НДІ вивчення проблем злочинності імені академіка В. В. Сташиса

bona fides

Матеріали круглого столу

"Цифрова трансформація кримінального провадження в умовах воєнного стану"

м. Харків

23 грудня 2022 року

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ВИВЧЕННЯ ПРОБЛЕМ
ЗЛОЧИННОСТІ ІМЕНІ АКАДЕМІКА В. В. СТАШИСА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ
Відділ дослідження проблем кримінального процесу та судоустрою

ЦИФРОВА ТРАНСФОРМАЦІЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Матеріали круглого столу,
присвяченого Всеукраїнському тижню права
(м. Харків, 23 грудня 2022 року)

Електронне наукове видання

Харків
«Право»
2022

DOI: https://doi.org/10.31359/9789669984395
УДК [343.1:004](477)”364”(082)
Ц75

Рекомендовано до друку вченою радою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України (постанова № 12/4 від 28 грудня 2022 р.)

Ц75 **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.

ISBN 978-966-998-439-5

У збірнику висвітлено актуальні проблеми цифровізації кримінального провадження. Він містить результати дискусії за ключовими напрямами, що стосуються: 1) «цифрових» новацій кримінального процесуального законодавства під час воєнного стану; 2) цифрової трансформації досудового розслідування; 3) використання діджитал-технологій під час судового розгляду; 4) цифровізації кримінального провадження та захисту прав і законних інтересів людини; 5) використання штучного інтелекту в кримінальному провадженні; 6) цифрових інструментів боротьби зі злочинністю.

Збірку розраховано на широке коло читачів, зокрема на науковців, викладачів, аспірантів, студентів вищих юридичних навчальних закладів, фахівців у галузі права та всіх, хто цікавиться питаннями цифровізації кримінального провадження.

УДК [343.1:004](477)”364”(082)

ISBN 978-966-998-439-5

ЗМІСТ

Батиргареєва В. С.
Цифрова трансформація кримінальної процесуальної діяльності: щодо деяких викликів воєнного стану 6
Борисов В. І.
Концептуальні положення як інформаційне підґрунтя законопроєкту (на прикладі підготовки Кримінального кодексу України 2001 року) 11
Глинська Н. В.
Цифрова трансформація кримінального провадження під час воєнного стану 18
Дроздов О. М.
Дистанційне судове провадження: актуальні питання за практикою ЄСПЛ 23
Тетерятник Г. К., Стукаленко Г. В.
Цифрові аспекти відновлення втрачених матеріалів кримінального провадження 29
Шаренко С. Л.
Щодо актуальних питань діяльності суду під час воєнного стану 33
Авдєєва Г. К., Коновалова В. О.
Штучний інтелект у боротьбі зі злочинністю: напрями використання та проблеми законодавчого врегулювання 36
Ахтирська Н. М.
Використання штучного інтелекту в правосудді: виклики та стандарти Ради Європи 40
Барабаш А. А.
Впровадження цифрових технологій і забезпечення доступу до правосуддя в умовах воєнного стану 45
Булулуков О. Ю., Коновалова В. О.
Цифрова інформація у кримінальному провадженні в умовах воєнного стану 49
Гомоляко В. Є.
Особливості проведення обшуку в умовах воєнного стану 53
Данильченко Ю. Б.
Можливості використання цифрової інформації для запобігання та розкриття кримінально протиправних порушень Правил дорожнього руху 57

Демура М. І.
До питання про цифрову трансформацію кримінального провадження в умовах воєнного стану 61
Дунаєва Т. Є.
Щодо розслідування кіберзлочинів: досвід зарубіжних країн 66
Клепка Д. І.
Концепція «Paperless» vs кримінальне провадження 71
Коростельова Л. А.
Шукай AL: як штучний інтелект може допомогти у пошуку злочинців 75
Костюченко О. Ю.
Електронне подання до суду та цифровізація судового процесу як елементи впровадження ефективного судочинства та гарантія достовірності доказів 78
Котюк М. В.
Роль цифрових технологій при розслідуванні державної зради в умовах воєнного стану 82
Крицька І. О.
Європейські принципи та рекомендації щодо використання штучного інтелекту в кримінальному судочинстві 87
Марочкін О. І.
Актуальні питання цифровізації кримінальної процесуальної діяльності 92
Метелев О. П.
Деякі проблемні питання на шляху цифровізації кримінального процесу 96
Неділько Я. В.
Висновок спеціаліста у кримінальних провадженнях щодо кіберзлочинів: нормативна дуальність та практична доцільність 100
Нетеса Н. В.
Кібер-інформаційні посягання у сфері національної безпеки в умовах гібридної війни 103
Пашковський М. І.
Неоднорідність впливу цифрових технологій на кримінально-процесуальну форму 108

Погорецький М. М.
Забезпечення прав людини при проведенні негласних слідчих (розшукових) дій слідчими Служби безпеки України (проблемні питання) 112
Подкопаєв С. В.
Участь органів прокуратури в процесах цифрової трансформації кримінального провадження (організаційний аспект) 117
Рєпіна Ю. С.
Перспективи використання штучного інтелекту в кримінальному судочинстві України 122
Шевчук В. М.
Проблеми цифровізації криміналістики в умовах російсько-української війни 127
Яремчук В. О.
Цифрова трансформація використання криміналістичних знань у кримінальному провадженні під час воєнного стану 133
Baltrūnienė Ju., Shevchuk V.
Artificial intelligence technologies in law enforcement and justice: Ukrainian and European experience 135
Konovalova V. O., Shevchuk V. M.
Application of digital technologies in criminalistics in the conditions of war 141

ЦИФРОВА ТРАНСФОРМАЦІЯ КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ: ЩОДО ДЕЯКИХ ВИКЛИКІВ ВОЄННОГО СТАНУ

Батиргареєва Владислава Станіславівна,
доктор юридичних наук, професор, головний науковий співробітник ДНУ ІПБП НАПрН України,
директор НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України
ORCID: https://orcid.org/0000-0003-3879-2237

Тема війни і тема цифри сьогодні є визначальними темами нашого суспільства. Ще деякий час тому соціальними робінзонами нас хотів зробити COVID-19, ізолювавши людей в їх оселях. Сьогодні ж війна хоче зробити з нас вигнанців, примушуючи залишати власні домівки, власну країну. Російська агресія відкрила браму пекла, за якою чимало питань звичного соціального контексту, здавалося б, втрачають свій сенс. Однак українці – сильна і мужня нація. А тому в ситуації, що склалася, важливо зберегти соціальні зв'язки, перелаштувати всі сфери нашого життя у відповідності до викликів і небезпек, що нас оточують щодня. І так сталося, що цифровізація, котра розпочалася ще деякий час тому, якраз й допомагає нам зберегти основний контекст суспільних відносин та не випасти із фрейму соціалізації.

Фахівці Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України ще задовго до введення в Україні воєнного стану активно почали працювати над розробкою проблематики цифрової трансформації кримінально-процесуальної діяльності. Цьому принаймні є чимало причин.

По-перше, кілька років тому в НДІ розмірковували над майбутньою темою фундаментального дослідження. Словосполучення «цифровізація (або діджиталізація) кримінально-процесуальної діяльності» тільки-но почало посідати верхні чати актуальних проблематик, що визначатимуть майбутній образ кримінального провадження та правосуддя. Недаремно, одним із популярних у світі слів останніми роками є саме слово «діджиталізація». І наші фахівці своєчасно змогли відчути цей нерв і зробити цю проблематики мейнстримовою темою Інституту.

По-друге, станом на 14 грудня 2022 р. бомбардуваннями та розстрілами з артилерії й танків російські війська зруйнували 12 приміщень

судів (2 приміщення зруйновано частково) та 94 приміщення судових установ пошкоджено частково: вибиті вікна, в деяких відсутнє електропостачання, теплопостачання, водопостачання, пошкоджено стелю, внутрішні двері, зазнали руйнування внутрішні перегородки між кабінетами, пошкоджені зали судових засідань тощо [1]. Недивлячись на це, соціальна сфера відправлення правосуддя у широкому розумінні цього слова одна з перших в умовах воєнного стану змогла налагодити роботу, максимально використовуючи при цьому можливості, що дає цифра.

По-третє, на теперішній час Україна є передовою державою (у будь-якому разі в Європі) у плані запровадження цифрових застосунків і цифрових послуг як таких для населення України. Процесуальна сфера так само не є виключенням. Так, наприклад, сьогодні програмні засоби фіксування судових засідань дозволяють отримувати доступ до запису судового засідання через Електронний кабінет Електронного суду після сплати судового збору.

По-четверте, аналіз правозастосовної практики та великої кількості проєктів законів, спрямованих на регламентацію питань, що пов'язані з цифровою трансформацією, свідчить про неабияку актуальність зазначеної проблематики [2, с. 295]. Цього, зокрема, вимагає від нас й імплементація положень Конвенції Ради Європи про кіберзлочинність, ратифікованої Україною у 2005 р.

По-п'яте, ми остаточно і безповоротно входимо до нової парадигми життя людини у XXI ст., де буде панувати її велич цифра. Тому з *Homo sapiens* ми семимильними кроками перетворюємося на *Homo digitale* (людину цифрову).

На мій погляд, на проблематику цифрової трансформації кримінально-процесуальної діяльності цікаво подавитися не лише з ракурсу фахівців у відповідній сфері, а й під кутом зору пересічної людини, що живе в умовах воєнного стану. А це означає, що така людина буде шукати і намагатися роздивитися ті виклики і складнощі, що можуть стати на заваді прогресивного розвитку цифрової трансформації процесуальної діяльності, а так само буде замислюватися над тими завданнями, які потрібно вирішити якомога скоріше. Отже, про що йдеться?

Треба визначитися з тим, чи можлива сьогодні ініціація та реалізація кримінально-процесуальної діяльності, зокрема, відправлення правосуддя, за участю тих учасників кримінального процесу, що перебувають на тимчасово окупованих територіях? Чи можуть громадяни з окупованих

територій зафіксувати, наприклад, випадки правопорушень та повідомити про це українські органи, передавши, припустимо, докази за допомогою використання інформаційно-комунікаційних технологій? Якщо так, то в який спосіб? Тобто йдеться про доступ наших громадян з тимчасово окупованих територій до правосуддя у широкому смислі слова. Уявляється, що відповідь на таке запитання є важливим кроком у контексті реінтеграційного блоку і підтримки українців, які постраждали в результаті російської агресії на тимчасово окупованих територіях України.

Ще одна проблема, знання про яку слід донести до пересічної людини особливо в умовах воєнного стану. Мова йде про фактичне використання тих можливостей, що дає цифрова трансформація в аналізованій сфері. Так, важливо з'ясувати, наскільки сьогодні в цілому населення України є обізнаним про можливості та особливості цифрової процедури відправлення правосуддя та чи існує поняття цифрових прав учасників процесу? Нарешті, хто має опікуватися питаннями цифрового лікбезу стосовно кримінального процесу (знову ж таки в умовах воєнного стану)? Поряд із цими запитаннями виникає ще одне: наскільки швидко населення України «озброїться» гаджетами, придатними для реалізації своїх, скажімо так, цифрових прав? До того ж, як відомо, застосування цифрових застосунків платформи «Дія» зіштовхується з проблемою покриття території України якісним інтернет-зв'язком. Якщо не забезпечити ці «вихідні параметри» для успішної реалізації цифрових прав, то процеси відповідної трансформації будуть перманентно пробуксовувати.

Останніми роками фахівці в галузі боротьби зі злочинністю працюють над розв'язанням завдання щодо запровадження електронних доказів у кримінальному процесі як самостійного процесуального джерела. І є дуже непростою справою визнати за цифровою інформацією самостійне доказове значення. До того ж постійно точаться суперечки з приводу необхідності дотримання балансу між входженням до орбіти кримінального процесу цифрових об'єктів як процесуальних доказів та непорушністю права особи на privacy. У зв'язку з цим конче потрібною у кримінальному процесі є сувора регламентація процедури проведення, припустимо, обшуків, пов'язаних із доступом до інформації, котра міститься на електронних носіях, пристроях тощо. Напевно, вже настав час введення до контексту кримінального процесу поняття «обшук інформаційно-комунікаційного пристрою». Це питання є особливо важливим

з огляду на велику кількість зафіксованих злочинів проти основ національної безпеки, кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку тощо. Справа в тому, що від час їх вчинення винними особами активно використовуються цифрові пристрої, в яких залишається цифровий «слід» протиправних діянь. Так, наприклад, нещодавнє наше дослідження виявило, що найпоширенішим способом вчинення виправдовування, визнання правомірною або заперечення збройної агресії рф та глорифікації її учасників (ст. 436[2] КК України) є поширення відповідних матеріалів у соціальних групах за допомогою Інтернет-ресурсів [3, с. 42]. А це означає, що під час розслідування цього злочину контент, розміщений за допомогою електронних приладів у відповідних менеджерах, ставатиме предметом вивчення. У свою чергу, простежити процес генерування такої інформації стає можливим лише завдяки доступу до тих електронних приладів, якими принаймні користувалася винна особа.

Пересічну людину також може хвилювати процедура верифікації як самої цифрової інформації, що може мати будь-яке доказове значення, так і учасників кримінального процесу. Адже процедура ідентифікації учасника кримінального провадження за допомогою електронного підпису, що використовується зазвичай при підписанні будь-якого документа в електронній, на мій погляд, не дає гарантії, що такий прийом не можуть використовувати зловмисники. Тому паралельно тут виникає це одна проблема – як убезпечити інформаційні ресурси та саму людину від протиправного на неї впливу під час здійснення кроків щодо ідентифікації певних об'єктів та особи учасника кримінального процесу.

Ще одна проблема, яка межує з висловленою вище, полягає у запобіганні витоку, спотворенню або знищенню інформації, що циркулює мережами та знаходиться на цифрових платформах правоохоронних органів. Фактично йдеться про всілякі можливі правопорушення у цій сфері, починаючи від кібератак і закінчуючи банальними корупційними вчинками.

Говорячи про цифрову трансформацію кримінального процесу, слід звернути увагу і на адаптованість правової матерії до тих можливостей і потреб практики, а одночасно і до тих загроз, що супроводжують діджиталізацію даної соціальної сфери. Іншими словами, чи достатньо сьогодні наявної правової матерії, аби пришвидшити діджиталізацію у кримінально-процесуальній діяльності? Напевно, можливості цифри

та її поширення у кримінальному процесі на кілька кроків випереджають процес адаптації законодавства до властивостей і наслідків діджиталізації. Тому предстоїть багато роботи як у доктринальній сфері, так і в площині законодавства для того, щоб забезпечити кримінально-процесуальну діяльність новітнім сучасним інструментарієм для боротьби зі злочинністю.

Знову ж ще одна паралель… Запровадження цифрових процедур і важелів від фахівців у галузі кримінального процесу потребує знань відповідної спрямованості. У цьому плані, як здається, нам не обійтися без розв'язання питань щодо підготовки кадрів за спеціальною додатковою освітою або принаймні підвищення кваліфікації

І нарешті. Слід запитати: а чого боїться цифра? Відповім: цифра боїться темряви. Адже вона не живе без світла. Тому знищення агресором об'єктів української енергетики, що відбувається зараз, здатне вбити діджиталізацію, а значить, перетворити нас з *Homo digitale на Homo cave* (людину печерну). Отже, серйозним викликом для дистанційної роботи, збирання цифрових доказів тощо є блєкаут. Але ж маю надію, що і на цей виклик ми знайдемо симетричну відповідь.

Список використаної літератури:

1. ДСА України вживаються заходи щодо відновлення пошкоджених приміщень судів. URL: https://dsa.court.gov.ua/dsa/pres-centr/news/1358939/.
2. Демура М. І., Клепка Д. І., Крицька І. О. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження. *Часопис Київського університету права.* 2020/1. С. 295–300.
3. Батиргареєва В. С. До кримінологічного аналізу виправдовування, визнання правомірною або заперечення збройної агресії рф та глорифікації її учасників як нового виклику безпеці інформаційного простору України. *Інформація і право.* №4(43)/2022. С. 37–49.

КОНЦЕПТУАЛЬНІ ПОЛОЖЕННЯ ЯК ІНФОРМАЦІЙНЕ ПІДҐРУНТЯ ЗАКОНОПРОЄКТУ (НА ПРИКЛАДІ ПІДГОТОВКИ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ 2001 РОКУ)

Борисов Вячеслав Іванович,
доктор юридичних наук, професор, академік НАПрН України,
радник при дирекції НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Створення законопроєкту – це доволі складна, відповідальна та, як правило, тривала нормотворча діяльність, що пов'язана з регламентованим порядком його підготовки та прийняття. Насамперед це стосується підготовки кодексів, що охоплюють велику групу суспільних відносин зі специфічним предметом правового регулювання й мають значну кількість юридичних норм та інститутів. Серед *вихідних питань* майбутнього законопроєкту, що потребують поглибленого вирішення саме представниками наукової спільноти, провідне місце займають *концептуальні положення*, визначення яких на початковому етапі роботи над таким нормативно-правовим актом як кодекс, набувають значимості необхідного інформаційного підґрунтя для створення консолідованого, логічно узгодженого джерела права високого рівня.

Варто зазначити, що уявлення про концептуальні положення, пов'язані з потребою внесення значимих змін у чинне законодавство або необхідністю розробки принципового нового, такого як кодекс, формуються поступово, з розвитком наукових знань у сфері права. Однак, особливої актуальності потреба з визначення концептуальних положень набуває в період сутнісних соціальних трансформацій. Саме такі докорінні перетворення для українського суспільства відбулися 24 серпня 1991 року з проголошенням незалежності України. Почалися зміни, спрямовані на реформування суспільного життя, що охопили різноманітні напрями, в їх числі й процеси, пов'язані з кодифікацією законодавства. Вже 31 жовтня 1991 року Президія Верховної Ради України прийняла Постанову про підготовку проєктів законодавчих актів України, у тому числі Кримінального кодексу (далі – КК) України [9].

На виконання цієї Постанови Кабінетом Міністрів України розпорядженням №176-р від 24 березня 1002 р. були створені робочі групи

з підготовки законопроєктів, у їх числі й група з підготовки проєкту КК України. Керівниками останньої було призначено В. В. Дацюка (на той час Генерального прокурора України) та В. Я. Тація (ректора Національної юридичної академії України, тепер – Національний юридичний університет імені Ярослава Мудрого). 18 вересня 1992 р. зазначена група разом із Відділенням кримінально-правових наук Академії правових наук України (на той час – це громадське об'єднання науковців) та представниками практичних установ провели робочу нараду, на якій обговорили положення концепції проєкту КК [8, с. 127].

Ознайомлення з положеннями, які розглянули учасники наради, дозволяє виділити з них два основні напрями вирішення проблеми. Перший з них стосувався питань щодо закріплення в майбутньому нормативно-правовому акті суто юридичних вирішень, другий – віддзеркалював досягнення політичних цілей, пов'язаних з утвердженням у КК України нових цивілізаційних стандартів [10, с. 233] та положень, що в умовах соціальних змін набули для суспільства переважного значення.

Варто підкреслити, що найбільшого пріоритету на початку 90-х років XX століття набули ідеї, пов'язані з *утвердженням загальнолюдських цінностей*, головною з яких є людина, її природні права і свободи [2, с. 68–69]. Обґрунтування саме такого бачення, як домінуючого, випливало з міжнародно-правових документів. Це, зокрема, Загальна декларація прав людини від 10 грудня 1948 року, Підсумковий документ зустрічі представників держав-учасників Наради по безпеці та співробітництву в Європі, що відбулася у Відні 15 січня 1986 року, та інші не менш доленосні для людства міжнародно-правові акти. На фоні зростання гуманітарної складової авторитету міжнародних відносин, поруч з людиною та розумінням її найвищою соціальною цінністю, серед провідних концептуальних положень кримінального законодавства стали набувати значення й судження щодо *відповідності національних норм загальновизнаним принципам і нормам міжнародного права*.

Таким чином, робота над новим кримінальним законодавством України почалася з чіткого розуміння вихідних для часу перетворень політико-правових концептуальних положень, що надалі знайшли закріплення в нормах КК 2001 року. Так, серед завдань, визначених у ст. 1 цього нормативно-правового акта, на перше місце була поставлена охорона прав і свобод людини й громадянина. У ст. 3 зазначено, що КК України ґрунтується на Конституції України та загальновизнаних принципах

і нормах міжнародного права. Доречно звернути увагу, що в наведеному визначенні (ст. 3 КК) законодавцем вказано ще на одне концептуальне положення політико-правового характеру, яке на початку робот із реформування національного кримінального законодавства не набуло очевидності. Чинна на той час Конституція Української Радянської Соціалістичної Республіки 1978 року за своєю суттю втратила вплив на українське суспільство, а, отже, залишилася поза увагою розробників проєкту КК. Лише з *розгортанням роботи над проєктом нової Конституції України ідея врахування відповідності їй нового кримінального законодавства набула беззастережного загального визнання*, що й було вже в 1994 році зазначено в Основних концептуальних положеннях, що підлягали обговоренню під час підготовки проєкту КК України [6, с. 179–184].

