних інвестицій у інфраструктуру та навчання суддівського корпусу [43].

Окремо варто зупинитися на досвіді використання ВКЗ під час допиту свідків, які перебувають за кордоном. Такі свідчення можуть бути отримані за міжнародною правовою допомогою, але процедура часто затягується через бюрократію. ВКЗ дозволяє провести допит у режимі реального часу, що особливо актуально у справах, пов'язаних із воєнними злочинами, де свідки можуть перебувати у різних країнах.

Перспективи розвитку дистанційного правосуддя в Україні пов'язані з подальшою гармонізацією законодавства з європейськими стандартами. Наприклад, Директива ЄС 2016/343 (<https://eur-lex.europa.eu/eli/dir/2016/343/oj/eng>) передбачає право обвинуваченого на участь у судовому засіданні, що може включати ВКЗ за наявності об'єктивних перешкод. Впровадження електронного судочинства, зокрема через систему «Е-суд», має стати основою для автоматизації процесуальних дій, від подачі клопотання до оголошення вироку. Однак, як зазначає О.Петров, ключовим залишається забезпечення балансу між технологічними інноваціями та гарантіями прав людини, зокрема права на особистий контакт із захисником [45].

Підсумовуючи, інтеграція відеоконференцзв'язку та онлайн-слухань у кримінальне судочинство України є об'єктивним кроком у відповідь на сучасні виклики. Проте для повноцінного функціонування цих механізмів необхідне подальше вдосконалення технічної інфраструктури, підвищення кібербезпеки, навчання учасників процесу та адаптація законодавства до динаміки технологічного прогресу. Як зазначає академік В. Філіпчук,

«цифровізація правосуддя – це не мета, а інструмент, який має працювати на захист прав людини, а не проти них». Тому кожен крок у цьому напрямку потребує ретельного аналізу та врахування уроків вже наявного досвіду [46].

3.3. Переваги та виклики цифровізації судового розгляду

Цифровізація судового розгляду стала однією з ключових тенденцій розвитку сучасної правової системи, що пов'язана із загальною цифровою трансформацією суспільства. У сучасному світі цифрові технології охоплюють усі сфери життя, включаючи правосуддя. Впровадження інноваційних технологічних рішень у судову систему є відповіддю на виклики сучасності, які вимагають забезпечення доступності, прозорості, оперативності та ефективності судового процесу. Однак, як і будь-яка трансформація, цифровізація має не лише переваги, а й численні виклики, що потребують детального аналізу та зваженого підходу. Однією з найважливіших переваг цифровізації судового розгляду є підвищення доступності правосуддя для громадян. Завдяки впровадженню електронних сервісів, учасники судового процесу отримують можливість подавати документи в електронному вигляді, здійснювати моніторинг руху справ, брати участь у засіданнях через відеозв'язок, не залишаючи власного місця перебування. Це особливо актуально для осіб, які проживають у віддалених населених пунктах або мають обмежені фізичні можливості. Таким чином, цифровізація сприяє дотриманню принципу рівного доступу до правосуддя, що є основоположним у демократичному суспільстві.

Іншою важливою перевагою є підвищення ефективності та оперативності судового процесу. Завдяки електронному документообігу, процес розгляду справ пришвидшується, оскільки зникає необхідність у фізичному переміщенні документів, їх копіюванні та зберіганні в паперовій формі. Судді, адвокати, прокурори та інші учасники процесу можуть

оперативно обмінюватися інформацією, що дозволяє економити час та ресурси. Крім того, цифрові платформи дозволяють автоматизувати низку процедур, зменшуючи ризики людської помилки, втрати документів або їх спотворення. Це підвищує точність ведення справ і сприяє прозорості процесуального провадження.

Одним із ключових напрямів цифровізації є впровадження систем відеоконференцзв'язку, які дають змогу проводити судові засідання в онлайн-форматі. Це стало особливо важливим в умовах пандемії COVID-19, коли фізична присутність у судових залах була обмежена. Відеозасідання дозволяють забезпечити безперервність правосуддя навіть за надзвичайних обставин, а також знижують витрати на транспортування підсудних, свідків та інших учасників процесу. Зниження витрат є ще одним суттєвим плюсом цифровізації. Відмова від паперового документообігу, зменшення потреби у фізичній присутності сторін, автоматизація частини процесів – усе це дозволяє суттєво скоротити витрати як з боку держави, так і з боку громадян. Електронні сервіси також зменшують навантаження на апарат судів, що дає можливість сконцентруватися на більш важливих завданнях, ніж копіювання та розсилання паперових документів.

Яскравим прикладом того, як цифровізація змінює ландшафт кримінального процесу, є так звана "справа адвокатів-хакерів", розслідувана НАБУ [104].

У ній ключову роль відіграли саме цифрові докази: електронні листування, повідомлення в месенджерах, метадані файлів. Встановлення злочинної діяльності стало можливим завдяки технічним засобам спостереження та аналізу цифрових слідів. З одного боку, це демонструє переваги - оперативність, точність, об'єктивність фіксації подій. З іншого - порушує низку питань щодо автентичності цифрових доказів, захисту інформації та меж правомірного втручання в особистий простір учасників процесу. Таким чином, справа не лише ілюструє ефективність цифрових

інструментів, але й нагадує про необхідність юридичних гарантій при їх використанні.

Прозорість та підзвітність судового процесу значно зростають з переходом на цифрові технології. Завдяки записам відеозасідань, електронним протоколам та відкритому доступу до інформації про хід судових справ зменшується можливість для корупційних зловживань, маніпуляцій та фальсифікацій. Участь громадськості та ЗМІ в судових засіданнях через онлайн-доступ забезпечує публічність процесу, що є важливою гарантією справедливості.