Наведені положення: інтереси людини, її права і свободи; відповідність Конституції України; відповідність загальновизнаних принципам і нормам міжнародного права – є стратегічними, основоположними в системі концептуальних положень. Необхідність їх додержання закріплювало вирішення політичних завдань, пов'язаних із реформуванням кримінального законодавства. Однак, визначення концептуальних положень, на підставі яких формується нове законодавство, не обмежується лише стратегічними. Не менш важливе значення мають концептуальні положення тактико-правового рівня, які віддзеркалюють доктрину кримінального права, ті її положення, що набули на час роботи над проєктом КК загальновизнаного сприйняття.

Треба зазначити, що концептуальні положення тактико-правового рівня не були попередньо, тобто до початку роботи над КК, якимось чином оформлені в систематизований перелік із подальшим затвердженням на рівні наукового зібрання (наприклад, резолюції конференцій або урядового розпорядження). Вони викристалізовувалися у процесі роботи над проєктом КК України. Передусім розробниками була звернута увага на необхідності дотримання загальноприйнятих підходів до формування спеціалізованого нормативно-правового акта – Кримінального кодексу. Це *систематизація* норм – поділ їх на дві великі частини: Загальну та Особливу, далі – поділ на розділи залежно від предмета регулювання для Загальної частини та об'єкта охорони – для Особливої. Структура норм обрана традиційна, а саме: оформлення їх у статті з відповідними номерами та поділ останніх, за потреби, на частини. Текст норми повинен викладатися відповідно до вихідних вимог *зако-*

нодавчої техніки: це системність і чіткість формулювання правових приписів [1, с. 446]. Ці вимоги надають приписам кримінального законодавства якості *правової визначеності,* що дозволяє суб'єктам правопізнання, передусім будь-якому громадянину, однозначно сприймати їх зміст та передбачати, знати правові наслідки певної поведінки. Серед вимог, пов'язаних із наданням нормам КК такої якості, розробники проєкту наголошували також й на необхідності додержання *єдиної термінології* [1, с. 446].

У часи реформування кримінального законодавства, як правило, актуалізується й питання *наступності*. У праві концептуально вирішується можливість збереження досягнень попереднього законодавства, що витримали апробацію часом і на час прийняття нового законодавства відповідають стандартам цивілізованого кримінального права. Найбільші дискусії розгорнулися навколо принципів, інститутів та найбільш важливих понять кримінального права. Так, на відміну від підходів до підготовки проєкту КК робочою групою Кабміну України, розробники альтернативного Кримінального кодексу України, що готувався під керівництвом професора В. М. Смітієнко, поставили під сумнів основні досягнення доктрини кримінального права, зокрема, фундаментальні принципи, вихідні інститути, загальне поняття злочину, що на той час становлення національного права поділялися більшістю провідних науковців [5, с. 10]. Наприклад, стосовно поняття злочину пропонувалося відмовитися в ньому від ознаки суспільної небезпечності, зберегти лише ознаку протиправності [1, с. 448].

Поміркковані позиції більшості розробників Кримінального кодексу, що був прийнятий у 2001 році, дозволили зберегти і розвинути положення про підстави кримінальної відповідальності, межі чинності кримінального закону, форми вини, відповідальність за незакінчений злочин, співучасть тощо [3, с. 538–539].

Постійні звернення до концептуальних положень при обговоренні змісту проєкту нового КК, їх відшліфовка в дискусіях з опонентами, врахування слушних пропозицій та доповнень дозволило його розробникам вже в 1994 році визначитися із основними концептуальними положеннями цього законопроєкту [7, с. 273–275]. Було запропоновано розглядати їх у межах п'яти блоків: 1) джерела проєкту КК; 2) структура його Загальної та Особливої частин; 3) їх зміст; 4) законодавча техніка; 5) перехідні положення.

Джерела проєкту КК. Це широка наукова, правотворча та правозастосовна база, вітчизняний та зарубіжний досвід, опираючись на які розробники могли вирішувати питання: *співвідношення* проєкту та Конституції України; іншого законодавства; а також міжнародно-правових актів щодо прав людини, кримінального правосуддя, діяльності кримінальної юстиції.

Структура КК. Запропоновано зберігати традиційний поділ КК на частини та глави (за чинним КК – розділи). Визначено, що поділ частин на глави повинен стати значно дрібнішим порівняно з КК УРСР 1960 року. Так, Загальна частина чинного КК на час його прийняття складала 15 розділів (у КК 1960 р. їх було лише 5), Особлива – 20 розділів (було 11). В основу послідовності глав Загальної частини покладена логіка їх розвитку. До числа нових глав у 1994 році були запропоновані «Підстава кримінальної відповідальності», «Поняття злочину. Класифікація злочинів», «Особи, які підлягають кримінальній відповідальності», «Вина та її форми», «Незакінчений злочин» та інші. У процесі подальшої роботи над проєктом назви окремих глав були змінені, як і їх зміст. Передбачалося також, що обсяг Загальної частини майбутнього КК значно збільшиться. Були запропоновані принципи формування цієї частини КК: а) додержання непорушності захисту природніх і невідчужуваних прав і свобод людини і громадянина; б) строга залежність між злочином і покаранням; в) відповідність системи покарань загальноприйнятим стандартам та економічним можливостям держави; г) розумне обмеження судового розсуду при визначенні міри кримінальної відповідальності; ґ) широке використання кримінального заохочення.

Що стосується Особливої частини проєкту КК, то було зазначено, що послідовність її глав повинна відповідати новій ієрархії цінностей: людина (особистість, громадянин), суспільство, держава.

Вимоги до змісту КК. При визначені змісту норм дотримуватися їх повної деідеологізації, десоціологізації, деміфологізації, демілітаризації, а також декриміналізації діянь визначених без достатніх підстав кримінально караними. Проєкт не повинен мати кон'юнктурних та декларативних положень. Його норми ґрунтується на: а) соціальній обумовленості кримінально-правової заборони; б) суворій відповідності визнання діяння злочином теорії криміналізації; в) розумному співвідношенні загальних і спеціальних норм; г) дотриманні єдиних критеріїв при визначені обставин, що обтяжують кримінальну відповідальність

(кваліфікуючі обставини); г) обмеженому використанні бланкетних диспозицій; д) формуванні санкцій з урахуванням класифікаційних груп, визначених в Загальній частині та інше.

Законодавча техніка. Визнано необхідним: а) формувати норми загальної частини найбільш абстрактно, а Особливої – казуїстично; б) викладати норми чітко, ясно, однозначно; в) будувати їх відповідно до вимог системності та логічної послідовності; г) обмежено використовувати спеціальні терміни й оціночні поняття; ґ) викладати норми стисло та з поділом на частини; д) створити главу з роз'ясненнями застосованих термінів, а також надавати за необхідності примітки до окремих статей та глав, інше.

Перехідні положення повинні охоплювати вирішення питань, пов'язаних зі зворотною дією кримінального закону у часі та узгодженістю його з актами суміжних галузей права.

Визначені концептуальні положення стали *вихідною інформацією* для розробників проєкту КК у подальшій діяльності. Робота над цим законопроєктом тривала понад 8 років. Він став результатом колективної праці вчених і практичних працівників, комітетів Верховної Ради України і, звичайно. Народних депутатів, які й прийняли його 5 квітня 2001 р. [4, с. 7]

Список використаної літератури:

1. Бажанов М. М. Избранные труды / сост.: В. И. Тютюгин, А. А. Байда, Е. В. Харитонова, Е. В. Шевченко; отв. ред. В. Я. Таций. Харьков: Право, 2012. 1244 с.

2. Баулин Ю. В. О реформе советского уголовного законодательства в современных условиях. *Тезисы выступлений в областной конференции молодых ученых и соискателей*. Х.: Харьковские высшие курсы МВД СССР, 1990. С. 68–69.

3. Баулін Ю. В. Наступність у кримінальному праві. Велика українська юридична енциклопедія: у 20 т. Т. 17: Кримінальне право / редкол. В. Я. Тацій (голова), В. І. Борисов (заст. Голови) та ін.; Нац. акад. прав. Наук України; Ін-т держави і права ім. В. М. Корецького НАН України; Нац. юрид. ун-т ім. Я. Мудрого. 2017. С. 538–539.

4. Кримінальне право України: Загальна частина: Підручник / М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.; за ред. проф. М. І. Бажанова, В. В. Сташиса. В. Я. Тація. 2-е вид. переб. і допов. К.: Юрінком Інтер, 2004. 480 с.

5. Кримінальний кодекс України (проект): Проблеми теорії та практики. 1994, С. 10.

6. Матеріали проекту Кримінального кодексу України 2001 року. *Архів Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України*. Книга 1 (1991–1994 рр.). С. 179–184.

7. Матеріали проекту Кримінального кодексу України 2001 року. *Архів Національного юридичного університету імені Ярослава Мудрого*. Книга 6 (1994–1995 рр.). С. 273–275.

8. Пояснювальна записка до проекту Кримінального кодексу України, підготовленого робочою групою Кабінету Міністрів України. *Українське право,* 1997. Число 2(7). С. 127.

9. Про підготовку проєктів законодавчих актів України: Постанова Президії ВР України від 31 жовтня 1991 р. №1759-XII. *ВВР України*. 1991. №52. Ст. 780.

10. Смородинський В. С. Кодифікація законодавства. *Велика українська юридична енциклопедія*: у 20 т. Т. 3. Загальна теорія права / редкол.: О. В. Петришин (голова) та ін. Х.: Право, 2017. 952 с.

ЦИФРОВА ТРАНСФОРМАЦІЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ПІД ЧАС ВОЄННОГО СТАНУ

Глинська Наталія Валеріївна,
доктор юридичних наук, старший науковий співробітник
завідувачка відділом дослідження проблем кримінального процесу
та судоустрою НДІ ВПЗ ім. акад В. В. Сташиса НАПрН України

Діджиталізація обґрунтовано визнається однією з основних тенденцій розвитку українського кримінального провадження. Запровадження новітніх цифрових технологій у цій царині є вельми затребуваним з огляду на перспективу суттєвого підвищення ефективності діяльності суб'єктів кримінального провадження при вирішенні його завдань, зокрема, у спосіб надання органам досудового розслідування нових можливостей щодо розкриття злочину, встановлення особи, яка його вчинила, та її місця знаходження, прискорення провадження через застосування режиму відеоконференції тощо. Це, з одного боку. Із другого боку, автоматизація та переведення кримінального провадження в електронний формат (створення електронного кримінального провадження), що є одним з основних напрямів цифровізаії кримінального провадження (далі – ЦКП), значно спростить взаємодію суб'єктів кримінального провадження внаслідок упровадження електронної форми процесуальної комунікації, зменшить час погодження певних різновидів процесуальних рішень, а отже, сприятиме реалізації принципу розумних строків.

Чому в екстраординарних умовах функціонування кримінального судочинства у воєнний час проблематика подальшої цифровізації кримінального провадження ЦКП стає ще більш актуальною?

Триваюча з 24 лютого 2022 р. повномасштабна російська збройна агресія проти України поставила перед кримінальним судочинством багато нових викликів. З одного боку, це необхідність мобілізації усіх можливих міжнародних і національних інструментів для притягнення до відповідальності країни-агресора та її вищого керівництва, розслідування учинених на території України воєнних злочинів. З другого боку, об'єктивною стала потреба вимушеного прискорення та спрощення певних процедур і порядків, зокрема, щодо збирання доказів із метою забезпечення дієвості кримінального процесуального механізму розслі-

дування та судового розгляду усіх кримінальних правопорушень, а також більш активного використання цифрових технологій для дистанційного проведення окремих процесуальних дій та ін.

І в цьому сенсі, якщо пандемія COVID-19 вже довела важливість та потребу цифрових технологій для забезпечення функціонування кримінального провадження в дистанційних умовах та створила стимул для реформування системи правосуддя у цьому напряму, реалії ж воєнного стану в Україні стали додатковим поштовхом до прискорення ЦКП із метою розв'язання нових завдань, що постали в цих нелегких умовах (зокрема, щодо необхідності обов'язкового забезпечення фіксування проведення певних процесуальних дій технічними засобами, опрацювання великої кількості інформації, що знаходиться у відкритих джерелах, забезпечення ефективної системи комунікації із населенням, проведення слідчих (розшукових) дій на великих територіях тощо).

До того ж російське вторгнення в Україну поставило одним з першочергових завдань прискорену європейську інтеграцію нашої держави, а значить, й приведення кримінального процесуального законодавства у відповідність до вимог міжнародно-правових актів, зокрема Конвенції про кіберзлочинність, Європейської етичної хартії про використанню штучного інтелекту у судовій системі та її середовищі, концепції «Цифровий порядок денний для Європи» в рамках європейської стратегії економічного розвитку «Європа 2020: стратегія розумного, сталого і всеосяжного зростання» та Рекомендацій CM / Rec (2020) 1 Комітету Міністрів державам-членам щодо впливу алгоритмічних систем на права людини тощо, а також необхідність урахування європейського та міжнародного досвіду щодо ЦКП.

При цьому примітним є те, що проблематика ЦКП нерідко пов'язується дослідниками з упровадженням e-case-менеджменту та переведенням окремих процесуальних відносин у систему електронного документообігу. Однак ЦКП не обмежується виключним використанням технологій; вона характеризується зміною культури та способу мислення правозастосовників, набуттям ними цифрової компетентності; формуванням нових способів і принципів цифрової взаємодії учасників правовідносин тощо.

ЦКП -це багатоаспектне поняття, що в діяльнісному розумінні являє собою як процес розумного впровадження (розумне оснащення) цифрових та інформаціних 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 цієї царині. Цифрова трансформація кримінального провадження (ЦТКП) – це закономірний результат процесу ЦКП, якісна визначеність якого характеризується певним рівнем перетворенням кримінального провадження, обумовленим переходом до нових способів діяльності з використанням цифрових технологій, адаптацією до специфіки цифрового середовища (цифрової інформації).

Актуальними напрямами цифровізації кримінального судочинства є:

– переведення документообігу в царині кримінального провадження в електронну форму (нагальна необхідність переведення документування кримінального провадження в електронний сегмент є базовою передумовою розробки електронного кримінального провадження);

– подальше впровадження електронного правосуддя в Україні;

– розширення можливості здійснення правосуддя в дистанційному форматі;

– запровадження єдиної інтегрованої електронної системи органів кримінальної юстиції, поєднаної із загальнодержавними електронним реєстрами та базами даних (електронного кримінального провадження (ЕКП));

– використання інформаційно-аналітичних систем та інтелектуальних алгоритмів для підвищення ефективності розслідування кримінальних правопорушень;

– розширення цифрового сегменту під час проведення слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій;

– вдосконалення судового контролю в умовах ЦКП;

– забезпечення виконання координаційних функцій у царині ЦКП;

– використання технології штучного інтелекту в кримінальному провадженні;

– створення єдиної цифрової платформи для процесуальної комунікації учасників кримінального провадження та електронної взаємодії населення з державними органами на початковому етапі досудового розслідування (створення online серверів для подання заяв, повідомлень про вчинене правопорушення);

– впровадження електронних механізмів запобігання порушенню прав і свобод учасників кримінального провадження;

– використання електронних доказів у кримінальному провадженні;

– дослідження процесуальних особливостей розслідування кіберзлочиннів;

– використання цифрових технологій під час міжнародного співробітництва в кримінальному провадженні та ін.

Визначені напрями, безумовно, є тісно пов'язаними один з одним. Утім, окреме їх виділення як самостійних векторів наукової розвідки є необхідним для всебічного та повного аналізу відповідної проблематики та отримання наукових результатів, що в сукупності створюватимуть концепцію цифрової трансформації кримінального провадження в Україні.

Формула ЦТКП має корелювати із забезпеченням прав та свобод особи в цій царині. Відповідно гарантованість прав та свобод особи під час кримінальної процедури є основним вектором прийняття цифрових рішень.

Як влучно зазначено у Висновку № 14 (2011) Консультативної ради європейських суддів «Судочинство та інформаційні технології» *ІТ повинні бути інструментом або засобом забезпечення гарантій, встановлених ст. 6 ЄКПЛ.*

В цьому сенсі показовою є позиція Європейського суду з прав людини (далі – ЄСПЛ) стосовно того, що держава за певних умов може бути визнана відповідальною, якщо вона не запроваджує заходів електронного правосуддя. Так, в одному з рішень проти Словаччини (з приводу не створення інфраструктури для подачі заяв за допомогою електронних процедур) було констатовано, що якщо подача заяви в електронному вигляді необхідна в силу об'єктивних обставин, нав'язане державою обмеження може призвести до порушення статті 6 (1) Конвенції про захист прав людини і основоположних свобод (далі – Конвенція), фундаментального права на доступ до правосуддя та права на справедливий судовий розгляд; держава своєю поведінкою «непропорційно обмежила право заявника представити свою справу в суді ефективним чином».

Принагідно зауважімо, що той же ЄСПЛ в аспекті гарантованих прав і свобод за статтею 6 Конвенції (право на справедливий суд) у своїй практиці наголошує на недопустимість відмови особі звертатись до суду в традиціному «паперовому форматі». Так, у рішення по справі XAVIER

LUCAS v. France, ЄСПЛ у визнав відмову апеляційного суду прийняти від заявника паперову версію процесуального документа надмірним формалізмом, адже адвокат заявника обґрунтовував неможливість подання документа за допомогою електронної платформи помилками в її функціонуванні. Тож ЄСПЛ констатував порушення вимог статті 6 Конвенції.

Вразливість царини кримінального провадження обумовлює особливий підхід, зокрема, до унормування можливості та процедури дистанційного провадження. В цьому сенсі цінними є дороговкази, що були напрацьовані європейською правовою спільнотою за результатом аналізу досвіду здійснення судочинства в умовах пандемії.

У затвердженому Європейською комісія з питань ефективності правосуддя (CEPEJ) на 36-му пленарному засіданні (16–17 червня 2021 р.) Керівництві щодо проведення судових проваджень у режимі відеоконференції, окреслено низку основних заходів, які мають вживатись державами й судами, щоб під час проведення судових проваджень у режимі відеоконференції запобігти підриву права на справедливий суд, яке гарантується статтею 6 Конвенції. При цьому поряд із загальними рекомендаціми у Керівництві державам визначаються окремі дороговкази, спрямовані на усунення будь-яких ризиків порушення прав сторін під час проведення дистанційних судових засідань у кримінальних провадженнях, зокрема, права на захист. Такі особливості стосуються гарантування забезпечення активної участі обвинуваченого, ефективності спілкування із захисником тощо.

ДИСТАНЦІЙНЕ СУДОВЕ ПРОВАДЖЕННЯ: АКТУАЛЬНІ ПИТАННЯ ЗА ПРАКТИКОЮ ЄСПЛ

Дроздов Олександр Михайлович,
доктор юридичних наук, професор, заслужений юрист України,
доцент кафедра кримінального процесу Національного юридичного університету імені Ярослава Мудрого

Сучасні технології, які ще й до того стрімко розвиваються, впроваджуються в усі сфери людського життя. Звісно, що ці технології значно полегшують та спрощують найрізноманітніші процеси. Разом з тим застосування технологій обумовлює необхідність вирішення специфічних завдань, які раніше й не виникали.

Відомо, що кримінальне провадження зачіпає основоположні права людини, такі як право на свободу та особисту недоторканність, право на справедливий суд. Тому застосування цифрових технологій має бути доволі обережним, виваженим, що своєю чергою потребує глибокого розуміння змісту самих основоположних прав людини. Однак сутність кримінального провадження сама по собі не виключає доцільності оптимізації судового провадження, розгляду та вирішення кримінальних справ судом за допомогою цифрових інструментів.

Наразі кримінальне процесуальне законодавство включає нечисленні норми, що регламентують застосування технологій у кримінальному провадженні, що свідчить про поступову та обережну цифровізацію цієї фундаментальної галузі. Загалом в КПК встановлено, що дистанційне судове провадження згідно з правилами статті 336 КПК може здійснюватися в судах першої, апеляційної та касаційної інстанцій під час здійснення судового провадження з будь-яких питань, розгляд яких віднесено до компетенції суду (ч. 9 ст. 336 КПК). Водночас судова практика, яка формується в умовах воєнного стану, обумовлює необхідність більш детальної регламентації використання цифрових технологій у кримінальному провадженні. Однак щоб увесь потенціал сучасного рівня розвитку цифрових технологій міг бути використаний повною мірою та без негативного впливу на якість кримінального процесу, слід при розробці нових норм та практик враховувати релевантну практику Європейського суду з прав людини (далі – ЄСПЛ). Отже в цій

публікації спробую висвітлити відповідну практику ЄСПЛ з окреслених питань[1].

1. ЄСПЛ не часто звертається до розгляду питань, пов'язаних із судовими засіданнями у режимі відеоконференції, з точки зору права на справедливий судовий розгляд відповідно до статті 6 Європейської конвенції з прав людини (далі – Конвенція). Однак прецедентне право ЄСПЛ містить деякі керівні принципи щодо цього.

Основні принципи прецедентної практики Суду щодо участі обвинуваченого в судовому слуханні через відеоконференцію викладені у справі «*Марчелло Віола проти Італії*» (2006, § 67): участь обвинуваченого у провадженні в режимі відеоконференції не суперечить Конвенції; тим не менш, звернення до цього заходу в будь-якому окремому випадку має служити законній (легітимній) меті; заходи для надання показань повинні відповідати вимогам дотримання належної правової процедури, як це викладено у статті 6 Конвенції.

У своїй прецедентній практиці ЄСПЛ послідовно застосовував вищезазначені принципи. Однак він наголосив на необхідності забезпечення відповідних процедурних гарантій. Зокрема, Суд постановив, що підсудний повинен мати можливість стежити за процесом і бути заслуханим без технічних перешкод і мати ефективне та конфіденційне спілкування з адвокатом (*Grigoryevskikh v. russia*, 2009, § 83).

2. Розпочнемо з «*легітимної мети*» судових проваджень у режимі відеоконференції. У згадуваній справі «*Марчелло Віола проти Італії*» стосовно участі члена мафії в апеляційному розгляді в режимі відеоконференції через те, що він перебував під особливим режимом ув'язнення, ЄСПЛ встановив, що участь заявника в апеляційному розгляді в режимі відеоконференції переслідувала законні цілі згідно з Конвенцією: запобігання заворушенням, запобігання злочинам, а також захист свідків і жертв правопорушень щодо їхніх прав на життя, свободу та безпеку (§ 72).

Також у справі «*Марчелло Віола*» ЄСПЛ вважав легітимною метою дотримання вимоги «розумного строку» в судовому розгляді. На думку ЄСПЛ, режим відеоконференції також мав на меті скоротити затримки,

[1] Огляд практики ЄСПЛ здійснено на підставі посібника: KEY THEME Article 6 (criminal limb) Hearings via video link (Last updated: 31/08/2022). URL: https://ks.echr.coe.int/documents/d/echr-ks/hearings-via-video-link

які виникають у передачі затриманих, і таким чином спростити та прискорити кримінальне провадження (там само).

Проте з практики ЄСПЛ випливає, що національні органи влади повинні навести достатні підстави, якщо вони вирішать, що обвинувачений братиме участь у судовому розгляді в режимі відеоконференції. У справі «*Медвєдєв проти росії*» (2017, § 30), ЄСПЛ зазначив, що заявник, який був ув'язнений у Москві, не міг особисто брати участь у слуханні апеляції в Москві та що Уряд не обґрунтував рішення організувати участь заявника через відеозв'язок, а не забезпечення його присутності в залі суду.

3. Далі, наскільки це дозволяє формат наукової доповіді, торкнуся питань *явки в судове засідання* під час судового провадження в першій інстанції:

ЄСПЛ ще не розробив конкретних принципів щодо судового розгляду у першій інстанції у режимі відеоконференції. Однак зазначені вище стандарти, розроблені у справі «*Марчелло Віола проти Італії*» також застосовуються в цьому контексті (*Asciutto v. Italy* (2007 р.), §§ 62–72). Крім того, у справі «*Сахновський проти росії*» (ВП, 2010, § 96), стосовно розгляду у режимі відеоконференції, ЄСПЛ зазначив, що особа, обвинувачена у вчиненні кримінального правопорушення, повинна, виходячи із загального принципу, заснованого на понятті справедливого судового розгляду, мати право бути присутньою у судовому засіданні в суді першої інстанції. Дійсно, згідно з прецедентною практикою ЄСПЛ, у деяких випадках участь у судовому засіданні у режимі відеоконференції може бути заходом, що забезпечує ефективну участь у провадженні (*Bivolaru v. Romania (№ 2),* 2018, §§ 138–139, 144–145; *Dijkhuizen проти Нідерландів*, § 56).

Слід також мати на увазі, що стаття 6 Конвенції у цілому гарантує право обвинуваченого на ефективну участь у кримінальному провадженні в суді (*Муртазалієва проти росії* [ВП], 2018, § 91). Загалом, це включає, серед іншого, не тільки його або її право бути присутнім, але також слухати та стежити за процесом. Відповідно, погана акустика в залі суду та проблеми зі слухом можуть стати приводом для встановлення порушення статті 6 Конвенції (*Стенфорд проти Сполученого Королівства*, 1994, §§ 26 і 29).

4. ЄСПЛ розглядав низку справ щодо *апеляційного провадження* через відеозв'язок (*Марчелло Віола проти Італії*, 2006; *Сахновський*

проти росії [ВП], 2010; *Шулепов проти росії*, 2008; *Юдін проти росії*, 2018; *Медведєв проти росії*, 2017 р.; *Слащев проти росії*, 2012 р.).

У справі «*Grigoryevskikh v. russia*», 2009, ЄСПЛ повторив, що стаття 6 Конвенції не завжди передбачає право на особисту присутність, навіть якщо апеляційний суд має повну юрисдикцію розглядати справу як з питань факту, так і з питань права (§ 77). Таким чином, він підкреслив, що використання відеопоказань само по собі не є порушенням статті 6 Конвенції.

ЄСПЛ зазначив, що фізична присутність обвинуваченого в залі суду є дуже бажаною, але це не є самоціллю. Це скоріше служить вищій меті – забезпеченню справедливості судового розгляду в цілому (Голубєв проти росії (ухв.), 2006).

У деяких випадках ЄСПЛ окремо не перевіряє, чи було порушено право бути присутнім на засіданні через саму участь у засіданні за допомогою відеозв'язку. Наприклад, у справі *Grigoryevskikh проти росії*, (§ 94), ЄСПЛ дійшов висновку, що скарга щодо проведення апеляційного слухання за допомогою відеозв'язку значною мірою збігається зі скаргою щодо відсутності правової допомоги під час апеляційного слухання. Таким чином, ЄСПЛ не вважав за потрібне окремо розглядати питання про те, чи в обставинах цієї справи участь заявника в апеляційному слуханні через відеозв'язок відповідала статті 6 Конвенції (див. також *Ichetovkina and Others v. russia*, 2017, § 45).

5. Згідно з прецедентною практикою ЄСПЛ, *здійснення права на правову допомогу* набуває особливого значення, коли заявник спілкується із залою суду через відеозв'язок (*Grigoryevskikh v. russia*, § 92):

Так ЄСПЛ постановив у кількох справах, що інтереси правосуддя вимагають, щоб для справедливого слухання заявники, які постали перед судом у режимі відеоконференції, були представлені адвокатом, особливо коли в судовому засіданні брав участь представник державного обвинувачення під час слухання справи (*Shulepov v. russia*, 2008, §§ 34–36; *Slashchev v. russia*, 2012; *Grigoryevskikh v. russia).* У вже згадуваному рішенні по справі *Сахновський проти росії,* ЄСПЛ наголосив на необхідності забезпечення відповідних умов і часу для консультації з адвокатом, коли підсудний бере участь у судовому засіданні через відеозв'язок (на противагу *Marcello Viola проти Італії* і *Голубєв проти росії* (ріш.), 2006, де адвокати заявників були присутні в залі суду). У цьому контексті ЄСПЛ також постановив, що право обвинуваченого спілкуватися

зі своїм адвокатом без ризику бути підслуханим третьою стороною є однією з основних вимог справедливого судового розгляду відповідно до статті 6 § 3(c) Конвенції. Якби адвокат не міг розмовляти зі своїм клієнтом без нагляду та надавати конфіденційні інструкції, його допомога втратила б значну частину своєї користі, тоді як метою Конвенції є захист конкретних і ефективних прав (*Сахновський проти росії*, § § 97, 102 і 104; *Медведєв проти росії*, 2017, § 30; *Юдін проти росії*, 2018, §§ 41–44; *Загарія проти Італії*, 2007)

6. Проведення судового засідання у режимі відеоконференції можуть викликати питання щодо необхідності забезпечення *гласності і відкритості судового провадження*, і певні аспекти прецедентного права можуть мати значення в цьому відношенні.

Згідно з прецедентною практикою ЄСПЛ, судовий процес відповідає вимозі публічності лише в тому випадку, якщо широка громадськість має можливість отримати інформацію про його дату та місце, і якщо це місце є для неї легкодоступним.

У багатьох випадках ці умови задовольняються простим фактом, що слухання проводяться у звичайній залі суду, яка є достатньо великою, щоб вмістити глядачів. Однак проведення судового процесу поза звичайною залою судових засідань у місцях, куди в принципі не має доступу широка громадськість, є перешкодою для його публічного характеру. У такому випадку держава зобов'язана вжити компенсаційних заходів, щоб забезпечити належне інформування громадськості та ЗМІ про місце слухання та надання їм ефективного доступу (*Riepan проти Австрії*, 2000, § 29; Hummatov проти Азербайджану, 2007, § 144).

При дистанційному судовому провадженні також може виникнути проблема щодо доступу до матеріалів справи та розкриття доказів.

ЄСПЛ постановив, що за певних умов обвинуваченому не обов'язково надавати прямий доступ до матеріалів справи, достатньо, щоб його захисники були поінформовані про матеріали справи (*Kremzow v. Austria*, 1993, § 52).

Проте обмежений доступ обвинуваченого до матеріалів суду не повинен перешкоджати тому, щоб докази були доступні обвинуваченому до судового розгляду, а обвинуваченому була надана можливість прокоментувати їх через свого адвоката в своїх усних поясненнях (*Öcalan проти Туреччини* [ВП], 2005, § 140).

Коли обвинуваченому було дозволено самостійно захищатися, відмова йому в доступі до матеріалів справи становить порушення прав на захист (*Фуше проти Франції* (*Foucher v. France)*, 1997, §§ 33–36).

Щоб сприяти здійсненню захисту, обвинуваченому не можна перешкоджати отримувати копії відповідних документів із матеріалів справи або складати та використовувати будь-які зроблені нотатки (*Rasmussen проти Польщі*, 2009, §§ 48–49; *Moiseyev проти росії*, 2008 р., §§ 213–218; *Matyjek проти Польщі*, 2007 р., § 59; *Seleznev проти росії*, 2008 р., §§ 64–69).

Що стосується електронних файлів і розкриття електронних даних, важливо забезпечити, щоб захист мав можливість брати участь у встановленні критеріїв для визначення того, що може мати значення для розкриття інформації (*Sigurđur Einarsson та інші проти Ісландії*, 2019), § 90; див. також *Rook проти Німеччини*, 2019, §§ 67 і 72).

Більше того, щодо ідентифікованих або позначених даних, будь-яка відмова дозволити стороні захисту проводити подальші пошуки таких даних у принципі порушує питання щодо забезпечення відповідних умов для підготовки захисту (*Sigurđur Einarsson and Others v. Ісландії*, § 91).

У зв'язку з цим ЄСПЛ нагадує, що «процедура, за допомогою якої сторона обвинувачення сама намагається оцінити важливість прихованої нею інформації для захисту та зважити це проти суспільних інтересів у збереженні інформації в таємниці, не може відповідати вищезазначеним вимогам ст. 6 § 1 Конвенції (*Роу і Девіс проті Сполученого Королівства*, 2000, § 63)

Спосіб, у який обвинувачений з'являється на судовому засіданні, яке проводиться в режимі відеоконференції, також може мати значення з точки зору права на справедливий суд. Наприклад, ЄСПЛ постановив, що було б важко узгодити таке, що принижує гідність, поводження з підсудним під час судового провадження з поняттям справедливого судового розгляду, беручи до уваги важливість рівності сторін, презумпції невинуватості та довіри. які суди в демократичному суспільстві повинні вселяти в громадськості, перш за все в обвинувачених (*Ярослав Бєлоусов проти Росії*, 2016, § 147).

Підбиваючи підсумки можна стверджувати, що наведена практика ЄСПЛ має слугувати надійним орієнтиром для формування належної правової процедури здійснення дистанційного судового провадження.

ЦИФРОВІ АСПЕКТИ ВІДНОВЛЕННЯ ВТРАЧЕНИХ МАТЕРІАЛІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Тетерятник Ганна Костянтинівна,
доктор юридичних наук, професор, завідувач кафедри кримінального процесу Одеського державного університету внутрішніх справ

Стукаленко Ганна Володимирівна,
аспірантка кафедри кримінального процесу Одеського державного університету внутрішніх справ

Інститут відновлення втрачених матеріалів кримінального провадження з початком повномасштабної збройної агресії рф зазнав значних змін. Питання ефективної процедури відновлення матеріалів кримінального провадження як гарантії забезпечення права учасників кримінального провадження на справедливий суд було предметом розгляду ЄСПЛ у справах «Хлєбік проти України» (Заява № 2945/16) від 25 липня 2017 року, «Кукроченко та Золотухін проти України» (заяви № 20936/16 та № 53257/16). У них крім іншого ЄСПЛ дослідив, чи зробила держава усе можливе, щоб організувати судову систему таким чином, щоб гарантувати право на справедливий суд для людей, на яких вплинули бойові дії [1, с. 446–448].

Законом України № 2201-IX від 14.04.2022 р. розділ IX-1 КПК України було доповнено статтею 615–1 «Відновлення втрачених матеріалів кримінального провадження», а Законом України «Про внесення змін до Кримінального процесуального кодексу України щодо уточнення положень про відновлення втрачених матеріалів кримінального провадження, скасування запобіжного заходу для проходження військової служби в умовах воєнного стану» від 16.11.2022 року № 2751-IX внесено низку змін до зазначеної норми.

Не підлягає сумніву важливість й актуальність питання збереження матеріалів кримінального провадження, а у випадку їх втрати – ефективного відновлення, особливо у нинішніх умовах, пов'язаних із тимчасовою окупацією окремих територій України, активними бойовими діями у нашій державі, обстрілами рф об'єктів цивільної та критичної інфраструктури, що внаслідок різних факторів можуть призвести до втрати таких.

На нашу думку, ч. 14 ст. 615 КПК України також є спробою законодавця створити певні гарантії до збереження та можливого відновлення втрачених матеріалів кримінального провадження. У вказаній нормі зазначається: «Копії матеріалів кримінальних проваджень, досудове розслідування в яких здійснюється в умовах воєнного стану, в обов'язковому порядку зберігаються в електронній формі у дізнавача, слідчого чи прокурора» [2]. Автори коментарів до розділу розділ IX-1 КПК України вбачають наступні шляхи реалізації цього припису.

По-перше, *виготовлення в електронній формі з використанням кваліфікованого електронного підпису службової особи* [3, с. 46]. На сьогодні кваліфікований електронний підпис є уже розповсюдженим у багатьох сферах життя. Зокрема, завдяки цифровому застосунку «Дія» та іншим можливостям генерування криптографічних підписів. Крім того, відповідно до ч. 4 ст. 106–1 КПК України «Документи, підписані, погоджені в інформаційно-телекомунікаційній системі досудового розслідування з використанням кваліфікованого електронного підпису, їх примірники в електронній та паперовій формах визнаються оригіналами документів». А також до «воєнних» новел кримінального процесуального законодавства належить можливість виготовлення постанови в електронній формі з використанням кваліфікованого електронного підпису службової особи, яка прийняла відповідне процесуальне рішення, або створюється з використанням Інформаційно-телекомунікаційної системи досудового розслідування відповідно до статті 106–1 КПК України (ч. 6 ст. 110 КПК України). Втім, інформаційно-телекомунікаційна система досудового розслідування не функціонує на сьогоднішній день в органах досудового розслідування повноцінно. Певний прогрес системи електронного документообігу вбачається здебільшого в НАБУ та САП. Крім того, можливість винесення постанови в електронній формі не знімає питань збереження та електронної форми інших матеріалів кримінального провадження.

По-друге, *створення документів з використанням Інформаційно-телекомунікаційної системи досудового розслідування* [3, с. 47]. Обмеженість цього шляху уже зазначена вище.

По-третє, *оцифрування, тобто переведення матеріалів кримінального провадження в електронний формат* [3, с. 48]. На сьогоднішній день така форма є найбільш розповсюдженою на практиці. Представники органів досудового розслідування мають сканувати відповідні матеріали

кримінальних проваджень, формувати в електронні томи. Слід відзначити, що Офісом Генерального прокурора надаються відповідні рекомендації щодо такого оцифрування та оформлення матеріалів. Натомість дотепер відсутні підзаконні нормативно-правові акти, які б могли більш детально алгоритмізувати такі процедури. Крім того, досить складною організаційно є ця робота з урахуванням навантаження на органи досудового розслідування в умовах воєнного стану та широкомасштабної збройної агресії.

Частина 14 ст. 615 КПК України встановлює загальне правило щодо копіювання і збереження матеріалів досудового розслідування, що здійснюється в умовах воєнного стану, слідчим, дізнавачем чи прокурором. Втім, невирішеною залишається низка питань:

1) у якому форматі мають створюватися такі копії;

2) на яких носіях чи цифрових платформах вони мають зберігатися (адже зрозуміло, що копіюватися мають не тільки паперові документи, а й фото-, аудіо-, відео- дані, які можуть займати значний обсяг. Крім того, мають бути встановлені відповідні технічні вимоги до таких носіїв та платформ, з метою унебезпечення витоку інформації);

3) який строк копіювання і подальшого збереження цих матеріалів;

4) яку відповідальність за дотримання вимог ч. 14 ст. 615 КПК України мають нести службові особи, визначені у ній;

5) якими є гарантії забезпечення таємниці досудового розслідування, персональних даних учасників кримінального провадження, унеможливості внесення змін до скопійованих матеріалів та їх знищення при копіюванні і збереженні такої інформації (іще й в умовах широкомасштабної війни);

6) які особливості та механізми копіювання і зберігання матеріалів негласних слідчих (розшукових) дій та матеріалів, що містять відомості, які становлять державну таємницю;

7) який порядок передання таких матеріалів у випадку зміни особи, яка веде досудове розслідування, процесуального керівника, передачі матеріалів за підслідністю та ін.

Окрім того, що має бути розроблений відповідний міжвідомчий підзаконний нормативно-правовий акт, у якому б визначалися організаційні питання та окремі механізми копіювання і збереження таких матеріалів, відповідні зміни та доповнення до КПК України, конкретизації підлягає і сама ч. 14 ст. 615 КПК України. Доцільно конкретизувати, що обов'язок

копіювання і збереження таких матеріалів лежить на дізнавачі, слідчому, у провадженні яких знаходяться відповідні матеріали або, які призначені як старші групи чи відповідальні особи за збереження таких. Використання терміну «прокурор» також створює труднощі для тлумачення цієї норми. Формулювання «досудове розслідування в яких здійснюється в умовах воєнного стану» також має розмиті темпоральні ознаки. Наприклад, досудове розслідування може здійснюватися у кримінальних провадженнях, які були зупинені до початку воєнного стану, але після підлягали відновленню. У такому випадку виникає питання: чи усі матеріали підлягають копіюванню та збереженню в електронній формі чи тільки ті, які зібрані в умовах воєнного стану? Логічною буде відповідь: усі. Натомість, яким чином забезпечити копіювання і збереження такого обсягу матеріалів кримінального провадження ще й в умовах описаної правової невизначеності цієї процедури, незрозуміло.

Таким чином, попри певні позитивні зрушення щодо питань нормативного врегулювання відновлення втрачених та збереження в електронній формі матеріалів кримінального провадження, слід констатувати необхідність забезпечення правової визначеності вищезазначених питань, створення ефективних механізмів копіювання і збереження матеріалів досудового розслідування. У подальшому це може стати дієвою гарантією відновлення матеріалів кримінального провадження у разі їх втрати.

Список використаної літератури:

1. Тетерятник Г. К. Кримінальне провадження в умовах надзвичайних правових режимів: теоретико-методологічні та праксеологічні основи: монографія. Одеса: Видавничий дім «Гельветика», 2021. 500 с.

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. №4651-VI. Відомості Верховної Ради України. 2013. №9–10, №11–12, №13. Ст. 88.

3. Гловюк І., Дроздов О., Тетерятник Г., Фоміна Т., Рогальська В., Завтур В. Особливий режим досудового розслідування, судового розгляду в умовах воєнного стану: науково-практичний коментар Розділу IX-1 Кримінального процесуального кодексу України. Видання 2. Електронне видання. Дніпро-Львів-Одеса-Харків, 2022. Станом на 03 травня 2022. 58 с.