Проте, разом із перевагами цифровізація судочинства приносить і численні виклики, які потребують вирішення. Однією з головних проблем є питання кібербезпеки та захисту персональних даних. Судові процеси передбачають обробку великої кількості конфіденційної інформації, і витік таких даних може мати серйозні наслідки для учасників процесу та довіри до судової системи загалом. Забезпечення належного рівня захисту даних вимагає значних інвестицій у IT-інфраструктуру, кваліфікований персонал та постійне оновлення систем безпеки.

Іншою проблемою є цифрова нерівність, яка проявляється в нерівному доступі до цифрових технологій серед різних категорій громадян. Не всі мають необхідні технічні засоби, навички або стабільне інтернет-з'єднання для повноцінної участі в електронному судочинстві. Це особливо стосується людей похилого віку, малозабезпечених верств населення та жителів сільської місцевості. Таким чином, є ризик, що цифровізація замість забезпечення рівного доступу навпаки поглибить соціальні диспропорції. Також важливо враховувати проблему адаптації кадрів до нових умов. Судді, секретарі, адвокати та інші працівники судової системи мають володіти цифровою грамотністю, вміти користуватися відповідними платформами та сервісами. Для цього потрібне якісне навчання, перенавчання та постійна підтримка. Недостатній рівень підготовки

персоналу може призвести до технічних збоїв, затримок та порушення процесуальних прав учасників справ. Технологічні збої – ще один виклик цифровізації. Залежність від техніки означає, що в разі несправностей або хакерських атак уся система може зазнати значних збоїв. Випадки перебоїв в інтернет-з'єднанні, збоїв у роботі серверів або програмного забезпечення можуть паралізувати діяльність суду, що є особливо небезпечним у кримінальних справах, де строки мають критичне значення.

Юридичні аспекти цифровізації також потребують ретельного врегулювання. Зміна формату судового процесу вимагає змін у законодавстві, зокрема щодо допустимості електронних доказів, правил ідентифікації учасників онлайн-засідань, механізмів фіксації та зберігання електронних протоколів. Недосконалість нормативної бази може стати перешкодою для повноцінного функціонування цифрового судочинства. Важливо також зберігати баланс між ефективністю та дотриманням процесуальних гарантій. Наприклад, участь у судовому засіданні через відеозв'язок може ускладнити процес захисту прав обвинуваченого, унеможливити конфіденційне спілкування з адвокатом або призвести до порушення права на безпосередній розгляд справи суддею. Тому важливо розробити чіткі механізми, які б забезпечували реалізацію всіх прав учасників процесу незалежно від формату його проведення.

В Україні процес цифровізації судочинства розпочався ще на початку 2010-х років, однак значного поштовху він набув після початку пандемії COVID-19. В умовах карантину судова система була змушена адаптуватися до нових реалій, і саме тоді активізувалося впровадження електронного суду, онлайн-засідань та інших цифрових рішень. Одним із ключових інструментів стала підсистема «Електронний суд» (<https://cabinet.court.gov.ua/notifications>), яка дозволяє подавати позови, заяви, клопотання та інші документи в електронному вигляді, отримувати судові рішення, стежити за перебігом справ та здійснювати інші

процесуальні дії дистанційно. Поступово відбувається інтеграція електронного судочинства з іншими державними реєстрами та платформами, що сприяє уніфікації даних та спрощує процес перевірки інформації.

У той же час, на думку комітету Верховної Ради з питань правової політики, судова система стикається з низкою викликів, що гальмують цифрову трансформацію. Ключовими є нестача фінансування, і недостатній рівень цифрової грамотності суддів та персоналу для чіткого виокремлення, які частини судового процесу потребують змін [102]. Проблеми також виникають із забезпеченням кібербезпеки та захистом персональних даних, особливо з огляду на воєнний стан та постійні кібератаки з боку ворога. У цьому контексті важливо не лише впроваджувати цифрові рішення, але й створювати умови для їх стабільного та безпечного функціонування. Еспішна цифровізація судочинства можлива лише за умов комплексного підходу, який охоплює технологічну модернізацію, навчання кадрів, оновлення законодавства, забезпечення кібербезпеки та постійний діалог між державою, юридичною спільнотою та громадськістю. Естонія є одним із прикладів країни, яка змогла побудувати ефективну цифрову судову систему завдяки поєднанню сучасних технологій, політичної волі та активної участі громадянського суспільства [103, с. 21-28].

Цифровізація також відкриває нові можливості для аналітики та прогнозування. Завдяки збору великих масивів даних про судову практику можливо застосовувати елементи штучного інтелекту для аналізу типових рішень, виявлення системних проблем та підвищення якості правосуддя. Проте, важливо уникнути надмірної автоматизації рішень, яка може поставити під сумнів принцип індивідуального підходу до кожної справи. Судочинство повинно залишатися гуманним і зосередженим на справедливості, а не лише на ефективності. Цифровізація судового процесу є невідворотною і необхідною умовою модернізації правосуддя. Її переваги

очевидні – це зручність, швидкість, економія ресурсів, прозорість та доступність. Однак не менш важливо враховувати виклики, які виникають у процесі цифрової трансформації. Для того, щоб цифровізація не стала джерелом нових проблем, а навпаки – сприяла підвищенню довіри до судової системи, необхідно діяти зважено, поетапно та системно. Важливо забезпечити рівний доступ до цифрових послуг, навчати кадри, гарантувати захист даних та оновлювати законодавство відповідно до нових реалій.