ЩОДО АКТУАЛЬНИХ ПИТАНЬ ДІЯЛЬНОСТІ СУДУ ПІД ЧАС ВОЄННОГО СТАНУ

Шаренко Світлана Леонідівна,
доктор юридичних наук, доцент кафедри кримінального процесу Національного юридичного університету імені Ярослава Мудрого, голова Київського районного суду м. Харкова

Умови воєнного стану, які викликані збройною агресією російської федерації проти України, значною мірою впливають на всі правовідносини та інституції в країні. Відповідно до ст. 10 Закону України «Про правовий режим воєнного стану», повноваження судів не можуть бути припинені, скорочення чи прискорення будь-яких форм судочинства забороняється. Але, разом з тим, судова гілка влади також зазнала впливу війни та її наслідків, що внесло свої корективи в процеси здійснення судочинства.Частина судів України призупинили свою діяльність через активні бойові дії, а інші продовжили здійснювати правосуддя. На наш погляд, проблемним виявилося питання визначення об'єктивної неможливості відправлення правосуддя самими суддями цих судів. Так, наприклад, у м. Харкові, який не був окупованим, однак піддавався постійним обстрілам, із 9 загальних судів продовжили виконувати свій конституційний обов'язок лише 3 суди, а інші призупинили роботу. Законність таких рішень є сумнівною, оскільки голова військової адміністрації не приймав рішення про евакуацію державних підприємств, установ, організацій із міста. Більш того, правоохоронні підрозділи активно виконували свої безпосередні обов'язки, а також допомогали цивільному населенню з забезпеченням продуктами харчування, ліками; розселяли тих, хто втратив житло; перевозили власним транспортом спеціалістів об'єктів критичної інфраструктури; доставляли населення до лікарень. Разом з тим, у зв'язку з відсутністю суддів у 6 районних судах міста та апеляційного суду області, слідчі та прокурори змушені були долати щонайменше 150 км в один кінець для того, щоб звернутися з клопотанням про дозвіл на здійснення негласних слідчих розшукових дій або звернутися з обвинувальним актом для його розгляду по суті тощо. Відсутність в законодавстві норми, яка б упорядковувала порядок призупинення здійснення судочинства (станом на 24.02.2022) та невнесення таких дефініцій до теперішнього часу, створили колапс в результаті якого на-

селення не тільки не отримало доступу до правосуддя, а взагалі втратило надію віднайти свої справи, в яких містяться оригінали документів, квитанції про сплачений судовий збір тощо. Оскільки суди, яким була визначена підсудність справ, як правило, взагалі не реєстрували ці справи (така ситуація існує і на цей час).

Питання впровадження можливості дистанційного правосуддя набуло піку своєї популярності ще в лютому-березні 2020 року, коли весь світ був стурбований Covid-19 та викликами, які постали у зв'язку з його поширенням. У 2020 р. Верховна Рада України прийняла закони, які надали можливість реалізувати право учасникам справи брати участь в судових засіданнях, тим самим реалізуючи своє право на справедливий судовий розгляд, дистанційно. У свою чергу, Державна судова адміністрація розробила порядок проведення відеоконференцзв'язку під час судового засідання за участі сторін поза межами приміщення суду. Таким чином, було передбачено використання системи EasyCon або інших доступних для суду та учасників судового процесу засобів, що забезпечують проведення судових засідань в режимі відеоконференцзв'язку. Такий механізм проведення судових засідань в дистанційному форматі, без присутності учасника справи безпосередньо в залі судового засідання, допоміг значно нормалізувати здійснення правосуддя в умовах карантину. Проте практика показує, що умови воєнного стану перешкоджають реалізувати права осіб на розгляд їх справи судом навіть у такий спосіб. Так, наразі в Україні відсутнє повністю безпечне місце і чи не щодня у кожній місцевості нашої держави лунають сирени, що в свою чергу передбачає необхідність особи (судді, учасника справи або працівника суду) переміститись в укриття. Ігнорування зазначених вказівок може мати сумні наслідки, що, на жаль, мали місце в Миколаївській області, коли в результаті ракетного удару по Миколаївській ОДА, у якій був розміщений Господарський суд Миколаївської області, загинули працівники суду.Таким чином, під час повітряних тривог потрібно переривати судове засідання для перебування в укритті. Кількість таких вимушених «переривань» за день може бути різна, як і різна їх тривалість, тому зазначена проблема потребує свого подальшого опрацювання та вирішення з урахуванням імперативних засад судочинства та необхідності забезпечення безпеки працівників суду та учасників справи. Подальші кроки розширення можливостей дистанційного судочинства потребують також технічного та нормативного підґрунтя. У Верховній Раді зареєстрований

законопроект від 26.04.2022 р., яким пропонується забезпечення можливості не лише учасникам справи, але й суддям брати участь в судових засіданнях дистанційно.

Найбільш згадуваною зміною до КПК стала можливість виконання керівником органу прокуратури повноважень слідчого судді у випадку, коли останній об'єктивно не може їх здійснювати. Хто та в який об'єктивний спосіб може визначити відсутність такої можливості законодавцем не визначено. Зазначена норма є найбільшим відступом від судового контролю, адже застосування стороною обвинувачення запобіжного заходу, яким обмежено право на свободу, не може бути оскаржене, затримана особа та її захисник не спілкуються з прокурором, не дають пояснень з приводу обставин затримання і т.д.

Важливим етапом трансформації «воєнних» змін до КПК стало і повернення до загальних строків затримання особи без ухвали слідчого судді. Пропонований строк у 216 год. обурив правозахисників, через що власне і повернулась дія норми про 72 год. Якщо ж у визначений строк немає змоги доставити затриману особу до слідчого судді, тоді обрання запобіжного заходу здійснюється дистанційно. При чому на зв'язку знаходиться затримана особа і при цьому застосовуються будь-які доступні технічні засоби для відеозв'язку.

Воєнний стан в країні фактично прискорив цифрову трансформацію в кримінальному судочинстві, адже відеоконференцзв'язок, дистанційне правосуддя для всіх учасників кримінального провадження, так і для складу суду, який його розглядає, забезпечують доступ до безпечного правосуддя, що є складовою права на справедливий суд.

ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ: НАПРЯМИ ВИКОРИСТАННЯ ТА ПРОБЛЕМИ ЗАКОНОДАВЧОГО ВРЕГУЛЮВАННЯ

Авдєєва Галина Костянтинівна,
кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України,

Коновалова Віолетта Омелянівна,
доктор юридичних наук, професор, академік НАПрН України, головний науковий співробітник НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Термін «штучний інтелект» (ШІ) виник у середині 50-х р.р. минулого століття як новий напрям інформатики і був визначений американським вченим-математиком Джоном Макарті як «наука і техніка створення інтелектуальних машин» [1]. На сьогодні єдиного загальновизнаного визначення цього терміну не існує, оскільки це міждисциплінарна наука, яка поєднує багато її галузей (інформатика, математика, соціологія, психологія, право та ін.).

У загальному розумінні під системами ШІ традиційно розуміють комп'ютерні системи, що здатні не лише виконувати певні завдання за заздалегідь заданим алгоритмом, а й вирішують творчі завдання на основі аналізу значної за обсягом різноманітної інформації та імітують процеси мислення людини [2, с. 6].

У сучасному світі системи ШІ активно використовуються у системах комунікації, промисловості, сільському господарстві, медицині, транспорті, освіті, науці, побуті та ін. Військове застосування штучного інтелекту та машинного навчання охоплює спостереження, розвідку, аналіз інформації та пропонування певних оптимальних рішень щодо нанесення бойових ударів, надання гуманітарної допомоги, ліквідації наслідків надзвичайних ситуації, прийняття управлінських або логістичних рішень військовим командуванням тощо [3].

Навіть у боротьбі зі злочинністю та забезпеченні громадської безпеки такі системи показали свою ефективність. Зокрема, системи безпеки дорожнього руху виявляють порушення та забезпечують дотриман-

ня правил дорожнього руху, допомагають ідентифікувати транспортні засоби та осіб в несприятливих умовах (низька роздільна здатність фото- або відеокамери, темрява, снігопад, дощ тощо). Прогнози росту злочинності, створені спеціальними системами ШІ, дозволяють підвищити ефективність заходів її попередження.

В Україні створено онлайн-архів для накопичення інформації про скоєні військовими РФ воєнні злочини в Україні [4]. Накопичення інформації про такі злочини є лише підготовчим етапом до їх розслідування. Провина представників російської влади і військових армії РФ має бути доведена шляхом ретельного збирання процесуальних доказів. Під час такого розслідування потрібно не лише довести, що ці злочини були вчинені, а й пов'язати їх з конкретними особами-злочинцями, висунути їм обгрунтоване обвинувачення та притягнути до відповідальності.

При розслідуванні воєнних злочинів системи ШІ ефективно вирішують завдання щодо ідентифікації осіб за фотознімками, відеозаписами та пробами ДНК. Зокрема, за допомогою американської системи розпізнавання осіб Clearview AI, яка використовує базу даних з 10 млрд фотопортретів (в т.ч. – з соціальних мереж), встановлено особи окремих злочинців-військових РФ за їх фотознімками. За допомогою даної системи ідентифіковано понад 1000 осіб (живих і загиблих). Система показала свою ефективність навіть при аналізі зображень понівечених тіл [5].

Після звільнення м. Ізюм Харківської області на деокупованій території ексгумували близько 900 тіл загиблих громадян України, понад 200 з яких ідентифікувати не вдалося. Задля проведення такої ідентифікації 19 грудня 2022 р. харківські слідчі отримали у подарунок від США три лабораторні комплекси для проведення ДНК-експертиз, в яких аналіз результатів дослідження здійснюватиметься за допомогою системи ШІ.

Системи ШІ в усьому світі використовуються під час розслідування злочинів для отримання інформації про осіб та їх дії, різноманітні об'єкти і явища, з метою виявлення і попередження шахрайських дій, для ідентифікації осіб і предметів (в т.ч. – зброї) за їх слідами та ін [6].

Завдання розвитку технологій штучного інтелекту в Україні є одним з пріоритетних напрямів у сфері науково-технологічних досліджень. Вивчення та аналіз «Концепції розвитку штучного інтелекту в Україні» [7] (далі – Концепція) дозволило виокремити напрями удосконалення процесів створення і використання технологій ШІ в Україні, а саме:

– розроблення та використання систем штучного інтелекту лише за умови дотримання верховенства права, основоположних прав і свобод людини і громадянина, демократичних цінностей, а також забезпечення відповідних гарантій під час використання таких технологій;

– відповідність діяльності та алгоритму рішень систем штучного інтелекту вимогам законодавства про захист персональних даних, а також додержання конституційного права кожного на невтручання в особисте і сімейне життя у зв'язку з обробкою персональних даних;

– забезпечення правового регулювання штучного інтелекту (в тому числі у сферах освіти, економіки, публічного управління, кібербезпеки, оборони, боротьби зі злочинністю, у судочинстві);

– розширення меж доступу до великих масивів інформації у цифровому вигляді, допомога в її аналізі і прийнятті процесуальних рішень;

– застосування технологій штучного інтелекту в судовій практиці.

Основним завданням державної політики у сфері правового регулювання галузі штучного інтелекту в Концепції проголошено захист прав та свобод учасників відносин у галузі штучного інтелекту, розроблення та використання технологій штучного інтелекту з дотриманням етичних стандартів. Оскільки з 23 червня 2022 р. Україна набула статусу країни-кандидата на вступ до Європейського Союзу, ці завдання треба виконувати шляхом імплементації норм, закріплених у «Рекомендаціях щодо штучного інтелекту», що прийняті у червні 2019 року Організацією економічного співробітництва та розвитку (OECD/LEGAL/0449), за умови дотримання етичних стандартів, передбачених в Рекомендаціях CM/Rec(2020)1, схвалених 8 квітня 2020 р. Комітетом міністрів Ради Європи для держав-членів щодо впливу алгоритмічних систем на права людини, у законодавство України [7].

У 2018 р. Європейська комісія з питань ефективності правосуддя прийняла «Етичну хартію про використання штучного інтелекту в судових системах та їх середовищі» [8], яка закріплює принципи використання систем ШІ під час здійснення правосуддя, а саме:

– дотримання основних прав людини при використанні ШІ;

– запобігання будь-якої дискримінації між окремими особами чи групами осіб;

– якість та безпека при обробленні судових рішень і даних, які мають міститися у безпечному технологічному середовищі;

– прозорість, неупередженість та справедливість.

На жаль, в «Плані заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки» не містяться конкретні заходи

щодо законодавчого регулювання процесів використання ШІ у боротьбі зі злочинністю, а заплановано лише «запровадження правового регулювання з питань формування державної політики у галузі штучного інтелекту» та «впровадження технологій штучного інтелекту в національну систему кібербезпеки». [9]. Однак, на сьогодні питання законодавчого врегулювання процесів використання систем ШІ у боротьбі зі злочинністю є вкрай актуальними, зокрема, у протидії суспільно небезпечним явищам та розслідуванні кримінальних правопорушень шляхом аналізу наявних даних і допомоги у прийняття процесуальних рішень за умови дотримання етичних стандартів.

Список використаної літератури:

1. John McCarthy, «What is Artificial Intelligence». Society for the Study of Artificial Intelligence and Simulation of Behavior, Computer Science Department, Stanford University, 2007. http://jmc.stanford.edu/articles/whatisai/whatisai.pdf
2. Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції // Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 6–10. С. 6.
3. Russia's war crimes. URL: https://war.ukraine.ua/russia-war-crimes/
4. Більш детально див.: Бодняк О. Війна і роботи. URL: https://zaxid.net/statti_tag50974/
5. Джеймс Клейтон. Як штучний інтелект допомагає ідентифікувати загиблих в Україні. BBC News Україна. URL: https://www.bbc.com/ukrainian/features-61105661
6. Christopher Rigano, «Using Artificial Intelligence to Address Criminal Justice Needs», October 8, 2018, nij.ojp.gov: https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs
7. Концепція розвитку штучного інтелекту в Україні. Схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. №1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556–2020-%D1%80#Text
8. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: https://rm.coe.int/ethical-charter-en-forpublication-4-december-2018/16808f699c
9. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки. Затверджено розпорядженням Кабінету Міністрів України від 12 травня 2021 р. №438-р. URL: https://zakon.rada.gov.ua/laws/show/438–2021-%D1%80#n10

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВОСУДДІ : ВИКЛИКИ ТА СТАНДАРТИ РАДИ ЄВРОПИ

Ахтирська Наталія Миколаївна,
кандидат юридичних наук, доцент, доцент кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка

Математик Ірвінг Джон Гут під час Другої світової війни був головним статистиком у Тюрінговій команді зі зламу шифрів, який став першим, хто передбачив позитивні наслідки та загрози створення штучного інтелекту, застерігши про те, що ультрарозумна машина, яка перевершує в інтелектуальній діяльності найрозумнішу людину, зможе створювати ще розумніші машини; а тоді, поза сумнівом, відбудеться «вибух інтелекту», і людський розум залишиться далеко позаду. Тому перша ультрарозумна машина стане останнім винаходом людини – але тільки в тому разі, якщо машина виявиться слухняною і навчить нас керувати собою[1, 16].

Ігровий штучний інтелект в 1952 році перевершив людину у *шашках*, в 1979 році – у *нардах*, в 1982 році – *Traveller TCS*, в 1997 році – в *шахах*, в 2012 році досягнуто дуже сильного рівня гри в *го*, наразі у 2022 році досягнуто рівня людини. Конвергенція між нанотехнологіями, біотехнологіями, інформаційними технологіями та когнітивними науками та швидкість, з якою нові технології надходять на ринок мають наслідки не лише для прав людини та способів їх реалізації, а й для фундаментального поняття про те, що характеризує людину. Поширення нових технологій та їх застосування стирає межі між людиною та машиною, між діяльністю он-лайн та оф-лайн, між фізичним та віртуальним світом, між природним і штучним, між реальністю і віртуальністю. Людство нарощує свої здібності, підвищуючи їх за допомогою машин, роботів і програмного забезпечення. Сьогодні є можливість створити мозок – комп'ютер, те, що є «доповненою» людиною.

Наразі існують широкі можливості застосування штучного інтелекту. Можливості систем розпізнавання обличчя використовуються в автоматизованих пунктах перетину кордону в Європі та Австралії. Державний департамент США для видачі віз використовує систему розпізнавання

обличчя з базою даних, що налічує більше ніж 75 млн. фотозображень. Системи спостереження використовують складні алгоритми штучного інтелекту та технології виявлення інформації в даних (data-mining) для аналізу великих обсягів голосових повідомлень, відео-потоків, текстів, перехоплених із комунікаційних каналів і збережених у гігантських дата-центрах.

Парламентська асамблея Ради Європи із занепокоєнням відзначила, що законодавцям стає дедалі важче адаптуватися до швидкості, з якою розвиваються наука і технології, які потребують розробки необхідних правил і стандартів. Захист людської гідності в XXI столітті передбачає розвиток нових законодавчих механізмів та встановлення міжнародного співробітництва, яке сприятиме вирішенню нових викликів найбільш ефективно. Вплив штучного інтелекту на права людини є одним із найважливіших факторів, які визначатимуть період, у якому ми живемо, а тому встановлення правильного балансу між технологічним розвитком і захистом прав людини є терміновою справою.

Наразі немає узгодженого визначення «штучного інтелекту», однак в Рекомендації 2102 (2017) використовується загальний термін «як набір наук, теорій і методів, направлених на покращення здатності машин робити речі, які вимагають інтелекту». Система штучного інтелекту – це машинна система, яка дає рекомендації, передбачення або рішення для заданого набору цілей. Це робиться шляхом: (i) використання вхідних даних від машини та/або людини для сприйняття реального та/або віртуального середовища; (ii) абстрагування такого сприйняття в моделі вручну або автоматично; і (iii) отримання результатів з цих моделей, будь то шляхом людськими або автоматизованими засобами, у вигляді рекомендацій, прогнозів або рішення [2].

В Європейській етичній хартії про використання штучного інтелекту в судовій системі визначено п'ять основних принципів: 1) принцип поваги до основних прав покликаний забезпечити сумісність впровадження інструментів і послуг штучного інтелекту з основними правами людини; 2) принцип недискримінації, запобігання розвитку або посилення будь-якої дискримінації між окремими особами чи групами; 3) принцип якості та безпеки стосовно обробки судових рішень та даних, використання сертифікованих джерел; 4) принцип прозорості, неупередженості та справедливості; 5) принцип «під контролем користувача», що означає виключення директивного підходу і забезпечення поінформованості

учасників щодо застосування під час ухвалення судових рішень штучного інтелекту та надання їм права вибору. Наразі відбувається розробка та введення в дію принципів Хартії щодо використання штучного інтелекту в судових системах та вивчення можливостей сертифікації інструментів та послуг штучного інтелекту, а також узгоджуються інструменти щодо меж та гарантій державам-членам та іншим спеціалістам в галузі правосуддя, які бажають створити або використовувати механізми штучного інтелекту в судових системах для підвищення ефективності та якості правосуддя; в 2023 році планується запуск «Ресурсного центру по кіберправосуддю та штучному інтелекту», в якому буде наданий огляд систем штучного інтелекту, які використовуються під час здійснення правосуддя.

Спеціальний комітет Ради Європи по штучному інтелекту (CAHAI) 12 березня 2021 року надав підсумковий документ дослідження «Можливі елементи правової бази щодо штучного інтелекту на основі стандартів Ради Європи в галузі прав людини, демократії та верховенства права», що стало предметом розгляду першого засідання Консультативної ради CEPEJ з питань штучного інтелекту, метою якого є моніторинг застосування штучного інтелекту в системі правосуддя та відповідне консультування робочих груп (12 вересня 2022 року). Рада Європи застерегла, що використання штучного інтелекту може мати певні негативні наслідки (про що свідчать попередні дані): дискримінація (наприклад, що афроамериканці мають більший ризик рецидиву); «упередження міркувань» програмного забезпечення може призвести до аномальних або невідповідних результатів через плутанину між простими лексичними випадками судових доказів і причинно-наслідковими зв'язками, які були вирішальними в міркуваннях суддів.

Усі європейські суди різною мірою стикаються з повторюваними цивільними справами малої вартості. Досить поширена ідея полегшити процедуру за допомогою інформаційних технологій та/або аутсорсингу судів. Великобританія, Нідерланди та Латвія є прикладами країн, які мають вже реалізовані або збираються впровадити ці типи ухвалення автоматизованих рішень. Для транскордонних позовів Європейський Союз встановив за допомогою Регламенту № 524/2013 загальну структуру, яка доступна на Інтернет-сервісі (європейські дрібні позови). Однак обсяг цих послуг онлайн-розв'язання суперечок поступово розширюється. Вони перестали бути обмеженими щодо альтернативних заходів ви-

рішення спорів, а також стосуються не лише спорів невеликої вартості, а й податкових спорів, спорів, пов'язаних із послугами соціального забезпечення, або шлюборозлучних процесів.

Вирішення спорів он-лайн, як спосіб альтернативного вирішення спорів, вимагає обов'язкового роз'яснення учасникам, що на платформі он-лайн їхній спір розглядається повністю автоматизованим способом, щоб дозволити сторонам зробити усвідомлений вибір, можливо, не погодившись з порадою та вирішивши звернутися до справжнього суду за змістом статті 6 ЄКПЛ.

В кримінальному судочинстві штучний інтелект використовується для запобігання правопорушенням, прогнозування ризику рецидиву та оцінки рівня небезпеки. Водночас, використання статистики та штучного інтелекту в кримінальному провадженні показало ризик спровокувати відродження детерміністської доктрини на шкоду доктринам індивідуалізації санкцій**.** Так, у Сполучених Штатах було виявлено дискримінаційні ефекти алгоритму, який використовується в програмному забезпеченні COMPAS (Correctional Offender – профілювання менеджменту для альтернативних санкцій), метою якого є оцінка ризику рецидиву, коли суддя повинен визначити покарання. Цей алгоритм, який був розроблений приватною компанією і який мають використовувати судді в деяких американських федеральних штатах, включає різноманітні запитання, на які відповідав обвинувачений, або отримана інформація з інших інформаційних джерел, та включає наявність телефона вдома, труднощі з оплатою рахунків, сімейну історію, кримінальну історію тощо. Алгоритм оцінює особу за шкалою від 1 (низька ризик) до 10 (високий ризик). Водночас, цей тип алгоритму не працює ефективно, оскільки люди без будь-якої кримінальної історії можуть відтворити точно таку саму оцінку, просто відповівши на запитання анкети (наприклад, невчасна сплата рахунків).

У випадку наявної законодавчої можливості, коли суддя, скориставшись штучним інтелектом для ухвалення рішення, може не погодитись з ним та ухвалити власне, що ймовірно зумовить негативні наслідки. Суддя, який прийме рішення проти передбачення алгоритму, ймовірно йде на ризик, оскільки він бере на себе більшу відповідальність (підозру в упередженості тощо). Навіть, якщо штучний інтелект не врахував всі фактори, судді не захочуть взяти на себе цей додатковий тягар, особливо в тих країнах, де їхні законні гарантії в дисциплінарних питаннях є недостатніми.

Список використаної літератури:

1. Nick Bostrom. Super Intelligence. Paths, Dangers, Strategies. Oxford University Press. Oxford.2014. P. 16.

2. Recommendation 2102 (2017) Technological convergence, artificial intelligence and human rights. https://www.coe.int/en/web/artificial-intelligence/work-in-progress#05EN

3. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ І ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ПРАВОСУДДЯ В УМОВАХ ВОЄННОГО СТАНУ

Барабаш Анастасія Анатоліївна,
молодший науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Впровадження цифрових технологій в судочинство є загальною тенденцією розвитку інформаційного суспільства. Сучасні цифрові технології завдяки широкому застосуванню змінюють характер взаємовідносин у суспільстві, дозволяють членам суспільства перебувати в постійній комунікації один з одним, і стала причиною глобальних модифікацій соціальних і правових інститутів, зокрема і в організації та порядку здійснення правосуддя.

Застосування цифрових технологій при забезпеченні доступу до правосуддя є важливим інструментом модернізації судової системи та елементом електронного врядування. Згідно Рекомендацій Rec (2001) 2 Комітету Міністрів Ради Європи державам-членам *щодо побудови та перебудови судових систем та правової інформації*, сучасні інформаційні технології стали незамінним засобом у сфері здійснення правосуддя і таким чином вони сприяють ефективному управлінню державою, яке необхідне для нормального функціонування демократії [1]. Основні стандарти щодо електронного правосуддя в Європі були передбачені вже у наступних документах: Рекомендаціях (95) 11 Комітету міністрів Ради Європи державам-членам стосовно відбору, оброблення, подання та архівації судових рішень у правових інформаційно-пошукових системах; Рекомендаціях (2001) 3 Комітету міністрів ради Європи державам-членам щодо надання судових та інших юридичних послуг громадянам з використанням новітніх технологій; Рекомендаціях (2003) 15 Комітету міністрів ради Європи державам-членам про архівування електронних документів у правовій сфері та ін.

Щодо впровадження європейських стандартів електронного правосуддя в національну судову систему, слід зазначити, що Україна однією з перших країн-партнерів ЄС, імплементувала положення та засади

Європейського кодексу електронних комунікацій шляхом ухвалення 30 вересня 2020 року Закону України «Про електронні комунікації».

1 грудня 2018 року в газеті «Голос України» та на офіційному вебпорталі «Судова влада України» Державна судова адміністрація України оголосила про створення та забезпечення функціонування Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС) [2]. ЄСІТС побудовано на основі хмарних технологій, що забезпечують опрацювання та зберігання даних віддалено та надають доступ користувачам Інтернету до програмного забезпечення та обчислювальних ресурсів. Спеціальне програмне забезпечення розроблено також для проведення судових засідань поза судами [3, с. 143]. А 5 жовтня 2021 року Вища рада правосуддя оголосила про початок функціонувати трьох підсистем (модулів) ЄСІТС: «Електронний кабінет», «Електронний суд», підсистема відеоконференцзв'язку [4].

Варто зазначити про пілотний проєкт Мінцифри, який передбачає функціонування сучасного судочинства із документами у смартфоні. За допомогою тимчасового QR-коду відбувається перевірка дійсності таких документів, таким чином можна потрапити у будівлю суду. Також використання електронних документів застосовується для ознайомлення із матеріалами справи, для запису на особистий прийом до керівництва або для участі в судових справах. Тестування спрощення доступу до правосуддя за цифровими документами у застосунку Дія розпочалося на базі П'ятого апеляційного адміністративного суду [5].

Однак, на відміну від України, як підкреслює Р. Ханик Посполітак, електронне правосуддя в Європі уже було достатньо поширеним та широко застосовуваним, оскільки це сприяє реалізації принципу доступності правосуддя через спрощення роботи усіх суб'єктів судочинства, пришвидшення строків розгляду спору та усунення транскордонних бар'єрів в межах держав-членів при здійсненні судочинства. Тут є слушною думка Л. Ніколенко, що майбутнє судового процесу за інформаційними технологіями, «спрямованими на реалізацію та дотримання встановлених принципів та стандартів, у тому числі принципу доступності до правосуддя». Хоча звісно, існують певні проблемні моменти, а саме: високий ризик втрати важливої інформації; відсутність повного технічного оснащення судів; забезпечення взаємозв'язку та уніфікації електронного документообігу суду з іншими електронними державними системами тощо [6, с. 340–341]. У науковій літературі також звертається увага на недо-

сконаліть надання технічної підтримки електронного судочинства, коли технічне забезпечення судів і обслуговування учасників процесів покладено на одного відповідального суб'єкта. Крім цього, необхідне підвищення рівня культури роботи з електронними засобами працівників судів, введення в судову систему електронного діловодства [3, с. 145]

У межах закріпленого права на справедливий суд, Закон України «Про судоустрій і статус суддів» визначає, що доступність правосуддя для кожної особи забезпечується відповідно до Конституції України та в порядку, встановленому законами України [7]. Разом із цим вона може виявитись обмеженою, у зв'язку із загрозою їх життю чи безпеці під час пересування або навіть просто через віддаленість розташування суду.

Погоджуючись із висновком М. Смокович, за умови дії правового режиму воєнного стану, територію України умовно можна поділити на територіальні зони, де: а) ведуться активні бойові дії або велися такі дії; б) триває тимчасова чи стійка окупація українських територій; в) є необхідні матеріальні умови та фізичні можливості для роботи суду (приміщення, комп'ютерна техніка, електрика, інтернет та ін.), або таких умов і можливостей немає і т.д. [8, с. 452–453].

Тут слід відзначити рішення Верховного Суду щодо особливостей здійснення правосуддя на території, на якій введено воєнний стан. Надано можливість учасникам судових процесів подати заяву про відкладення розгляду справ у зв'язку з воєнними діями та/або про розгляд справ у режимі відеоконференції за допомогою будь-яких технічних засобів, зокрема й власних [9].

Сам Верховний Суд, поряд із звичним прийомом кореспонденції, у разі технічної можливості, приймання документів може здійснюватися з використанням підсистеми «Електронний суд» або ж в електронному вигляді на електронні адреси Верховного Суду [10].

Використання електронних технологій у судовій системі сприяє більш ефективній судовій діяльності, спрощує обмін інформацією між судами, учасниками процесу, особливо в умовах воєнного стану. Перехід на електронне правосуддя, безумовно, полегшить доступ до правосуддя, а також зробить його більш прозорим та доступним.

Список використаної літератури:

1. Рекомендація Rec (2001) 2 Комітету Міністрів Ради Європи державам-членам щодо побудови та перебудови судових систем та правової

інформації в економічний спосіб: ухв. Комітетом Міністрів Ради Європи на 743 засіданні заступників міністрів 28 лютого 2001 року. URL: https://www. viaduk. net/clients/vsu/vsu. nsf/6b6c1e2e6ad3e2fcc225745c0034f4cc/7442a47eb0b374b9c2257d8700495f8b/$FILE/%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D1%96%D1%8F%20Rec%20 (2001) %202. pdf (дата звернення: 09.12.2022)
2. Про затвердження Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи: Вища рада правосуддя; Рішення від 17.08.2021 № 1845/0/15–21. URL: https://zakon.rada.gov.ua/rada/show/v1845910-21#Text (дата звернення: 09.12.2022)
3. Олійничук О., Олійничук Р., Колесніков А. Електронне правосуддя як елемент сучасної системи судочинства. Актуальні проблеми правознавства. № 3 (27). 2021. С. 141–147
4. Оголошення Вищої ради правосуддя від 4 вересня 2021 р. Газета «Голос України». № 168 (7668). 2021.
5. Прес-офіс Міністерства та Комітету цифрової трансформації. Доступ до П'ятого апеляційного адміністративного суду за цифровими документами у Дії. Міністерство та Комітет цифрової трансформації України URL: https://thedigital.gov.ua/news/dostup-do-pyatogoapelyatsiynogo-administrativnogo-sudu-za-tsifrovimi-dokumentami-udii?fbclid=IwAR0N5q_U8Q-OwS39ndKXXH41JPcxqKqgXuZYHITkTKdl 7c8fgzJAd0EZOmE
6. Ніколенко Л. М. Електронне правосуддя як спосіб підвищення ефективності судового розгляду. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 71. 2022. С. 338–341
7. Про судоустрій і статус суддів: Закон України від 02.06.2016 № 1402-VIII. URL: https://zakon.rada.gov.ua/laws/show/1402–19#Text (дата звернення: 17.12.2022)
8. Смокович М. І. Здійснення правосуддя в умовах воєнного стану: до питання законодавчих змін. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 70. 2022. С. 450–455.
9. Особливості здійснення правосуддя на території, на якій введено воєнний стан. Веб-портал: Верховний Суд. Судова влада України. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1261727/ (дата звернення: 17.12.2022)
10. Порядок прийому документів. Веб-портал: Верховний Суд. Судова влада України. URL: https://supreme.court.gov.ua/supreme/ gromadyanam/por_priyom/ (дата звернення: 17.12.2022)

ЦИФРОВА ІНФОРМАЦІЯ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ В УМОВАХ ВОЄННОГО СТАНУ

Булулуков Олег Юрійович,
кандидат юридичних наук, доцент кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого

Коновалова Віолетта Омелянівна
доктор юридичних наук, професор, академік НАПрН України,
старший науковий співробітник
НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Розслідування кримінальних правопорушень в умовах воєнного стану сприяло виникненню низки питань, пов'язаних із здійсненням кримінального провадження та формуванням доказової бази обвинувачення. У зв'язку з цим до розділу IX[1] КПК України були внесені зміни щодо особливого режиму досудового розслідування та судового розгляду в умовах воєнного стану. Сутністю змісту положень розділу IX[1] КПК України є збільшення можливостей уповноваженої службової особи щодо виконання окремих процесуальних дій. Зазначене розширення поширюється на ситуації розслідування, коли об'єктивно неможливо дотримуватися звичайних для певної ситуації положень процесуального Закону, виходячи із складнощів, що виникають під час воєнного стану. У всіх інших випадках уповноважена службова особа повинна діяти відповідно до положень КПК України, які передбачають типовий порядок досудового розслідування та судового розгляду кримінального провадження. Внесені зміни спрямовані на прискорення процесу розслідування, а в подальшому – і судового розгляду. Зрозуміло, що швидкість та повнота розслідування кримінального правопорушення залишилася пріоритетною метою зазначеного розділу і на це вказують передбачені зміни строків і процедури досудового розслідування. Загально відомо, що послідовність дотримування процесуального Закону при розкритті та розслідуванні кримінального правопорушення сприяє об'єктивності в розслідуванні та відновленню порушених прав і законних інтересів особи. Вказана мета досягається шляхом введення особливого режиму досудового розслідування, що передбачений у розділі IX[1] КПК України.

Розширення повноважень окремих осіб водночас сприяє виникненню ризиків щодо забезпечення належним чином процесуальних гарантій «прав, свобод та законних інтересів учасників кримінального провадження» [1]. Йдеться про регламентацію здійснення окремих процесуальних дій поза судовим контролем.

Зміни, внесені до КПК України протягом березня – листопада 2022 р., дозволяють стверджувати про певну трансформацію досудового розслідування. Вказана трансформація, що відбулася у зв'язку з військовою агресією Росії проти України і введенням на всій території України воєнного стану сприяла оптимізації досудового розслідування та забезпеченню функціювання системи кримінального судочинства.

Важлива роль у кримінальному судочинстві в умовах воєнного стану належить доказам, що можуть бути отримані при проведенні слідчих (розшукових) дій під час досудового розслідування. Як з'ясувалося, одним із важливих видів доказів вчинення військових злочинів є цифрова інформація (цифрові докази), отримана з різних джерел і у різний спосіб.

Цифрова інформація охоплює різні сфери життя людини і є відображенням її поведінки, її відносин з іншими людьми, її захоплень та ін. Наявність смартфонів, комп'ютерів, планшетів і інших електронних пристроїв дозволяє людині використовувати цифрову інформацію для власних потреб. При використанні цифрової інформації остання має властивість відображуватися на різних електронних носіях та зберігатися на них досить тривалий термін часу. У разі необхідності зазначена інформація може бути встановлена та використана для доказування окремих фактів у кримінальному проваджені. Цілком природньо, що можливість отримання такої інформації зацікавила органи, що ведуть боротьбу зі злочинністю. І поступово «аналітична робота з такими джерелами еволюціонувала від епізодичного використання до своєрідної моделі інформаційно-цифрового розслідування події через відкриті джерела у кіберпросторі» [2, с. 37]. Інформація, що виявляється у такий спосіб визначається як «цифровий слід», що може бути використаний у кримінальному проваджені. Проте на сьогоднішній день (у зв'язку із відсутністю визначення у КПК України – розрядка наша. О. Б., В. К.) серед вчених, що досліджують злочини, які вчиняються із використанням різних електронних пристроїв точаться дискусії як щодо назви таких слідів так і їх сутності [3, с. 91]. В зв'язку з тим, що основою зазначених слідів є цифрова інформація, цілком логічно називати їх «цифровими слідами».

У кримінальних провадженнях використання цифрової інформації в доказуванні вчинення певною особою кримінального правопорушення стає все більш звичайною справою. Розвиток цифрової криміналістики сприяв тому, що цифрова інформація і цифрові сліди у кримінальному процесі використовуються у системі доказів. Процес входження зазначених доказів у кримінальне судочинство є поступовим і це зрозуміло. Кожна новація у процесі досудового розслідування повинна пройти наукову аргументацію із посиланням на окремі ситуації, окремі приклади із практики розслідування та судового розгляду. У теперішній час поняття «цифрові докази» досліджуються вченими-процесуалістами на предмет відповідності їх критеріям: «достовірності, правдивості, надійності, релевантності, переконливості, належності та допустимості» [2, с. 37]. Окрім цього, здійснюються пошуки «шляхів алгоритмізації, оптимізації та автоматизації роботи з відкритими джерелами даних. Основними кроками такої діяльності є: Крок 1. Ідентифікація джерел (визначення яку інформацію ми потребуємо, де і як її знайти). Крок 2. Колекціонування даних (збір даних самостійно або за допомогою спеціальних програм). Крок 3. Обробка даних (систематизація та фільтрація інформації, яка є важливою, яка ні, а яка потребує додаткової верифікації чи уточнення). Крок 4. Аналіз (вивчення та уточнення даних, визначення їх значення для розслідування. Крок 5. Звітність (оформлення даних у вигляді звітних документів, які можна згодом використати залежно від поставлених завдань» [2, с. 38–39). Науковий пошук в напрямку визначення алгоритму роботи з відкритими джерелами цифрової інформації при розслідуванні кримінальних правопорушень є продовженням досліджень Центру з прав людини Юридичної школи Каліфорнійського університету права в Берклі. Результатом зазначених досліджень був Протокол Берклі, документ, у якому в деталізованому вигляді викладені рекомендації щодо збору та використанню цифрової інформації з відкритих джерел [4]. У теперішний час документ використовується «українськими неурядовими громадськими організаціями та журналістами у розслідуванні злочинів, вчинених російськими військовослужбовцями та високопосадовцями на території України» [5]. Вказані розслідування здійснюються паралельно із досудовим розслідуванням та сприяють виявленню фактів кримінальних правопорушень.

Цифрова інформація в кримінальних провадженнях в умовах воєнного стану є важливою для встановлення осіб, що вчинили військові

злочини. Можна назвати типові джерела такої інформації: а) фото та відео з телефонів свідків- громадян України; б) фото та відео із супутників тих що належать Україні і іншим державам; в) фото та відео, отримані неурядовими організаціями що здійснюють незалежне розслідування; г) фото та відео з зарубіжних телевізійних каналів; д) фото, відео та листування з телефонів полонених або вбитих окупантів; е) фото, відео та листування з телефонів окупантів, що були загублені під час відступу; є) фото, відео та листування з комп'ютерів і планшетів окупантів та колаборантів; ж) фото, відео та листування, що є в соціальних мережах; з) записи перехоплених телефонних розмов; и) відео записи виступів окупантів та колаборантів на телевізійних каналах; і) відео записи з камер спостереження в місці перебування окупантів та колаборантів й ін.

Цифрова інформація та цифрові докази в кримінальному процесуальному кодексі України ще не отримали належного правового статусу. Проте досвід Америки та Західної Європи щодо використанні цифрових доказів у кримінальному судочинстві, на нашу думку, буде сприяти прийняттю рішення щодо визначення їх статусу в національному кримінальному процесуальному законодавстві.

Список використаної літератури:

1. Кримінальний процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text
2. Дуфенюк О. Використання відкритих джерел цифрової інформації під час розслідування злочинів. *Інформація та документ у сучасному науковому дискурсі:* матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.). Івано-Франківськ: ІФНТУНГ, 2022. С. 37–41.
3. Авдєєва Г. К. Сутність цифрових слідів в криміналістиці. *Актуальні питання судової експертизи та криміналістики* : зб. матеріалів міжнар. наук.-практ. конфер., присвяч. 95-річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). Харків, 2018. С. 90–93.
4. Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf
5. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? URL : https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОБШУКУ В УМОВАХ ВОЄННОГО СТАНУ

Гомоляко Влада Євгеніївна,
аспірант відділу дослідження проблем кримінального процесу та судоустрою НДІ ВПЗ ім. акад. В. В. Сташиса НАПр України

Збройна агресія Російської Федерації проти України, яка набула повномасштабного характеру 24.02.2022 р. призвела до ряду викликів для здійснення досудового розслідування та відправлення правосуддя на території України. Ведення активних бойових дій у певних регіонах України та відсутність у працівників правоохоронних органів об'єктивної можливості доступу до територій, де були вчинені злочини, зумовлюють ряд проблем ще на етапі досудового розслідування, а саме: виявлення та своєчасне внесення відомостей про вчинене кримінальне правопорушення до Єдиного реєстру досудових розслідувань; особливості проведення окремих слідчих дій; обрання, продовження, зміну чи скасування запобіжного заходу тощо.

У зв'язку з цим, Законом України № 2201-IX від 14.04.2022, а також іншими законами, зокрема № 2108-IX від 03.03.2022, № 2110-IX від 3.03.2022, № 2111-IX від 3.03.2022, № 2125-IX від 15.03.2022, № 2137-IX від 15.03.2022, № 2160-IX від 24.03.2022, № 2198-IX від 14.04.2022, було внесено ряд змін в кримінальне процесуальне законодавство, які встановили деякі особливості здійснення досудового розслідування, судового розгляду в умовах воєнного стану. Але у зв'язку із нагальною потребою оперативно вирішити окремі питання, їх нормативне регулювання частогусто не відповідає стандартам якості закону. Це в свою чергу призводить до виникнення проблем на практиці, наприклад: зловживання своїми повноваженнями працівниками правоохоронних органів під час прийняття рішення про проведення обшуку та в процесі реалізації такої процесуальної дії, як наслідок порушення конституційних прав осіб, залучених до кримінальних процесуальних відносин. У зв'язку з цим, розгляд цього питання є вельми актуальним.