Зрештою, успіх цифровізації судочинства залежить від здатності суспільства адаптуватися до змін, від відкритості до інновацій та від бажання побудувати справедливую й ефективну правову систему, яка відповідатиме викликам ХХІ століття. Лише поєднання технологій із дотриманням основоположних прав і свобод людини дозволить досягти справжнього прогресу у сфері правосуддя. У перспективі цифрове судочинство може стати не лише інструментом для підвищення ефективності, а й основою для створення нової культури правосуддя – відкритої, доступної, сучасної та орієнтованої на потреби громадян. І хоча шлях до повноцінної цифровізації є складним та неоднозначним, він є необхідним кроком уперед, який дозволить побудувати більш справедливую та ефективну систему правосуддя в інтересах суспільства загалом.

Висновки до Розділу 3

У третьому розділі роботи досліджено процес цифровізації судового розгляду, зокрема перехід до електронного судочинства, застосування відеоконференцій та онлайн-слухань, а також проаналізовано переваги та виклики цієї трансформації.

У підрозділі 3.1 розглянуто процес переходу до електронного судочинства, що демонструє можливості використання сучасних інформаційних технологій для оптимізації судових процедур. Цей перехід сприяє підвищенню оперативності розгляду справ, зменшенню паперової

бюрократії та покращенню доступу до інформації для учасників судочинства.

Підрозділ 3.2 присвячено використанню відеоконференцій та онлайн-слухань, що дозволяє забезпечити дистанційну участь сторін у судових процесах. Такий формат проводить реформи у напрямку забезпечення безпеки, ефективного управління часом та ресурсами судових органів, а також сприяє зниженню логістичних витрат. Проте, важливою залишається потреба у високоякісному технічному забезпеченні та дотриманні принципів доступності та справедливості.

У підрозділі 3.3 проаналізовано переваги та виклики цифровізації судового розгляду. Серед основних переваг виділено підвищення прозорості процесу, можливість архівного зберігання матеріалів справ, а також спрощення адміністрування судочинства. Водночас, цифрова трансформація пов'язана з низкою викликів: необхідністю адаптації правових норм до нових технологічних умов, вирішенням проблем кібербезпеки та захисту персональних даних, а також потребою в підвищенні кваліфікації суддів і судового персоналу.

Таким чином, проведений аналіз засвідчує, що цифровізація судового розгляду є важливим кроком до модернізації правової системи, спрямованим на підвищення ефективності та доступності правосуддя. Ефективне впровадження електронного судочинства потребує комплексного підходу, що включає модернізацію технічної інфраструктури, оновлення нормативної бази та навчання кадрів, що у майбутньому сприятиме зміцненню довіри до судової системи та забезпеченню справедливості в правозастосуванні.

ВИСНОВКИ

Під час дослідження проаналізовано сутність, правові засади, інституційне забезпечення та практичні аспекти цифровізації кримінального провадження в Україні. На основі теоретичного осмислення, аналізу законодавства, практики правоохоронних органів і судів, а також з урахуванням міжнародного досвіду можна сформулювати такі основні висновки:

1. Цифровізація кримінального провадження є складовою глобальної трансформації системи правосуддя, що передбачає використання сучасних цифрових технологій на всіх етапах – від досудового розслідування до виконання судових рішень. Її мета полягає у підвищенні ефективності, прозорості, доступності та справедливості кримінального процесу.

2. Україна, попри складну внутрішню ситуацію, активно впроваджує цифрові інструменти у сферу кримінального правосуддя. До ключових досягнень можна віднести функціонування **Єдиного реєстру досудових розслідувань (ЄРДР)**, розвиток **Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС)**, запровадження **електронного документообігу, відеоконференцій** та інших елементів електронного судочинства.

3. Одним із найважливіших наслідків цифровізації є **зміна парадигми доказової діяльності**. Відкриваються можливості для використання **електронних доказів**, але водночас виникають ризики щодо їх допустимості, достовірності, захищеності від фальсифікацій. Це потребує вдосконалення КПК України з урахуванням міжнародних стандартів, зокрема рекомендацій Ради Європи та практики ЄСПЛ.

4. Значний потенціал має впровадження **штучного інтелекту** в аналіз кримінальних справ, прогнозування рецидивів, оцінку ризиків тощо.

Однак його використання має бути суворо регламентованим, аби уникнути алгоритмічної упередженості, порушення права на захист чи презумпції невинуватості.

5. Проблеми цифровізації включають **правову невизначеність, недостатнє технічне забезпечення, низький рівень цифрової грамотності** окремих учасників процесу, а також **ризики порушення конфіденційності та кібербезпеки**. Це потребує не лише законодавчих змін, а й реалізації державних програм цифрової освіти та інфраструктурного розвитку.

6. У період воєнного стану цифровізація набула додаткового значення: саме завдяки дистанційним інструментам стало можливим здійснення окремих процесуальних дій та забезпечення безперервності правосуддя в умовах бойових дій або загроз безпеці.

7. У міжнародній практиці (особливо в країнах ЄС) активно впроваджуються комплексні системи е-судочинства, аналітики великих даних, електронного управління справами, блокчейн-технології. Україна має можливість перейняти ці інновації, адаптуючи їх до своїх правових та соціальних реалій.

8. Перспективи цифровізації кримінального процесу в Україні пов'язані з формуванням **єдиного міжвідомчого інформаційного простору, законодавчим закріпленням статусу електронних доказів, вдосконаленням процедур відеофіксації, розвитком аналітичних інструментів** для боротьби зі злочинністю та **гарантій прав учасників процесу в цифровому середовищі**.