Безпосередні зміни кримінального процесуального законодавства торкнулися ст. 615 КПК України, яка присвячена особливому режиму кримінального провадження в умовах воєнного стану. В указаній нормі було врегульовано ряд питань, зокрема:

– вирішено питання щодо початку кримінального провадження за неможливості доступу до Єдиного реєстру досудових розслідувань;

– регламентовано особливість прийняття певних процесуальних рішень за об'єктивної неможливості виконання слідчим суддею своїх повноважень;

– врегульовано порядок перебігу строків у кримінальному провадженні та порядок їх продовження, зупинення і поновлення тощо.

Як бачимо, більшість змін стосуються саме стадії досудового розслідування, що є цілком логічним, адже більшість складнощів у правозастосовній практиці виникає саме під час розслідування кримінальних правопорушень. Водночас спосіб унормування окремих питань здійснення досудового розслідування в умовах воєнного стану створив підґрунтя для можливого зловживання своїми повноваженнями стороною обвинувачення.

Одним з таких питань є проведення обшуку під час досудового розслідування кримінального правопорушення в умовах воєнного стану. Характерною особливістю обшуку є те, що під час здійснення цієї слідчої розшукової дії відбувається проникнення до житла чи іншого володіння особи. Відповідно до ч. 1 ст. 233 КПК України ніхто не має права проникнути до житла чи іншого володіння особи з будь-якою метою, інакше як лише за добровільною згодою особи, яка ними володіє, або на підставі ухвали слідчого судді, крім невідкладних випадків, пов'язаних із врятуванням життя людей чи майна чи з безпосереднім переслідуванням осіб, які підозрюються у вчинення кримінального правопорушення.

Отже, враховуючи положення зазначених статей, слідчий суддя уповноважений надати дозвіл на проведення такої слідчої дії, або легалізувати проведення обшуку в невідкладних випадках. Однак, відповідно до п. 2 ч. 1 ст. 615 КПК України якщо відсутня об'єктивна можливість виконання слідчим суддею повноважень, передбачених в тому числі статтею 233 КПК України – такі повноваження виконує керівник відповідного органу прокуратури за клопотанням прокурора або за клопотанням слідчого, погодженим з прокурором. Таким чином, першою особливістю здійснення обшуку під час воєнного стану є те, що рішення про його проведення може прийняти керівник відповідного органу прокуратури.

Однак, головною умовою для проведення обшуку за рішенням керівника органу прокуратури є об'єктивна неможливість виконання слідчим

суддею своїх повноважень. На практиці це викликає значну кількість зловживань, оскільки норма закону не надає перелік випадків, у яких слідчий суддя не може виконувати свої повноваження. Це є оціночним поняттям, а відтак прокурор на власний розсуд буде визначати можливість/неможливість слідчим суддею відправляти правосуддя, перебираючи на себе його повноваження. У цьому випадку нівелюється функція судового контролю за дотриманням прав і свобод людини і громадянина під час досудового рпозслідування.

На практиці вже спостерігаються непоодинокі випадки, коли прокурори, не звертаючись до слідчого судді, самостійно приймали рішення про проведення обшуку, навіть на тих територіях, де не велися активні бойові дії і слідчі судді у повному обсязі виконували свої повноваження. Деякі практикуючі юристи висловлюють думку про те, що *логічною була б конструкція цієї норми про те, що така неможливість виконання слідчим суддею своїх повноважень має підтверджуватись офіційним оголошенням на веб-порталі суду (яке долучається до матеріалів кримінального провадження) та не визначення Верховним Судом іншого суду, який здійснюватиме судочинство на певній території (курсив наш – В. Г.)* [2].

Крім того, ч. 7 ст. 223 КПК України встановлює, що обшук здійснюється з обов'язковою участю не менше двох понятих незалежно від застосування технічних засобів фіксування відповідної слідчої (розшукової) дії, крім особливостей, встановлених статтею 615 цього Кодексу. Недарма вказана норма робить відсилку до ст. 615 КПК України, оскільки в ній зазначається, що якщо залучення понятих є об'єктивно неможливим або пов'язано з потенційною небезпекою для їхнього життя чи здоров'я, відповідні слідчі (розшукові) дії проводяться без залучення понятих. У такому разі хід і результати проведення обшуку або огляду житла чи іншого володіння особи, обшуку особи в обов'язковому порядку фіксуються доступними технічними засобами шляхом здійснення безперервного відеозапису. При цьому знову ж таки актуальним залишається питання зловживання своїми повноваженнями працівниками правоохоронних органів. Очевидно, що неможливо залучити понятих на тих територіях, де ведуться активні бойові дії або на територіях, які є прифронтовими. Однак поняття «потенційна небезпека» є оціночним, в сучасних реаліях можна сказати, що по суті на всій території України є потенційна небезпека для життя та здоров'я осіб. Відтак, проведення

обшуку без понятих є ще однією особливістю вказаної слідчої розшукової дії і потенційним джерелом зловживань працівників правоохоронних органів.

Хід і результати виконання обшуку обов'язково фіксуються у протоколі, що складається слідчим або прокурором, які проводять відповідну процесуальну дію, під час її проведення або безпосередньо після закінчення. Однак, знову ж таки, звертаючись до п. 1 ч. 1 ст. 615 КПК України, ми бачимо певні особливості. Зокрема, за відсутності можливості складання процесуальних документів про хід і результати проведення слідчих (розшукових) дій чи інших процесуальних дій фіксація здійснюється доступними технічними засобами з подальшим складенням відповідного протоколу не пізніше сімдесяти двох годин з моменту завершення таких слідчих (розшукових) дій чи відповідних процесуальних дій. Таким чином, законодавець дає можливість процесуально оформити проведення обшуку не одразу, а протягом 72 годин по його завершенню.

У такому випадку виникає ряд логічних запитань: як потрібно діяти, якщо в осіб, які брали участь у проведенні обшуку, відсутня можливість прибути для його підписання або вони свідомо відмовляються прибути, і яку відповідальність вони понесуть у разі неявки.

Ці питання наразі залишаються відкритими.

Отже, можна виокремити такі особливості проведення обшуку в умовах воєнного стану: по-перше, рішення про його проведення за певних умов може прийняти керівник відповідного органу прокуратури; по-друге, така слідча дія в певних випадках може проводитися за відсутності понятих; по-третє, протокол про проведення обшуку може складатися протягом 72 годин після його закінчення. Однак, на практиці вказані особливості можуть викликати ряд зловживань з боку правоохоронних органів, що свідчить про недосконалість певних законодавчих положень і необхідність вдосконалення чинного кримінального процесуального законодавства.

Список використаної літератури:

1. Під час воєнного стану в Україні дозволили проводити обшуки вночі й без понятих й затримувати на 9 днів. *Інтернет-видання Полтавщина.* 2022. URL : https://poltava.to/news/66023/ (дата звернення: 16.12.2022).

МОЖЛИВОСТІ ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ ДЛЯ ЗАПОБІГАННЯ ТА РОЗКРИТТЯ КРИМІНАЛЬНО ПРОТИПРАВНИХ ПОРУШЕНЬ ПРАВИЛ ДОРОЖНЬОГО РУХУ

Данильченко Юрій Броніславович,
доктор юридичних наук, доцент, старший науковий співробітник відділу кримінологічних досліджень НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Тенденції цифровізації суспільного життя – невід'ємний атрибут епохи Постмодерну. Кожна сучасна і більш-менш соціально активна людина має свої віртуальні аватари у діджитал-просторі. Мережева техніка і технології міцно увійшли у повсякденність, сформувавши додаткові виміри реальності. В них, в цих вимірах, формуються мотивації, задовольняються потреби, розгортаються багатоповерхові симулякри. Відтак і сучасна гуманітарна наука не може не використовувати ці простори і об'єкти для досліджень як самої особистості, її внутрішніх світів, так і інструментів впливу на них. Не є виключенням і сфера протидії кримінально протиправним порушенням правил дорожнього руху. Цілком зрозуміло, що ця сфера є вельми широкою, а її дослідженню присвячена чимала кількість наукових праць. Тому, виносячи за дужки опис наявних досягнень, акцентуймо увагу лише на деяких напрямах використання цифрової інформації для запобігання та розкриття кримінально протиправних порушень правил дорожнього руху.

1. Активізація, розширення масштабів використання камер фотовідеофіксації порушень правил дорожнього руху. При всій очевидності затребуваності цього кроку змушені констатувати явну недостатність присутності таких камер на автошляхах, мізерні площі покриття. При тому керівництво Національної поліції звітує, що 6 травня цього року відновили роботу камери фотовідеофіксації, а також вимірювання швидкості за допомогою засобів TruCAM. Й лише за перший місяць роботи обох видів фіксації було винесено 1,5 мільйона постанов про притягнення до відповідальності за перевищення швидкості [1]. Вважаємо, цей напрям роботи одним з пріоритетних.

2. Ситуативне використання безпілотних літальних апаратів з метою фіксації оперативної обстановки на автомобільних шляхах, зокрема

у місцях великої концентрації транспортних засобів, виникнення автомобільних заторів. Основна мета такого використання – фіксація можливих порушень правил дорожнього руху особами, які керують транспортними засобами і потрапили до затору. Перебування в заторах, як відомо, зумовлює наростання тривожності, агресивності водіїв, провокує прийняття рішень на користь вчинення правопорушень для прискорення проїзду відповідної ділянки автошляху (виїзд на смугу зустрічного руху з порушенням встановлених правил, порушень правил, обгону, розвороту тощо), що створює загрозу життю і здоров'ю учасників дорожнього руху.

Як засвідчує практика, добре себе зарекомендували для виконання подібних функцій квадрокоптери DJI Mavic, що вже є в арсеналі Державної прикордонної служби України. Безпілотні літальні апарати дозволяють ефективно проводити повітряну рекогносцировку під час супроводження спеціальних операцій, забезпечують публічну безпеку та порядок, а також допомагають у пошуку зниклих осіб. На думку експертів впровадження новітніх технологій мультиспектрального аналізу і 3D-моделювання значно покращить документування та фіксацію кримінальних правопорушень, й слугуватиме джерелом інформації під час розслідування особливо тяжких злочинів [2, с. 6]. Серед іншого DJI Mavic вже себе добре зарекомендував у справі фіксації дорожньо-транспортних пригод Національною поліцією [3]. Але потенціал його використання саме у превентивних цілях, на наше переконання, ще належить розкрити.

3. Протидія нелегальним перевезенням пасажирів через запровадження системи моніторингу з використанням технологій GPS-тракінгу автомобільних транспортних засобів, що займаються пасажирськими перевезеннями.

4. Удосконалення тактики огляду місця події та роботи поліцейських у складів слідчо-оперативних груп. Перш за все йдеться про необхідність розширення функціоналу таких груп та включення обов'язковим пунктом у їх діяльність виявлення виявлення відоекамер як в зоні безпосередньої дорожньо-транспортної пригоди, так і за напрямами імовірного під'їзду та можливого зникнення транспортного засобу, який брав участь у пригоді. Така діяльність сприятиме розширенню можливостей отримання доступу до відеодоказів кримінального правопорушення, а також встановлення ширшого кола свідків – очевидців кримінального правопорушення.

5. Організація та здійснення радіорозвідки як при первинному огляді місця події, так і на подальших етапах розслідування. Здійснення радіорозвідки передбачає можливість отримання інформації про найближчі до місця події станції стільникового зв'язку. Ця інформація в подальшому використовується для формування запитів до операторів мобільного (стільникового) зв'язку про підключені до базових станцій у визначений проміжок часу пристроїв стільникового зв'язку. Надалі застосовується комплекс оперативно-технічних та/або негласних оперативних (розшукових) заходів для визначення, поступового звуження кола осіб, імовірно причетних до дорожньо-транспортної пригоди, зрештою – ідентифікації конкретної особи за цифровими даними. Як програмне забезпечення для безпосереднього здійснення радіорозвідки використовується застосунок *Netmonitor*.

Окрім зиску від використання радіорозвідки з метою розкриття кримінальних правопорушень, встановлення винних осіб, така діяльність при правильному використання може мати і превентивний ефект. На нашу думку, не лише прикладне використання інструментів радіорозвідки, а й просвітниця діяльність відповідного спрямування здатна сприяти якщо не запобіганню вчиненню кримінально протиправних порушень правил дорожнього руху особами, які керуються транспортними засобами, то зниження тяжкості наслідків таких порушень. Широке інформування населення, зокрема цільове інформування водіїв, про можливості радіорозвідки у розкриття кримінальних правопорушень в межах реалізації концепції *Vision Zero* видається перспективним напрямом спеціально-кримінологічного запобігання. Оскільки кримінальне правопорушення, передбачене ст. 286 КК України є в цілому необережним, то і стадія готування йому не властива. Відтак, попередня робота щодо «радіо-підготовки» (придбання нових апаратів й номерів стільникового зв'язку, без шлейфу мережевої роботи, без прив'язки до мережевих аккаунтів, без контактів і т. д.) цілком закономірно не проводиться, особа залишається у зоні радіо-транспаретності. Таким чином розкриття кримінального правопорушення вчиненого такою особою – справа часу, і вельми незначного. Знання цієї обставини з великою часткою вірогідності здатне схилити особу відмовитись від рішення про втечу з місця події (наприклад, при наїзді на пішохода, вчиненні іншої дорожньо-транспортної пригоди, що потягла за собою середньої тяжкості чи інші, більш тяжкі, тілесні ушкодження). Це своєю чергою сприятиме активізації мотива-

ційного комплексу щодо компенсаторної діяльності, надання допомоги постраждалим, мінімізації завданої шкоди.

Список використаної літератури:

1. Безпека дорожнього руху в Україні: перемоги та нові виклики в умовах війни : огляд експертної дискусії / Центр демократії та верховенства права ; ГО «Асоціація велосипедистів Києва». 15.11.2022. URL: https://cedem.org.ua/news/bezpeka-dorozhnogo-ruhu-v-ukrayini/.
2. Атаманенко Ю. Ю. Сучасний стан і тенденції використання DJI Mavic в Україні // Безпека дорожнього руху в умовах воєнного стану : Матер. Всеукр. наук.-практ. онлайн-конференції (в авторській редакції), (м. Кривий Ріг, 27 травня 2022 року). Кривий Ріг, 2022 С. 6–8
3. Національна поліція отримала понад 30 нових БпЛА. URL: https://defence-ua.com/news/natsionalna_politsija_ponad_30_novih_bpla_foto-2537 (дата звернення: 20.11.2022).

ДО ПИТАННЯ ПРО ЦИФРОВУ ТРАНСФОРМАЦІЮ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Демура Марина Ігорівна,
кандидат юридичний наук, старший викладач кафедри кримінального процесу Національний юридичний університет імені Ярослава Мудрого

У вересні 2019 р. було створено Міністерство цифрової трансформації. Новостворене Міністерство відповідає за формування та реалізацію державної політики у сфері цифровізації, відкритих даних, національних електронних інформаційних ресурсів та інтероперабельності, впровадження електронних та адміністративних послуг, електронних довірчих послуг тощо. Із 2019 р. розпочався активний процес цифровізації усіх сфер суспільного життя України. Не оминув процес цифровізації і галузь кримінального процесуального права.

На початку 2022 р. здавалося, що країна перебуває в стані постійної цифрової трансформації – з'явилося безліч цифрових додатків «Дія», «Дія.Цифрова освіта», «Дія.Бізнес», проєкти «Безпека дітей в Інтернеті», «Е-резидентство», «Дія.City» тощо. Планувалося повне перетворення України на справжню цифрову державу шляхом створення єдиного порталу, де можна отримати всі послуги онлайн швидко, зручно та людяно, та мобільного додатка в якому усі потрібні документи в одному місці. Але 24 лютого повністю змінило ці плани і змусило державу зосередитися на одному – дати військову відсіч ворогу і відновити територіальну цілісність України. Водночас, процеси цифрової трансформації нашої держави в цілому, а також окремих галузей права, в умовах воєнного стану, не зупинилися, а в окремих випадках – навіть пришвидшилися. Не оминули ці процеси і галузь кримінального процесу.

Було прийнято Закони України № 2111-IX від 03.03.2022, № 2137-IX від 15.03.2022, № 2201-IX від 14.04.2022 та багато інших нормативних актів, якими внесено зміни до КПК України.

Враховуючи обмежений обсяг дослідження, пропонуємо зупинитися на окремих нововведеннях до кримінального процесуального законодавства, які були викликані введенням в дію особливого правового режиму – воєнного стану і містять в собі ознаки цифрової трансформації кримінального провадження.

1. Дистанційна участь захисника у проведення процесуальної дії (ч. 12 ст. 615 КПК України).

Аналіз цієї норми дає підстави для наукової дискусії. Так, І. Гловюк звертає увагу, що ч. 12 ст. 615 КПК України щодо можливості дистанційної участі захисника у проведенні окремої процесуальної дії в редакції, що прийнята законодавцем, не забезпечує здійснення ефективного захисту [1, с. 59–60]. На переконання колективу авторів науково-практичного коментаря до Розділу IX-1 КПК України, «має бути врахована думка захисника та його підзахисного щодо можливості здійснення «дистанційного захисту» з огляду на такі конвенційні вимоги як практичність та дієвість (ефективність) професійної правничої допомоги, зокрема в аспекті конфіденційності спілкування з адвокатом». Також науковці звертають увагу, що в ч. 12 ст. 615 КПК України можливість дистанційної участі захисника забезпечується шляхом застосуванням технічних засобів – відео, аудіозв'язку. На їх думку, аудіозв'язок не здатен повною мірою відповідати вимогам статті 6 Конвенції про захист прав людини і основоположних свобод. Доцільно забезпечувати дистанційну участь захисника за необхідності шляхом проведення окремої процесуальної у режимі відеоконференції, яка має фіксуватися за допомогою технічних засобів відеозапису» [2]. Цілком підтримуємо точку зору авторів, звернемо увагу ще на інші моменти. Так, виникає питання «яким чином забезпечити конфіденційне спілкування підозрюваного із захисником перед проведенням процесуальної дії у режимі відеоконференції?». Спілкування перед проведенням процесуальної дії має на меті формування лінії захисту, обрання спільної позиції, надання захисником порад з приводу поведінки, варіантів відповідей під час проведення подальшої процесуальної дії тощо. Отже, конфіденційне спілкування підозрюваного із захисником обов'язково має бути забезпечено дізнавачем, слідчим, прокурором перед проведенням відповідної процесуальної дії з метою гарантування дотримання прав та свобод підозрюваного, а також з метою реалізації гарантій адвокатської діяльності. Нами пропонується норму ч. 12 ст. 615 КПК України доповнити положенням наступного змісту: «Перед проведенням процесуальної дії, дізнавач, слідчий, прокурор зобов'язані забезпечити право підозрюваного вільно і без обмежень у часі спілкуватися із захисником із дотриманням умов, що забезпечують конфіденційність спілкування». Узагальнюючи цитовані положення, висловлені науковцями, а також власні думки, норму щодо дистанційної

участі захисника для проведення процесуальної дії, на наше переконання, можливо реалізувати за таких умов:

– дізнавачем, слідчим, прокурором має бути врахована думка захисника та його підзахисного щодо можливості здійснення «дистанційного захисту»;

– перед проведенням процесуальної дії, дізнавач, слідчий, прокурор зобов'язані забезпечити право підозрюваного вільно і без обмежень у часі спілкуватися із захисником із дотриманням умов, що забезпечують конфіденційність спілкування.

2. Електронна форма постанови слідчого, прокурора (ч. 6 ст. 110 КПК України).

З одного боку, наведена норма є проявом цифровізації кримінального провадження. Вона була прийнята 15.03.2022 р. і залишиться чинною після скасування воєнного стану. З іншого боку, її аналіз викликає цілу низку питань. Зокрема, яким чином уникнути зловживають і пересвідчитися в отриманні учасниками провадження копії постанови. Вбачається, що слідчий, дізнавач, прокурор, має роздрукувати на паперовому носії відповідну постанову і направити її учасникам кримінального провадження засобами поштового зв'язку. Тобто забезпечити виключно електронний документообіг сьогодні вкрай складно.