Цифровізація кримінального провадження - це процес інтеграції цифрових технологій у всі стадії кримінального процесу, зокрема у досудове розслідування, судовий розгляд, апеляційне та касаційне провадження. Основною метою цифровізації є підвищення ефективності, оперативності, прозорості та доступності правосуддя шляхом використання

електронного документообігу, відеоконференцій, електронних баз даних, цифрових засобів фіксації процесуальних дій тощо. У рамках цифровізації також передбачається створення єдиної інформаційної системи досудового розслідування, яка дає можливість автоматизованого обміну інформацією між правоохоронними органами, прокурорами, адвокатами та судами.

Правові основи цифрового кримінального провадження (ЦКП) в Україні на сьогодні є лише частково сформованими. У законодавстві України передбачено окремі елементи електронного провадження, такі як відеоконференції під час судових засідань, електронний облік матеріалів, зберігання інформації у цифровому вигляді тощо. Разом із тим, відсутня єдина комплексна система правового регулювання, яка б охоплювала всі аспекти цифровізації кримінального провадження. Не всі процесуальні дії детально регламентовані в умовах цифрового середовища, а практика впровадження окремих елементів (зокрема електронного обміну між органами досудового розслідування та судами) часто стикається з технічними, організаційними й правовими труднощами. Отже, правові основи є недостатніми й потребують подальшого вдосконалення шляхом прийняття окремих законодавчих актів, а також гармонізації з міжнародними стандартами.

Міжнародний досвід свідчить про активне впровадження цифрових рішень у кримінальне провадження в країнах Європейського Союзу, США, Естонії.

Висновок щодо впровадження цифрових технологій у досудове розслідування полягає в тому, що Україна перебуває на початковому етапі цифрової трансформації у сфері кримінального провадження. Впровадження цифрових інструментів у досудове розслідування дозволяє зменшити навантаження на слідчих, пришвидшити обмін інформацією, підвищити прозорість розслідувань та забезпечити якісніший захист прав учасників процесу. Однак для ефективного функціонування цифрових

механізмів необхідно вирішити низку питань: удосконалити законодавство, створити технічну інфраструктуру, забезпечити кібербезпеку та навчання персоналу. Важливо також запозичити найкращі міжнародні практики та адаптувати їх до українських реалій, аби забезпечити баланс між інноваційністю та дотриманням процесуальних гарантій.

Цифровізація кримінального провадження має низку специфічних рис, які відрізняють її від цифровізації у цивільному, господарському чи адміністративному провадженні. Ці особливості зумовлені природою кримінального процесу, його завданнями, суб'єктним складом та підвищеними гарантіями прав людини, особливо щодо права на захист, презумпції невинуватості та недоторканності приватного життя.

По-перше, у кримінальному провадженні ключову роль відіграє сторона державного обвинувачення, яка здійснює процесуальне керівництво досудовим розслідуванням і представляє інтереси держави в суді. У зв'язку з цим цифрові рішення мають бути спрямовані не лише на оптимізацію процедур, але й на забезпечення реального балансу між інтересами обвинувачення та захисту, відповідно до принципу змагальності. Зокрема, електронні бази доказів, цифрові носії інформації, електронні матеріали кримінального провадження повинні бути однаково доступними для обох сторін процесу, включно з адвокатами. Це вимагає не лише правового врегулювання доступу, але й створення технічно надійних та прозорих механізмів, які б унеможливлювали маніпуляції або необґрунтоване обмеження прав сторони захисту.

По-друге, цифровізація досудового розслідування передбачає використання технічних засобів для фіксації практично всіх основних процесуальних дій. Зокрема, такі дії, як обшуки, допити свідків і підозрюваних, проведення експертиз, все частіше документуються за допомогою відео- та аудіозапису. Це створює додаткові гарантії процесуальної справедливості, адже зменшує ризики порушення прав

учасників провадження. Водночас таке фіксування потребує належного технічного забезпечення: від якісної апаратури до безпечного зберігання й обробки цифрових даних, які мають правове значення. Для порівняння, у цивільному чи господарському процесі аналогічні заходи здебільшого не використовуються або мають лише допоміжне процесуальне значення, без прямого впливу на доведення вини чи правомірності дій.

По-третє, цифрові інструменти, що застосовуються у кримінальному провадженні, безпосередньо пов'язані з втручанням у базові конституційні права громадян. Йдеться, зокрема, про право на свободу, приватність, таємницю листування та телефонних розмов, недоторканність житла тощо. Тому будь-яке використання технологічних засобів, таких як електронні засоби контролю (GPS-браслети, системи електронного спостереження, електронний арешт), має проходити не лише правову перевірку, а й оцінку відповідності стандартам прав людини. Особливо це важливо з огляду на те, що подібні заходи не мають аналогів у цивільному або господарському судочинстві, де обмеження прав особи мають значно м'якший характер і рідше застосовуються.

По-четверте, у кримінальних справах зазвичай обробляється великий обсяг інформації, яка має високий рівень конфіденційності та чутливості. Це можуть бути матеріали, що містять державну таємницю, персональні дані учасників процесу, деталі слідства, відео та фото з місця злочину, показання інсайдерів або таємних свідків. Такий обсяг і характер інформації зумовлює потребу у створенні спеціальних, підвищених стандартів захисту цифрових даних. На відміну від цивільного або господарського процесу, де більшість матеріалів є відкритими або мають обмежене коло осіб для ознайомлення, у кримінальному процесі кожен витік може становити загрозу як для справедливості судового розгляду, так і для життя або безпеки осіб, що беруть участь у справі.

Отже, цифровізація кримінального провадження в Україні є незворотним і водночас складним процесом, що потребує не лише технологічного вдосконалення, а й глибокого переосмислення правових підходів. У центрі цього процесу мають залишатися засади верховенства права, забезпечення рівності сторін, непорушність прав людини. Висновки та результати проведеного дослідження можуть слугувати важливою основою для формування сучасної концепції цифрової юстиції. Вони також можуть бути використані для оновлення та вдосконалення кримінального процесуального законодавства з урахуванням викликів цифрової трансформації державного управління та правосуддя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Діджиталізація» – слово 2019 року в Україні за версією онлайн-словника «Мислово». URL: <https://itc.ua/news/didzhitalizacziya-slovo2019-roku-vukrayini-za-versiyeyu-onlajn-slovnika-mislovo/> (дата звернення 05.04.2025)
2. Міхровська М. Цифрова трансформація сучасної держави. Міжнародний науковий журнал «Грааль науки». №6. 2021.-С.75–77.
3. Куйбіда, В. С., Карпенко, О. В., Наместнік В. В.. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. Вісник Національної академії державного управління при Президентові України. 2018. №1. С. 5–10 URL: http://nbuv.gov.ua/UJRN/vnaddy_2018_1_3. (дата звернення: 05.04.2025)
4. Encyclopedia of Information Science and Technology, Fourth Edition (10 Volumes). IGI Global, June, 2017. 8104 p
5. Про забезпечення реалізації деяких питань цифрового розвитку: наказ Державного агентства з питань електронного урядування України. №24. (2019). URL: <https://zakon.rada.gov.ua/rada/show/v0024883-19#Text> (дата звернення: 05.04.2025)
6. Цифрова трансформація. URL: https://uk.wikipedia.org/wiki/Цифрова_трансформація. (дата звернення: 05.04.2025)
7. What is Digital Transformation? Theagileelephant.com. website. URL: <http://www.theagileelephant.com/what-is-digital-transformation> (дата звернення: 05.04.2025)
8. Хлебінська О.І. Сутність цифрової трансформації з різних позицій підприємців та науковців. В: Економіка та держава, №9, 2021. с. 107-111.
9. Трансформація. Словник української мови. <http://sum.in.ua/s/transformacija> (дата звернення: 05.04.2025).

10. Глинська Н. В., Клепка Д. І. Понятійний контент цифровізації кримінального провадження URL: https://ivpz.kh.ua/wp-content/uploads/2023/10/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA-%D1%82%D0%B5%D0%B7_%D0%9F%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D1%96-%D0%BD%D0%B0%D0%BF%D1%80%D1%8F%D0%BC%D0%B8_2023.pdf#page=59 (дата звернення: 05.04.2025)
11. Довженко А.С. Цифровізація кримінального процесу як один із шляхів підвищення ефективності розслідування кримінальних правопорушень в умовах воєнного стану URL: <https://elar.navs.edu.ua/server/api/core/bitstreams/24881e7b-a87b-41fd-882c-223dee50ab4d/content> (дата звернення: 05.04.2025)
12. Петришин О. В. Права людини в цифрову епоху: виклики, загрози та перспективи / О. В. Петришин, О. С. Гиляка // Вісник Національної академії правових наук України. - 2021. - Т. 28, № 1. - С. 17-35. - Режим доступу: http://nbuv.gov.ua/UJRN/vapny_2021_28_1_3.
13. Цифрова трансформація кримінального провадження в умовах воєнного стану : матеріали круглого столу, присвяч. Всеукр. тижню права (м. Харків, 23 груд. 2022 р.) : електрон. наук. вид. / [редкол.: Н. В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Від. дослідж. проблем крим. проц. та судоустрою. – Харків : Право, 2022. – 148 с. – DOI: <https://doi.org/10.31359/9789669984395>.
14. Кримінальний процесуальний кодекс України: Закон від 13 квітня 2012 року № 4651-IV URL: <https://zakon.rada.gov.ua/laws/show/4651-17#n6974>
15. Закон України “Про електронні довірчі послуги” Закон України від 05.10.2017 № 2155-VIII) URL: <https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005#Text> (втратив чинність)

16. Савченко О.С. Систематизація наукових підходів до поняття «Цифровізація у публічному управлінні». Держава та регіони. Серія: Публічне управління і адміністрування, 2022 р., No 2 (76) URL: http://pa.stateandregions.zp.ua/archive/2_2022/12.pdf.
17. Офіційний веб-портал Судової влади України URL: <https://court.gov.ua/archive/1563352/>
18. Закон України «Про захист персональних даних» Закон України від 01.06.2010 № 2297-VI URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
19. Офіційний веб-портал Національної асоціації адвокатів України URL: <https://unba.org.ua/>
20. Концепція розвитку цифрової економіки та суспільства України на 2018– 2020 роки: розпорядження Кабінету Міністрів України 2018 №67-р URL: <https://zakon.rada.gov.ua/laws/show/67-2018-p#Text>. (дата звернення: 05.04.2025)
21. Стратегія розвитку прокуратури на 2021–2023 рр., затверджена наказом Генерального прокурора від 16 жовтня 2020 р. № 489. URL: https://www.gp.gov.ua/ua/iord?_m=publications&_t=rec&id=262782
22. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні : автореф. дис. ... докт. юрид. наук : 12.00.09. МВС України. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 40 с.
29. Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування : Закон України від 01 червня 2021 р. № 1498-IX. Відомості Верховної Ради України. 2021. № 31. Ст. 253. URL: <https://zakon.rada.gov.ua/laws/show/1498-20#Text>.