На наш погляд, питання про електронну форму постанови дізнавача, слідчого, прокурора варто розглядати ширше, зокрема у взаємозв'язку із таким узагальнюючим поняттям як «електронне кримінальне провадження». З цього питання науковці висловлюють точку зору, що нововведення стосовно електронної форми постанови «є важливим законодавчим рішенням у напрямі переведення документування кримінального провадження в електронну форму, що є передумовою розробки електронного кримінального провадження як єдиної платформи взаємодії учасників процесу» [3, с. 35]. Щодо питання про платформу, звернемо увагу науково обґрунтовані пропозиції щодо створення цифрової платформи для взаємодії суб'єктів кримінального провадження. Пропонується в якості одного із напрямків оцифрування кримінального провадження обрати створення цифрової платформи для взаємодії суб'єктів кримінальної процесуальної діяльності, оскільки це дасть змогу забезпечити правовий режим транспарентності кримінального процесу, тобто його прозорості, «відкритості» для учасників кримінального провадження. При цьому одним із напрямків реалізації цієї платформи є створення

єдиного електронного реєстру матеріалів досудового розслідування, що має забезпечити вільний доступ сторін до матеріалів провадження із наступними можливостями: онлайн подання процесуальних документів, обмін документами між учасниками, судами, установами; онлайн доступ до всіх відкритих матеріалів; забезпечення ідентифікації особи у кримінальному провадження за допомогою електронного підпису, за яким можна встановити, що документ в електронній формі підписала саме конкретна особа; обмін повідомленнями онлайн; отримання результатів розгляду клопотань учасниками провадження та інше [4, с. 299].

Повністю підтримуючи висловлені пропозиції, додамо, що в умовах воєнного стану вони набувають додаткової актуальності у зв'язку із тим, що учасники провадження можуть знаходитися в різних регіонах України, або навіть закордоном і для забезпечення їх ефективної участі у кримінальному провадженні, їм має бути надано доступ до матеріалів провадження у будь-який час та у будь-якому місці. Також за допомогою цифрової платформи взаємодії учасників процесу буде забезпечено права сторони кримінального провадження на доступ до процесуальної інформації і ознайомлення з матеріалами провадження і будуть нівельовані ситуації, коли суд вимушений визнати докази недопустимими внаслідок того, що сторона провадження не виконала вимог ст. 290 КПК і не відкрила певний матеріал тощо.

В подальших дослідженнях пропонується дослідити інші питання, що стосуються цифрової трансформації кримінального провадження в умовах воєнного стану, наприклад, щодо збереження копій матеріалів кримінальних проваджень в електронній формі у дізнавача, слідчого чи прокурора.

Список використаної літератури:

1. Головюк І. Питання реалізації конституційного права на професійну правничу допомогу у кримінальному провадженні в умовах воєнного стану. *Конституційні права і свободи людини та громадянина в умовах воєнного стану:* матеріали наукового семінару (2–3 червня 202 2 р.) / упор. М. В. Ковалів, М. Т. Гаврильців, Н. Я. Лепіш. Львів: ЛьвДУВС, 202 2. 315 с., С. 59–60.
2. Головюк І., Дроздов О., Тетерятник Г., Фоміна Т., Рогальська В., Завтур В. Особливий режим досудового розслідування, судового розгляду в умовах воєнного стану: науково-практичний коментар Розділу IX-1

Кримінального процесуального кодексу України. Видання 3. Електронне видання.
3. Глинська Н. В., Клепка Д. І. Цифровізація кримінального провадження: сучасні аспекти концептуалізації (частина 1). *Питання боротьби зі злочинністю.* 2022. № 43. Т. 1. С. 24–42, с. 35. DOI: 10.31359/2079-6242-2022-43-24.
4. Демура М. І., Клепка Д. І., Крицька І. О. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження. *Часопис Київського університету права.* 2020. № 1. С. 295–301, С. 299. DOI: 10.36695/2219–5521.1.2020.59

ЩОДО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ: ДОСВІД ЗАРУБІЖНИХ КРАЇН

Дунаєва Тетяна Євгенівна,
кандидат юридичних наук, науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Розслідування кіберзлочинів – це процес розслідування, аналізу та відновлення даних криміналістичної експертизи для цифрових доказів злочину. Слідчі з кіберзлочинів виконують багато завдань, зокрема визначають природу кіберзлочинів, проводять початкове розслідування, ідентифікують можливі цифрові докази, виконують їх дослідження, захищають цифрові пристрої та докази, а також представляють докази в судовій системі.

Як зазначає В. В. Марков, проаналізувавши досвід роботи поліції багатьох країн світу в сфері протидії кіберзлочинності, слід відзначити, що цей напрямок забезпечується такими основними шляхами, як покладення додаткових функцій на існуючі підрозділи поліції або створення спеціальних підрозділів. Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін. [1, с. 109]. Наприклад, в Індії підрозділи з розслідування кіберзлочинів для їх розкриття можуть залучати професійних хакерів. Під час розслідування кіберзлочинів значну увагу приділяють допомозі постраждалому у відновленні пошкодженої або втраченої інформації, вживають всі необхідні заходи для збереження доказів у справі [1, с. 109; 2, с. 193].

Протидія кіберзлочинності вважаються пріоритетом для забезпечення національної безпеки Франції та здійснюється не лише органами поліції (жандармерії), але й також на рівні Міністерства збройних сил та спеціально створених органів. Штаб із кіберзахисту при Міністерстві збройних сил Франції (COMCYBER), створений для підтримки розвідки, оборони та бойових завдань у кіберпросторі (2017). Співробітники штабу виконують широкий спектр діяльності та різноманітні операційні місії: від аналізу до таких дій, як зміцнення систем, дослідження, моні-

торинг та передбачення загроз, аудит, перевірка вторгнень, нагляд та захист інформаційних систем, виявлення та пошук компромісів, цифрове розслідування та моніторинг у соціальних мережах, участь в операціях та інжиніринг на підтримку операцій. Для виконання своїх місій Штаб із кіберзахисту Франції має штат і повноваження над трьома спільними організаціями: CALID, CASSI і CPROC [3]. Положення Закону про внутрішню безпеку Франції (2003) дозволяють проводити обшуки в інформаційній мережі, якщо інформаційні системи розташовуються на території держави. Шляхом укладення угод у Франції передбачена можливість надання дозволу проводити віддалений обшук інформаційних ресурсів без отримання попереднього дозволу країни, в якій розміщений сервер [4, с. 120].

У Великобританії існують окремі фахівці, які приймають участь у розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Там є інститут консультантів як спеціалізованих фахівців, які вивчають обставини конкретного кримінального провадження, аналізують наявну доказову базу і надають рекомендації слідчим щодо доцільності дослідження конкретних речових доказів, визначення виду експертиз та послідовності їх призначення [5, с. 83].

У США ФБР є основним федеральним правоохоронним органом, який розслідує кіберзлочини в країні та за кордоном. Інші агентства включають Секретну службу США, іммміграційну та митну службу США (ICE), службу поштової інспекції США та Бюро алкоголю, тютюну, вогнепальної зброї та вибухових речовин (ATF). Ці агентства мають місцеві офіси в кожному штаті. Державні та місцеві правоохоронні органи також розслідують кіберзлочини, які вчиняються в їх юрисдикції [6].

У 2013 р. було засновано Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre (ECC) з метою оперативних та інформаційно-аналітичних можливостей взаємодії країн-членів ЄС у боротьбі з кіберзлочинністю, проведення спільних розслідувань проявів кіберзлочинності в Європейському Союзі.

Спільні слідчі групи є одним із найефективніших інструментів для слідчих, які стикаються з проблемою боротьби з кіберзлочинністю. Найефективнішим способом забезпечення тісної співпраці між судовими органами в різних зацікавлених країнах є швидке формування спільної слідчої групи (JIT), найсучаснішого інструменту міжнародного співро-

бітництва у кримінальних справах. JIT – це юридична угода між двома або більше країнами щодо проведення спільних транснаціональних кримінальних розслідувань протягом фіксованого періоду часу, яка передбачає можливість прямого обміну даними та доказами, співпраці в режимі реального часу та успішного проведення термінових операцій. JIT також дозволяє сторонам бути присутніми під час проведення слідчих заходів на територіях одна одної, а отже, більш ефективно ділитися своїми технічними та людськими ресурсами. Євроюст надає фінансову та операційну підтримку JITs, а також надає експертні висновки та судовий аналіз.

Переваги використання JIT у справах про кіберзлочини, зокрема: негайне збереження та обмін електронними доказами; обмін технічними та людськими ресурсами та досвідом для вирішення завдань розслідування та аналітики; чіткий і ранній розподіл слідчих завдань між сторонами JIT, включаючи співпрацю з приватними особами. Одна JIT може мати справу з більш ніж одним видом злочину. Євроюст розміщує Мережу JITs, мережу компетентних органів з усієї Європи, які регулярно зустрічаються для обміну досвідом і передовим досвідом щодо розслідування та переслідування кіберзлочинів. Євроюст також працює на інших рівнях для протидії кіберзлочинності, включно з питаннями поводження з жертвами кіберзлочинності, доступу до даних для кримінально-процесуальних цілей, а також шифрування та зберігання даних, необхідних як докази. Євроюст також формує Європейську судову кіберзлочинну мережу (EJCN), яка була створена в 2016 р. для сприяння контактам між фахівцями-практиками, які спеціалізуються на протидії викликам, пов'язаним з кіберзлочинністю та розслідуваннями в кіберпросторі, а також – для підвищення ефективності розслідувань і судових переслідувань. У 2018 р. EJCN займався жертвами кіберзлочинності, доступом до даних, електронними доказами, навчанням, шифруванням і збереженням даних [7].

EJCN сприяє та покращує співпрацю між компетентними судовими органами шляхом обміну досвідом, найкращим досвідом та іншими відповідними знаннями щодо розслідування та судового переслідування кіберзлочинів. Євроюст проводить регулярні зустрічі мережі та підтримує обмін інформацією між членами EJCN та іншими зацікавленими сторонами, які відіграють важливу роль у забезпеченні верховенства права в кіберпросторі. Законодавчі рамки та слідчі повноваження, які

надаються прокурорам, часто вже не відповідають швидко мінливому технічному середовищу, що оточує цю загрозу. Тому прокурори та судді в усіх державах-членах ЄС часто стикаються з однаковими новими правовими проблемами та сірими зонами, такими. як обмеження доступу до хмарних даних і пряма співпраця з постачальниками послуг та іншими приватними особами, які зберігають більшість електронних доказів, від яких залежать кримінальні розслідування [8].

Аналіз європейського досвіду щодо розслідування кіберзлочинів засвідчив, що цим правопорушенням приділяється значна увага. Спільні слідчі групи є одним із найефективніших інструментів для слідчих, які стикаються з проблемою боротьби з кіберзлочинністю. Нормативне регулювання діяльності та слідчі повноваження, які надаються прокурорам та суддям здебільшого не відповідають швидко мінливому технічному середовищу, що оточує цю загрозу. Серед іншого, в усіх державах-членах ЄС вони часто стикаються з обмеженням доступу до хмарних даних і прямої співпраці з постачальниками послуг та іншими приватними особами, які зберігають більшість електронних доказів. Цей позитивний досвід організації розслідування кіберзлочинів доцільно було б використовувати в Україні, особливо в умовах щоденних кібератак кібервійськ РФ на об'єкти інфраструктури, урядові та фінансові ресурси України.

Список використаної літератури:

1. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. Право і безпека. 2015. №2 (57). С. 107–113.
2. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. С. 192–194.
3. Le commandement de la cyberdéfense (COMCYBER). *Ministre des Armées.* URL: https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber.
4. Буяджа С. Позитивний досвід правового регулювання боротьби з кіберзлочинністю в країнах ЄС. *European political and law discourse.* Vol. 4. Issue 4. 2017. P. 41–46. URL: https://eppd13.cz/wp-content/uploads/2017/2017-4-4/07.pdf.
5. Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин

(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. дис. … канд. юрид. наук : 12.00.09. Київ. 2021. 268 с.
6. Cyber crime investigation: making a safer Internet space. *Maryville univercity.* URL: https://online.maryville.edu/blog/cyber-crime-investigation/.
7. Tackling cybercrime through joint investigation teams. Eurojust. 07 June 2019. URL: https://www.eurojust.europa.eu/news/tackling-cybercrime-through-joint-investigation-teams.
8. European Judicial Cybercrime Network (EJCN). Eurojust. URL: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network.

КОНЦЕПЦІЯ PAPERLESS VS КРИМІНАЛЬНЕ ПРОВАДЖЕННЯ

Клепка Дар'я Ігорівна,
кандидат юридичних наук, науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Незважаючи на триваюче повномасштабне вторгнення російської федерації, складні соціально-політичні умови в яких опинилась України, наша держава не звертає з цифрового шляху, обраного ще декілька років тому. Так, глава Міністерства цифрової трансформації Михайло Федоров на першому International Diia Summit Brave Ukraine у Давосі, який відбувся 24 травня 2022 року, анонсував амбітний план «цифрового» розвитку нашої країни, який передбачає, серед іншого, адміністративні суди зі штучним інтелектом та повний *Paperless* до 2030 року.

Такі рішучі політичні кроки мають своє відбиття й на галузі кримінальної юстиції. Варто відмітити, що у національному кримінальному процесі спостерігаються поступові кроки щодо відходу від паперового документообігу. Ще у 2020 році розпочала свою роботу пілотна версія електронного кримінального провадження eCase, яка функціонувала у системі органів боротьби з корупцією (НАБУ, САП, ВАКС). Позитивний досвід функціонування пілотної версії електронного кримінального провадження став підставою для внесення змін до кримінального процесуального законодавства України та введення до понятійного апарату КПК інформаційно-телекомунікаційної системи досудового розслідування. Невдовзі спільним Наказом Національного антикорупційного бюро України, Офісом Генерального прокурора, Радою суддів України та Вищим антикорупційним судом від 15 грудня 2021 р. № 175/390/57/72 затверджено Положення про інформаційну-телекомунікаційну систему досудового розслідування. Водночас знову ж таки така Система запроваджується виключно у кримінальних провадженнях, досудове розслідування в яких здійснюється детективами Національного антикорупційного бюро України. Щодо зрушень у напрямі запровадження інформаційно-телекомунікаційної системи досудового розслідування у роботі інших органів досудового розслідування не спостерігається.

Окремий етап змін можна відмітити у «воєнний період», зокрема закріплення законодавцем можливості виготовлення постанови слідчого, прокурора в електронному вигляді (абзац 2, ч. 6, ст. 110 КПК). Крім того, відповідно до ч. 14 ст. 615 КПК в редакції зі змінами, внесеними згідно із Законом України № 2137-IX від 15.03.2022 та Законом України № 2201-IX від 14.04.2022, на дізнавача, слідчого чи прокурора покладено обов'язок збереження в електронній формі копії матеріалів кримінальних проваджень, досудове розслідування в яких здійснюється в умовах воєнного стану. Реалізація цього обов'язку дізнавачем, слідчим, прокурором, як влучно визначено у науково-практичному коментарі до Розділу IX-1 Кримінального процесуального кодексу України, є можливою у трьох формах : виготовлення матеріалів кримінального провадження в електронній формі з використанням кваліфікованого електронного підпису службової особи; створення документів з використанням Інформаційно-телекомунікаційної системи досудового розслідування; оцифрування, тобто переведення матеріалів кримінального провадження в електронний формат [1][1].

У контексті здійснення досудового розслідування воєнних злочинів та оцифрування процесуальних документів звернімо увагу на виступ Кріса Ендельса директора з розслідування та операцій на міжнародній науково-практичній конференції «Організаційно-правові засади участі Збройних Сил України у вирішенні завдань розслідування воєнних злочинів та інших порушень міжнародного гуманітарного права під час збройної агресії російської федерації проти України». Так, розповідаючи про досвід розслідування воєнних злочинів у Сирії, Кріс Ендельс звернув особливу увагу на необхідність своєчасного та оперативного фіксування такого різновиду кримінальних правопорушень, підкреслюючи переваги здійснення фіксування саме в електронному вигляді. За його словами

[1] *Примітка.* Крім того, не можна оминути увагою й проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи» (реєстр. № 8219 від 23.11.2022 р.), яким серед іншого, передбачається, що процесуальні документи в електронній формі можуть подаватися учасниками справи до суду з використанням Єдиної судової інформаційно-телекомунікаційної системи та/або її окремих підсистем (модулів) в порядку, визначеному Положенням про Єдину судову інформаційно-телекомунікаційну систему та\або положеннями, що визначають порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи.

ними було зібрано 1 млн. документів, які важать приблизно 5 тон, що робить переміщення такого обсягу документації практично неможливим. У той же час спікер звернув увагу, що цифровий формат зібраної документації вміщується на одному електронному носії інформації.

Нагадаємо, що національне кримінальне процесуальне законодавство передбачає фіксування ходу та результатів слідчих розшукових дій у протоколі. Водночас форма (паперова (друкована) або електрона) протоколу законодавцем не передбачається та за загальним правилом протоколи створюються в формі друкованого документа. Наведене надає підстави стверджувати, що запровадження електронного документообігу у кримінальному провадженні має перспективи не лише в процесі здійснення ординарних проваджень, а й є затребуваним під час здійснення досудового розслідування в особливому режимі.

Взагалі можна навести такі переваги оцифрування документообігу в кримінальному провадженні.

– Зникнуть спори щодо того, що захист ознайомлювали з одними матеріалами, а до суду передали інші або якась частина матеріалів з'явилася чи зникла.

– Простіше буде ознайомлюватися з матеріалами досудового розслідування – їх можна буде просто завантажити на носій і працювати у зручному місці у зручний час.

– Зникнуть спори щодо того, у кого знаходяться матеріали кримінального провадження і хто саме повинен здійснювати досудове розслідування, та тяганина при передачі матеріалів між органами.

– У взаємодія з іншими інституціями, зокрема з приводу розслідування воєнних злочинів.

– В окремих випадках забезпечення обізнаності особи про причини та характер кримінального обвинувачення проти неї.

– Оперативність та своєчасність фіксування кримінальних правопорушень.

– Ефективізація роботи органів досудового розслідування та суду.

– Процесуальна та фінансова економія тощо.

Звісно варто пам'ятати й про баланс використання електронних документів у кримінальному провадженні та забезпеченні прав та законних інтересів осіб, залучених до орбіти кримінального судочинства. На що, зокрема звертає увагу Консультативна рада європейських суддів у своєму Висновку №14 (2011) 9, де йдеться про те, що не всі особи мають

доступ до ІТ. Нині не потрібно відмовлятися від традиційних засобів доступу до інформації. Довідкові стенди та інші форми допомоги, що надаються в судах, не повинні зникнути з огляду на те, що ІТ зробили правосуддя доступним для всіх. Подібні заходи є проявом турботи про соціально незахищені та вразливі верстви населення. Використання ІТ не повинно обмежити процесуальні гарантії тих, хто не має доступу до сучасних технологій. Держави мають гарантувати надання відповідної допомоги тим сторонам у справі, які не мають цього доступу.

Підсумовуючи вище викладене варто зазначити, що концепція *Paperless* має свої переваги та перспективи у кримінальному провадженні. Водночас враховуючи ступінь інтрузивності в права особи в кримінальному процесі варто дуже обережно та послідовно підходити до відмови від паперових (друкованих) процесуальних документів. Вбачається, що оптимальним для національного кримінального процесу є закріплення в законодавстві поруч із паперовими формами процесуальних документів й електронні за аналогією з абзац 2, ч. 6, ст. 110 КПК.

Список використаної літератури:

1. Гловюк І., Дроздов О., Тетерятник Г., Фоміна Т., Рогальська В., Завтур В. Особливий режим досудового розслідування, судового розгляду в умовах воєнного стану: науково-практичний коментар Розділу ІХ-1 Кримінального процесуального кодексу України. Видання 2. Електронне видання. Дніпро-Львів-Одеса-Харків, 2022. Станом на 03 травня 2022. 58 с.

ШУКАЙ AL: ЯК ШТУЧНИЙ ІНТЕЛЕКТ МОЖЕ ДОПОМОГТИ У ПОШУКУ ЗЛОЧИНЦІВ

Коростельова Лілія Анатоліївна,
інспектор відділу супроводження програм інформатизації та роботи із відкритими даними УІАП ГУНП в Луганській області

Коли ми говоримо про правоохоронні органи, зокрема про Національну поліції України. Давайте будемо відверті, штучний інтелект, це не перше, що спадає на думку, діджиталізація- це поки не про нас. Ми ще не говоримо про машинне навчання нам би с таким розібратись. Світ невпинно рухається в цю сторону, корпорації витрачають мільярди доларів на програмні продукти на основі ШІ. Правоохоронна система світу не випадок.

Зазначену технологію активно вже використовує поліція Дубаїв у 2018 році за допомогою смарт-програм і штучного інтелекту протягом 48 годин, затримала групу з десяти чоловік, які, за версією слідства, вкрали суму еквіваленту $1,9 млн[1].

600 поліцейських департаментів США використовують технологію. Clearview AI для ідентифікації осіб у соціальних мереж для подальшого розслідування злочинів[2].