30. Закон України «Про правовий режим воєнного стану» Закон України від 12.05.2015 № 389-VIII URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text>
31. Оперативний моніторинг: правосуддя в умовах війни: моніторинговий звіт за 2022 р. / ред. к.ю.н. Олійник О.М. Київ: Міністерство юстиції України. Директорат правосуддя та кримінальної юстиції, 2022. 188 с. URL: <https://2022.uba.ua/wp-content/uploads/2022/07/om-pravosuddya-v-umovahvijny.pdf> (дата звернення 25.09.2022)
32. Глинська Н. В.,ЩОДО ОКРЕМИХ АКТУАЛЬНИХ ПИТАНЬ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ПІД ЧАС ВОЄННОГО СТАНУ <https://files.znu.edu.ua/files/Bibliobooks/Inshi69/0050385.pdf#page=131>
33. Висновок № 26 (2023) Консультативної ради європейських судів: Рухаючись вперед: використання асистивних технологій у судочинстві (Страсбург, 1 грудня 2023 року). URL: <https://hcj.gov.ua/page/vysnovky-kryes>
35. Штучний інтелект і технології можуть значно допомогти у роботі суддям, але не замінити їх, – Висновок КРЄС (28 грудня 2023 р.). URL: <https://ccu.gov.ua/novyna/syug-shtuchnyy-intelekt-i-tehnologiyi-mozhut-znachnodopomogty-u-roboti-suddyam-ale-ne>
36. Яновська О. Кримінальний процес під час воєнного стану: корективи, внесені війною в здійснення кримінальних проваджень. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1352467/>
37. Про електронні документи та електронний документообіг Закон України від 22.05.2003 № 851-IV <https://zakon.rada.gov.ua/laws/show/851-15#Text>
38. Hildebrandt, M. Law for Computer Scientists and Other Folk. Oxford University Press, 2020. global.oup.com
39. Institut Montaigne. "Artificial Intelligence and Security: Opportunities and Challenges for France." 2021.

40. European Commission. "Proposal for a Regulation on a European Approach for Artificial Intelligence." 2023.
[Shaping Europe's digital future](#)
41. Van Brakel, R. "Pre-emptive Big Data Surveillance and Its (Dis)Empowering Consequences: The Case of Predictive Policing." In: Exploring the Boundaries of Big Data. 2021.
42. Završnik, A. "Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings." European Journal of Criminology, 2022.
[ResearchGate](#)
43. Ferguson, A. "Policing Predictive Policing." Washington University Law Review, 2022.
[digitalcommons.wcl.american.edu](#)
44. Håkansson, A. "Proactive Prevention: Denmark's Domestic Practices of Human Rights Compliance." 2023.
[ResearchGate](#)
45. Bundeskriminalamt (BKA). "Autumn Conference 2024." 2023.
[bka.de](#)
46. Gómez-Carmona, C.D., et al. "Assessment of the Multi-Location External Workload Profile in the Workplace Using Wearable Technology." Sensors, 2021.
[mdpi.com+1mdpi.com+1](#)
47. Vogl, S. "Human-in-the-loop Machine Learning: Reconceptualizing the Role of Humans in AI Systems." Patterns, 2022.
48. Krimmer, T. "Criminal Procedure and Digital Evidence in Estonia." Digital Evidence and Electronic Signature Law Review, 2020.
49. National Audit Office (NAO). "Progress on the Courts and Tribunals Reform Programme." 2022.

50. Zöllner, F. "Artificial Intelligence in Criminal Justice: Strengthening or Challenging the Rule of Law?" Swedish Studies in European Law, 2023.

51. Kępiński, M. "Dolińska-Ficek and Ozimek v. Poland." European Court of Human Rights, 2021. hudoc.echr.coe.int

52. Mitsilegas, V. "The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law." Springer, 2022. link.springer.com

53. European Digital Rights (EDRi). "Tackling Cybercrime: Common Challenges and Legislative Solutions Identified by Europol and Eurojust." 2023.

54. European Court of Auditors. "Reducing the Backlog in the Crown Court." 2022.

[National](#) [Audit](#) [Office](#) [\(NAO\)](#)

55. Quattrocolo, S. "Criminal Justice, Artificial Intelligence Systems, and Human Rights." ERA Forum, 2021.

link.springer.com

56. Van der Hof, P. "The Use of Big Data and Algorithms by the Netherlands Police." Policing: A Journal of Policy and Practice, 2022.

[OUP](#) [Academic](#)

57. Leukfeldt, R. "The Use of Big Data and Algorithms by the Netherlands Police." Policing: A Journal of Policy and Practice, 2023.

[OUP](#) [Academic](#)

58. Georgieva, D. "Tackling Cybercrime: Common Challenges and Legislative Solutions Identified by Europol and Eurojust." 2022.

[Europol](#)

59. Duroyon, M. "A Legal Review of the AI Surveillance Software at the Paris 2024 Olympics." St. Andrews Law Review, 2023.

[StAndrews](#) [Law](#) [Review](#)

60. Taylor, L. "Criminal Justice, Artificial Intelligence Systems, and Human Rights." ERA Forum, 2022.

link.springer.com

61. Holm, S. "Predictive Policing and Algorithmic Fairness." Synthese, 2021.

62. Koulu, R. "Digital Futures ISPP Project Proposal." Senseable Stockholm Lab, 2022.

[KTH](#)

63. Barlou, G. "Digital Futures ISPP Project Proposal." Senseable Stockholm Lab, 2023.

63. Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерела доказів в кримінальному провадженні. Криміналістичний вісник. 2020. № 1(32). С. 37- 49.

64. Brindeau P. La dématérialisation des expertises civiles avec OPALEXE. Parole au juge, Experts. 2017. URL: https://www.martinique-expertsdejustice.com/wp-content/uploads/2018/03/article-RE_15_Brindeau_Aout2017.pdf

65. Orokos D., Hicks J., Lednev I., Stevens R., Strzalkowski T., Goel S. Development and Implementation of Forensic Science Research and Training Programs at the University at Albany's Northeast Regional Forensic Institute (NERFI). 2010. URL: <https://www.hsdl.org/?abstract&did=15680>

66. Радутний О. Е. Юридична освіта та сфера надання правових послуг в контексті штучного інтелекту. Інформація і право. 2019. № 2. С. 40-54. 67. Баранчук В. В. 3D сканування як спосіб фіксації на місці злочину: переваги й недоліки. Юридичний бюлетень. 2020. №16. С. 280-286.

68. Мурадов В. Електронні докази: криміналістичний аспект Порівняльне правознавство. 2013. № 3-2. С. 313-315. використання.

69. Цивільний процесуальний кодекс України: Закон від 18.03.2004 № 1618-IV. Дата оновлення: 08.02.2025. URL:

<https://zakon.rada.gov.ua/laws/show/1618-15#Text> (дата звернення: 01.03.2025).

70. Скрипник А. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні: дис. Ph.D. (доктор філософії) юрид. наук: 081 право. Харків, 2021. 204 С. 96. с. 369

71. Романюк В., Абламський С. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. Право і безпека. 2024. № 2 (93). С. 140-150.

72. Ангеленюк А.-М. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). Науковий вісник Ужгородського Національного Університету. Серія право. 2023. Випуск 79: частина 2. С. 214-218.

73. Гарасимів О., Марко С., Ряшко О. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. Науковий вісник Ужгородського Національного Університету. Серія право. 2023. Випуск 75: частина 2. С. 158-162.

74. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. Підприємництво, господарство і право. 2020. № 6. С. 243-247.

75. Кравчук В. М., Петренко І. О. Проблеми технологічного забезпечення досудового розслідування в Україні. Вісник кримінального судочинства. 2021. № 3. С. 45–52.

78. Лисенко О. С. Цифрова трансформація правоохоронних органів: виклики та перспективи. Юридична наука. 2022. Т. 29, № 4. С. 112–118.

79. Гончарук Ю. В. Кібербезпека в системі досудового розслідування: сучасний стан та напрями вдосконалення. Інформаційна безпека. 2020. Т. 26, № 2. С. 89–95.

80. Шевченко Т. П. Законодавче забезпечення кібербезпеки в правоохоронній діяльності України. *Право та суспільство*. 2021. № 5. С. 33–38.
81. Бойко М. І. Правовий статус цифрових доказів у кримінальному процесі України. *Вісник прокуратури*. 2022. № 12. С. 76–82.
82. Мельник О. В. Використання блокчейн-технологій у досудовому розслідуванні: правові аспекти. *Кібернетика і право*. 2023. Т. 11, № 1. С. 45–51.
83. Коваль П. І. Організаційні проблеми впровадження цифрових технологій у діяльність правоохоронних органів. *Адміністративне право і процес*. 2021. № 4. С. 98–104.
84. Національна академія внутрішніх справ. Звіт про результати опитування працівників правоохоронних органів щодо використання електронних систем у досудовому розслідуванні. Київ, 2023. 25 с.
85. Іваненко В. С. Довіра громадян до цифрових технологій у правоохоронній діяльності: соціологічний аналіз. *Соціологія: теорія, методи, маркетинг*. 2022. № 3. С. 132–139.
86. Київський міжнародний інститут соціології. Рівень довіри населення до електронних доказів у кримінальному процесі: результати всеукраїнського опитування. Київ, 2023. 30 с.
87. Міністерство внутрішніх справ України. Аналітичний звіт про ефективність функціонування Єдиного реєстру досудових розслідувань. Київ, 2023. 40 с.
88. Семенюк О. Л. Етичні аспекти використання штучного інтелекту в досудовому розслідуванні. *Етика і право*. 2023. Т. 15, № 2. С. 58–64.
89. Гриценко Т. В. Мобільні додатки для взаємодії громадян з поліцією: аналіз ефективності. *Інформаційне суспільство*. 2023. № 7. С. 77–83.

90. Зінченко О. М. Необхідність законодавчого врегулювання використання цифрових доказів у кримінальному процесі України. Юридичний вісник. 2023. № 6. С. 23–29.
91. Марченко І. С. Психологічні аспекти адаптації працівників правоохоронних органів до цифрових змін. Психологія і суспільство. 2023. Т. 20, № 3. С. 94–101.
92. Лист Верховного Суду від 03.03.2022 №1/0/2-22 “Щодо окремих питань здійснення кримінального провадження в умовах воєнного стану”. https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/war/Inform_yst_2022_03_03.pdf
93. Кравчук О. Кримінальне провадження в умовах воєнного стану: зміни до КПК. Судово-юридична газета, 9 березня 2022 р. <https://sud.ua/ru/news/blog/231730-kriminalne-provadzheniya-v-umovakhvoyennogo-stanu-zmini-do-kpk>
94. Кравчук О. О., Остащук І. Б. 2022. Судова символіка: монографія. Одеса: Видавничий дім «Гельветика», 528 с. URL: https://ela.kpi.ua/bitstream/123456789/46814/4/Kravchuk_Ostashchuk_Judicial_Symbolism.pdf
95. Сікора К. ВКЗ у кримінальному процесі і воєнний стан – як це працює, проблемні питання, чим корисна практика? Судово-юридична газета, 31 серпня 2022 р. <https://sud.ua/uk/news/blog/247392-vkz-u-kriminalnomu-protsesi-ivoyenniy-stan-yak-tse-pratsyuye-problemni-pitannya-chim-korisna-praktika>
96. ВРП підтримує законопроект щодо якнайшвидшого запровадження дистанційного судочинства в умовах воєнного стану. URL: <https://hcj.gov.ua/news/vrp-pidtrymuje-zakonoprojekt-shchodo-yaknayshvydshogozaprovadzheniya-dystanciynogo>
97. Капліна О. В., Туманянц А. Р., Шаренко С. Л. Судочинство у кримінальному провадженні під час пандемії covid-19: міжнародний досвід

та вітчизняна практика. Порівняльно-аналітичне право. № 3. 2020. С. 141-167.

98. Особливості функціонування судів в умовах пандемії COVID-19: жовтень 2020: Базовий посібник. Київ: Бюро демократичних інститутів і прав людини ОБСЄ, 2020. 58 с.

99. Судді ВС розповіли про необхідність внесення змін до законодавства у сфері кримінального та цивільного судочинства. URL: <https://sud.ua/uk/news/sudinfo/246618-suddi-vs-rozpovili-pro-neobkhdnist-vnese-nnya-zmin-dozakonodavstva-u-sferi-kriminalnogo-ta-tsivilnogo-sudochinstva>

100. ВКЗ у кримінальному процесі і воєнний стан – як це працює, проблемні питання, чим корисна практика? URL: <https://sud.ua/uk/news/blog/247392-vkz-ukriminalnomu-protsesi-i-voyenniy-stand-yak-tse-pratsyuye-problemni-pitannya-chimkorisna-praktika>

101. Запровадження онлайн-правосуддя в Україні потребує спрощення процесуальних правил. URL: <https://radako.com.ua/news/zaprovadzhennya-onlaynpravosuddya-v-ukrayini-potrebuie-sproshchennya-procesualnih-pravil>

102. Війна – це виклики, рішення і кроки, яких очікує суспільство URL: https://lb.ua/news/2022/12/28/540556_viyna-tse_vikliki_rishennya_i_kroki.html

103. Управління судовими інформаційними системами: міжнародний досвід. URL: <https://www.pravojustice.eu/storage/app/uploads/public/5fa/a5e/c73/5faa5ec73c202992255267.pdf>

104. Справа адвокатів-хакерів. Як НАБУ виявило паразитів. URL: <https://zn.ua/ukr/anticorruption/sprava-advokativ-khakeriv-jak-nabu-vijavilo-parazitiv.html>

105. Як працює система електронного кримінального провадження іКейс.

URL: https://ti-ukraine.org/research/yak-pratsyuye-systema-elektronnogo-kryminalnogo-provazhennya-ikejs/?utm_source=chatgpt.com

ДОДАТКИ

Додаток 1 – скріншот з реєстру

Єдиний державний реєстр судових рішень

Доступ до Реєстру здійснюється в тестовому (обмеженому) режимі. Для запобігання загрозам життю і здоров'ю суддів та учасників судового процесу, а також у разі виявлення ознак кіберзагроз, доступ до Реєстру або окремих рішень у ньому може бути обмежено.

Головна Законодавство Контакти Правила Допомога
Повний доступ

Пошук за контекстом
Введіть фрагмент тексту судового рішення

Суд та судді

Регіон суду: Оберіть

Найменування суду: _____

Інстанція: Оберіть

ПІБ судді: _____

Судова справа

Форма судочинства: Оберіть

Категорія справи: Оберіть

L _____

L _____

L _____

L _____

L _____

Справа №: _____

Статус сторін судового процесу: Оберіть

Судове рішення

Реєстраційний № рішення: _____

Період ухвалення (постановлення): з _____ по _____

Період надходження: з _____ по _____

Форма судового рішення: Оберіть

Пошук Очистити

Сортування: за релевантністю

[Використовувати інформаційно-правову електронну базу:](#) так

Постачальник посилань: Ліга Закон

Кількість записів на сторінці: 25

[Відгук про роботу сайту](#)

Документів у системі: 424564434

Додаток 2 – скріншот з Судової влади України

lenr.court.gov.ua/rud2024/pro_sud/kar/

Судова влада України | Суддівський районний суд м. Харкова | Про суд

Ленінський районний суд м. Харкова

Отримуйте інформацію лише з офіційних джерел

Єдиний Контакт-центр судової влади України 044 207-35-46

SA YNACT: Google

ПРО СУД

ПРЕС-ЦЕНТР

ГРОМАДЯНАМ

ПОКАЗНИКИ ДІЯЛЬНОСТІ

ІНШЕ

Для запобігання загрозам життю та здоров'ю суддів та учасників судового процесу у період воєнного стану, доступ тимчасово припинено. Судді здійснюють правосуддя в безперервному режимі в умовах відсутності загроз життю та здоров'ю учасників справи.

2025 © Всі права захищені

[Про суд](#)
[Прес-центр](#)
[Громадянам](#)
[Показники діяльності](#)
[Інше](#)

Додаток 3 - Сайт захищений відеоконференцзв'язок з судом -

vkz.court.gov.ua

ВКЗ

Технічна підтримка - | Інструкції | Перевірити налаштування обладнання | Українська - | Вхід

МЕНЮ

ЗАХИЩЕНИЙ ВІДЕОКОНФЕРЕНЦЗВ'ЯЗОК З СУДОМ

Участь у судовому засіданні чи відеоприйомі не потребує встановлення додаткових програм.
Для здійснення відеозв'язку необхідний браузер та інтернет.



Відеоприйом

Дозволяє проводити особисті прийоми громадян. Економить час та кошти, позбавляє від черг, задрок та нервового напруження біля кабінету. Дозволяє заздалегідь підготуватися до обговорення питань, тим самим підвищує ефективність особистого прийому. Під час відеоприйому існує можливість обговорювати файлами.

[ЗАЙТИ НА ВІДЕОПРИЙОМ](#)



Судові засідання (Відеоконференція)

Участь в судовому засіданні в адміністративному, цивільному та господарському процесах в режимі відеоконференції поза межами приміщення суду.

[ПЕРЕЙТИ ДО КОНФЕРЕНЦІЙ](#)