Наша вітчизняна правоохоронна система вже робить перші кроки до автоматизації процесів роботи. Активно, використовують підрозділи Національної поліції України технологію Clearview AI щодо розпізнання злочинців, а у військовий час пошук та ідентифікація окупантів.

В сучасних реаліях, наша мета зробити крок у бік штучного інтелекту, щоб AL став на сторожі правопорядку.

Однією із ідей, що може бути втілена у правоохоронну діяльність – це створення алгоритмів штучного інтелекту на протидію серійних злочинів за рахунок методики геопрофілювання Россмо.

І так, як це працює, для того, щоб програмне забезпечення на основі штучного інтелекту запрацювало потрібно по-перше:

– розробити модель нейромережі, яка включатиме накопичені великі дані по серійним злочинам за останні 15 років. Чому саме за останні 15 років?(Ми беремо дані за такий час, по принципу того, чим більше даних, тім краще ми навчимо нейромережу аналізувати дані). Я точно знаю, що це займе певний час, але якщо ми зробимо зараз, то зазначену технологію будуть використовувати наші покоління.

По-друге, після того як ми створимо модель, і саме програмне забезпечення, на карті України позначаємо точки, які є фактами серійних злочинів, ця точка, в собі окрім геолокації, буде містити набір даних(дані про скоєне кримінальне правопорушення, дата, час, місце скоєння кримінального правопорушення, номер провадження, дані про жертву), тобто інтерактивна карта України на який ми будемо бачити дані про серійні злочини за останні 15 років.

По-третє, при продовженні нанесенні на карту нових випадків схожих на ознаки серійності того чи іншого виду злочину, модель може спрогнозувати одного й того злочинця, а також виходячи із методології Россмо вона визначить приблизне фактичне місце проживання потенційного злочинця-серійника в радіусі 1.5–2 км, що надасть змогу сконцентрувати увагу правоохоронних органів на визначеному радіусі пошуку.

Застосування даного механізму геопрофайлінгу в умовах невизначеності допоможе правоохоронним органам визначити та звузити коло підозрюваних; встановити зв'язки між аналогічними злочинами та поєднати їх у серію злочинів з одним виконавцем, а також підготуватися до майбутньої взаємодії з конкретною особою, з урахуванням її можливих поведінкових реакцій

Які можливості відкриває зазначене програмне забезпечення:

– по-перше це прискорення розслідування.(приклад інших країн)

– по друге збільшує довіру за рахунок більшої прозорості та відсутності корупції. (розшири поняття).

– по-третє відкриває ширші можливості для розвитку за рахунок підсилення авторитету на міжнародній арені та можливості обмінюватись досвідом із колегами.

Отже, чим більше ми даних зберемо, тим більше якісними будуть наші результати, Коли як не сьогодні нам варто об'єднатися, щоб наша правоохоронна система стала сильнішою, бо війна нам дала те, що коли ми об'єднані ми сильніші.

Список використаної літератури:

1. Штучний інтелект допоміг поліції Дубая зловити шахраїв та повернути два мільйони доларів. URL : https://informator.press/arhiv2018/shtuchnyj-intelekt-dopomih-politsiji-dubaya-zlovyty-shahrajiv-ta-povernuty-dva-miljony-dolariv/ (дата звернення 10.12.2022)

2. Поліція США використовує штучний інтелект для розпізнавання облич у соцмережах. URL : https://cybercalm.org/novyny/politsiya-ssha-vykorystovuye-shtuchnyj-intelekt-dlya-rozpiznavannya-oblych-u-sotsmerezhah/ (дата звернення 10.12.2022)

ЕЛЕКТРОННЕ ПОДАННЯ ДО СУДУ ТА ЦИФРОВІЗАЦІЯ СУДОВОГО ПРОЦЕСУ ЯК ЕЛЕМЕНТИ ВПРОВАДЖЕННЯ ЕФЕКТИВНОГО СУДОЧИНСТВА ТА ГАРАНІЯ ДОСТОВІРНОСТІ ДОКАЗІВ

Костюченко Олена Юріївна,
кандидат юридичних наук, доцент, завідувачка кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка

Нерозробленість теорії електронних доказів призводить до певних труднощів, з якими стикаються правоохоронні органи та суди [1], [2], [3]. Нематеріальна природа будь-яких даних та інформації, що зберігаються в електронному вигляді, значно полегшує маніпуляції та створює більшу вразливість до змін, ніж традиційні форми доказів. Це створює особливі виклики для системи правосуддя, яка вимагає, щоб такі дані оброблялися певним чином, щоб забезпечити цілісність доказів, які надаються в межах проваджень. Зважаючи на унікальні характеристики, електронні докази визначають як будь-яку інформацію, що генерується, зберігається або передається в цифровій формі, яка згодом може знадобитися для підтвердження або спростування факту, оскаржуваного в межах провадження. Використання електронних доказів супроводжується використанням штучного інтелекту (для перевірки достовірності) та впровадженням електронного подання документів.

Робочій групі з кіберюстиції та штучного інтелекту Комісії з питань ефективності правосуддя (CEPEJ-GT-CYBERJUST) Ради Європи було доручено розробити інструменти, щоб запропонувати правила та гарантії для використання інформації та комунікаційні технології (ІКТ) або механізми штучного інтелекту (AI) у судових системах з метою підвищення ефективності та якості правосуддя. У вересні 2020 року CEPEJ-GT-CYBERJUST була розпочата робота над електронним поданням до суду (e-filing) документів. У квітні 2021 року представлено доповідь на тему «Аналітичний огляд поточного стану електронної подання документів до суду (електронне подання) у державах-членах Ради Європи». Інструкції з електронного подання документів до суду (електронне подання) та цифровізація судів базуються на висновках цього звіту.

Робота в рамках вищезгаданого дослідження щодо електронного подання документів до суду базувалася на ключових поняттях: 1) впровадження цифрових рішень у судочинстві слід розуміти як системну та комплексну реформу, що виходить далеко за рамки технологічного процесу; 2) електронне подання документів та оцифрування судових процедур, які є частиною цілої системи послуг, відбувається незалежно від того, цифрові вони чи ні.

Керівні принципи базуються на розумінні того, що система електронної подачі документів повинна створити цифровий канал, який забезпечує взаємодію та обмін даними та електронними документами між судами та учасниками провадження. Така концепція вимагає змін, які передбачають не лише використання сучасних технологій для підтримки роботи судової системи, а також законодавчих, організаційних та соціально-культурних питань, які впливають на функціонування суду. Цифровізація вимагає стандартизації та спрощення процесів з подальшими правовими змінами, що впливають на права учасників кожного процесу.

9 грудня 2021 Європейською Комісією з ефективності правосуддя були ухвалені Рекомендації щодо електронного подання документів до суду (е-подання) та оцифрування їх судом. Незважаючи на те, що Керівні принципи можна використовувати як основу для всіх судових проваджень, існують відмінності між вимогами до цивільних, адміністративних і кримінальних проваджень.

Керівні принципи створюють структуру для електронної системи подання документів, що дозволяє стороні розпочати судовий розгляд шляхом видачі та отримання електронних документів, обмінюватися процесуальними документами з іншими учасниками провадження та з суддями/прокурорами, надсилати та/або отримувати повідомлення та виклики в електронному вигляді, сплачувати судовий збір онлайн та/або отримати доступ до безпечного сховища всіх процесуальних документів; забезпечує ефективну обробку даних.

Заслуговує на увагу нова термінологія, що наводиться в даних Рекомендаціях, зокрема, *електронний документ* означає будь-який вміст, що зберігається в електронній формі, зокрема текст або звуковий, візуальний чи аудіовізуальний запис; *електронне судове подання* відноситься до технологічних рішень, що полегшують доступ до правосуддя, створення цифрового каналу, що забезпечує взаємодію та обмін даними та електронними документами між судами та користувачами судів; *вну-*

трішні користувачі – судді, прокурори та інші працівники судових органів, залучені до ведення судового провадження; *зовнішні користувачі* – учасники процесу.

Електронне подання до суду базується на наступних принципах:1) верховенство права (будь-яке нове законодавство щодо цифровізації має бути чітким, прозорим і передбачуваним, має передбачати вирішення всіх питань, які можуть виникнути внаслідок самої цифровізації, та забезпечувати дотримання прав усіх користувачів цифрового судочинства; 2) незалежність судової влади є основною складовою забезпечення верховенства права (правила, закони та практика цифровізації не повинні мати жодного негативного впливу або загрожувати незалежності судової влади, суддів та адвокатів); 3) всі гарантії справедливого судового розгляду поширюються на цифрове судове провадження (зміни до регламенту у зв'язку з оцифруванням провадження, у тому числі актів і документів, має бути приведено у відповідність до права на справедливий суд); 4) доступ до ефективних засобів судового захисту надається у випадку, якщо основні права будь-якого учасника провадження постраждати від використання технології; 5) принцип захисту даних, у тому числі стосовно якості та безпеки обробки.

Електронна система подачі документів має полегшувати доступ до судової інформації, отже, до правосуддя, і забезпечувати підзвітність, балансуючи між доступом і захистом персональних даних, між доступом і захистом професійної таємниці.

Рада Європи наголошує на прийнятті спеціального законодавства щодо електронного правосуддя, що розглядається як передумова успішної цифровізації судових процедур, спрямованих на формалізацію, спрощення, дематеріалізацію та уніфікацію судових процесів, дотримуючись належного балансу між технічними характеристиками та гнучкістю щодо конкретних випадків використання.

Автоматизовані операції (наприклад, автоматичний розподіл справ, виклики, сповіщення, відстеження справ, управління взаємовідносинами, планування, звітування тощо) і функції, що мінімізують робоче навантаження (наприклад, запровадження шаблонів із змінним змістом, попередньо заповненими даними) не слід розглядати як додаткові заходи, а як вбудовані в структуру електронної подачі документів. Для цілей електронного подання всі судові документи повинні оброблятися виключно в електронній формі (як електронні документи), дотримуючись автентичності, цілісності та конфіденційності.

Кваліфіковані електронні підписи (або еквівалентні послуги) слід застосовувати до певних типів правових актів для забезпечення їх автентичність і цілісність, наприклад, коли їх потрібно використовувати за межами сфери правосуддя (наприклад, судові рішення). Щоб дозволити використання програм з будь-якого пристрою і без встановлення додаткового обладнання (наприклад, пристрої для зчитування смарт-карт) або програмне забезпечення, дистанційне кваліфіковане підписування (кваліфікована електронна печатка може бути альтернативою кваліфікованому електронному підпису, оскільки це автоматично застосовується системою).

Таким чином, існуючи наразі ризики в системі правосуддя щодо визнання достовірності та належності електронних доказів (надання роздруківок; засвідчення копій суддею у разі надання технічного засобу, з якого було зроблено роздруківку; демонстрація сканованого зображення екрану пристрою тощо) будуть мінімізовані застосуванням електронних систем контролю з використанням штучного інтелекту та електронних реквізитів документів, що подаються до суду; електронний документообіг між судом та зовнішніми учасниками судового провадження сприятиме дотриманню розумних строків та скороченню судових витрат.

Список використаної літератури:

1. Постанова ВС від 09 квітня 2020 року // https://reyestr.court.gov.ua/Review/88749345?fbclid=IwAR0gdLCRQGS2SjQNaluaOMy8VHgqYwxD0VXB_Cnx5kC38lZihxNj8F1rJrA

2. Постанова ВС від 19 травня 2021 року. Справа № 204/4521/18. Провадження № 51–5165 км 20 // https://reyestr.court.gov.ua/Review/97134877

3. Постанова ВС від 28 січня 2021 року. Справа № 182/523/16-к. Провадження № 51–1103 км 20// https://reyestr.court.gov.ua/Review/94553286

4. Guidelines on electronic court filing (e-filing) and digitalisation of courts. Document adopted at the 37th plenary meeting of the CEPEJ, Strasbourg and online, 8 and 9 December 2021. https://rm.coe.int/cepej-2021–15-en-e-filing-guidelines-digitalisation-courts/1680a4cf87.

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ ПРИ РОЗСЛІДУВАННІ ДЕРЖАВНОЇ ЗРАДИ В УМОВАХ ВОЄННОГО СТАНУ

Котюк Михайло Володимирович,
аспірант, НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Збройна агресія та повномасштабне вторгнення Російської Федерації в Україну викликало необхідність запровадження воєнного стану й суттєво вплинули на усі сфери нашого життя. Окупаційні російські війська, які прийшли на територію України вбивати, мародерити, ґвалтувати, руйнувати, скоюють воєнні злочини, які є надзвичайно масштабними і потребують належної їх фіксації та документування, збирання доказової бази для розгляду їх міжнародних кримінальних інституціях задля притягнення до кримінальної відповідальності усіх підозрюваних, причетних до вчинення таких страшних воєнних злочинів, у тому числі й представників військово-політичного керівництва РФ. За таких умов правоохоронні та судові органи стикнулися з новими викликами, які у свою чергу потребують застосування інноваційних та реально дієвих методів, засобів та прийомів, які можуть забезпечити їх ефективне вирішення [4; 14; 15].

Російсько-українська війна та введення на території України воєнного стану зумовила появу нових завдань перед органами кримінальної юстиції та вітчичняною правовою системою, пов'язаних із військовою агресією РФ та зміною кримінальної ситуації в державі й негативною тенденцією зростання рівня сучасної злочинності і її трансформацією в реаліях воєнного часу. Так, з початку повномасштабного вторгнення росії в Україну (станом на 20.12.2022 р.) слідчі Національної поліції України розпочали 56 993 кримінальних проваджень за фактами вчинення на території України злочинів військовослужбовцями збройних сил російської федерації та їхніми пособниками. З них: 38 398 – за ст. 438 КК України (Порушення законів та звичаїв війни); 9144 – за ст. 110 КК України (Посягання на територіальну цілісність і недоторканність України); 2210 – за ст. 111–1 КК України (Колабораційна діяльність); 103 – за ст. 111 КК України (Державна зрада); 37 – за ст. 113 КК України (Диверсія) та ін [3].

За офіційними даними Офісу Генерального прокурора, з початку російсько-української війни було зареєстровано 18 438 злочинів проти

проти національної безпеки України, серед них виявлено 637 злочинів за фактами державної зради та колабораційної діяльності, зокрема, правоохоронці зареєстрували 415 кримінальних проваджень за ст. 111 КК України (державна зрада) та 222 за ст. 111–1 ККУ (колабораційна діяльність) [10]. Як бачимо, серед кримінальних правопорушень, які є особливо небезпечними в сучасних реаліях воєнного стану є вчинення державної зради (ст. 111 КК України). Як свідчить практика, такі злочини, заподіюючи значну шкоду громадській безпеці українському народу та нашій державі, є одним із чинників серйозної загрози національній безпеці України.

Вбачається, що державній зраді притаманний специфічний механізм її скоєння, своєрідні "слідова картина", характеристика особи злочинця, способи вчинення такої злочинної діяльності, які характеризуються високим рівнем законспірованності, латентності, а практичні працівники правоохоронних органів стикаються із значними труднощами під час їх виявлення, розкриття, розслідування та профілактики. Вирішення таких завдань та створення відповідного механізму передбачає запровадження ефективної системи протидії цим кримінальним проявам, реформування кримінального і кримінального процесуального законодавства, вжиття невідкладних заходів, спрямованих на вдосконалення слідчої та судової практики [13, с. 320–341], що ґрунтуються на новітніх досягненнях криміналістичної науки, техніки, міжнародного досвіду, у тому числі й застосування засобів цифрових технологій у криміналістиці.

Важливо зауважити, що у дослідженні проблематики використання цифрової інформації необхідно розрізняти засоби цифрової криміналістики як окрему галузь криміналістичних знань, спрямовану на дослідження цифрових слідів [6, с. 167], та застосування цифрових технологій у розслідуванні кримінальних правопорушень [11, с. 288], у тому числі й державної зради. Передусім пояснюється це тим, що застосування цифрових технологій являє собою своєрідний процес цифровізації криміналістики як закономірний сучасний етап розвитку та формування криміналістичної науки [12, с. 162], який передбачає впровадження цифрових технологій у різні галузі криміналістичної техніки та судової експертизи, до самого процесу досудового розслідування та судового розгляду матеріалів кримінальних проваджень державної зради.

У цьому плані слушним є твердження у спеціальній літературі [2, с. 105], що цифровізація в криміналістиці може охоплювати декілька напрямків, зокрема таких як-то: 1) використання цифрових технологій

для підвищення ефективності пошуково-пізнавальної діяльності слідчого, ефективної організації цієї діяльності на сучасному рівні, оптимізації взаємодії різних органів, установ при розслідуванні злочинів; 2) використання інформаційно-комунікативних технологій для розслідування злочинів. Широке поширення інформаційних комп'ютерних технологій сприяє подальшим розробкам в області алгоритмізації процесу розслідування в цілому і окремих його етапів; 3) рішення дидактичних завдань в сфері підготовки, перепідготовки, підвищення кваліфікації слідчих, слідчих-криміналістів, судових експертів, обміну досвідом [6, с. 392]. В свою чергу розвиток цифрової криміналістики відбувається у таких напрямах: 1) формування окремої наукової галузі в криміналітиці; 2) застосування спеціальних знань під час роботи з цифровими доказами; 3) проведения судових експертиз (зокрема, комп'ютерно-технічної експертизи) [6, с. 21].

На наш погляд, певний науково-практичний інтерес можуть мати засоби цифрової криміналістики, які допомагають у виявленні та розслідуванні державної зради в умовах воєнного часу. Вивчення та аналіз фахової літератури [7; 8; 9] дає можливість виокремити засоби і напрямки застосування цифрової криміналістики для ефективного документування та успішного розслідування цих кримінальних правопорушень: пошук за ключовими словами та хештегами, списки яких попередньо піготовлені, моніторинг радарівв та системи офіційного моніторингу суден Marine Traffic, аналіз супутникових знімків, використання технології аналізу «великих даних» (Big Data); аналіз геолокаційних міток, дослідження фото- та відеоматеріалів у відкритому доступі та наданих слідству, використання програм для аналізу та обробки цифрових зображень, дослідження телефонних розмов, аналіз електронних пристроїв, аналіз ігрових систем, система розпізнавання облич і пошуку їх у відповідних базах даних (в Україні використовують додаток з розпізнавання облич Clearview Af для ідентифікації потенційних злочинців і загиблих) [7, с. 32].

Важливим доповненням переліку засобів цифрової криміналістики під час розслідування державної зради може також бути: 1) дослідження хмарних сховищ; 2) дослідження мобільних пристроїв (телефонів); 3) дослідження програм (месенджерів та інших застосунків для смартфонів, що викори- стовуються для обміну інформацією); 4) дослідження інтернет-речей (IoT); 5) мережеві дослідження; 6) дослідження новітніх приладів і додатків (Alexa від Amazon, Google Assistant, Siri від Apple та

ін.); 7) дослідження додатків не лише для телефонів, а й інших систем (дослідження баз даних, Spotlight, America online instant messaging, дронів, Даркнету, засобів антикриміналістики, видалених і фрагментованих файлів, зображень, флеш-пам'яті, криповалют); 8) цифровий аналіз поведінки; 9) цифрова криміналістична розвідка та розвідка на основі відкритих джерел тощо [9].

Таким чином, у сучасній криміналістичній доктрині сьогодні в умовах війни досить значимим та актуальним є розроблення комплексу проблем криміналістичного забезпечення виявлення, документування та розслідування державної зради. Серед таких напрямків, на наш погляд, одним із найбільш перспективних постає саме проблематика застосування цифрових технологій при розслідуванні таких кримінальних правопорушень, у тому числі й актуальні питання перспектив формування, удосконалення та реалізації засобів цифрової криміналістики, як нового стратегічного напрямку розвитку сучасної криміналістики, який має бути адаптований до сучасних реалій воєнного часу, потреб практики та міжнародного досвіду у сфері протидії злочинності.

Список використаної літератури:

1. Главюк І. В. Використання у доказуванні комп'ютерних даних та арешт комп'ютерних систем або їх частин. *Актуальні проблеми діяльності органів досудового розслідування в умовах воєнного стану*: матеріали наук.-практ. семінару (м. Дніпро, 26 травня 2022 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2022. С. 47–50.
2. Думчиков М. О. Процеси діджиталізації и криміналістика: ретроспективний аналіз. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 100–108. С. 104–105.
3. Злочини, вчинені військовими рф під час повномасштабного вторгнення в Україну (станом на 20.12.2022) // Національна поліція України URL: https://www. npu. gov. ua/news/zlochyny-vchyneni-viiskovymy-rf-pid-chas-povnomasshtabnoho-vtorhnennia-v-ukrainu-stanom-na-20122022
4. Konovalova V. O., *Shevchuk V. M.* Prospective directions of research of innovations of separate criminalistic methodics. *Scientific practice: modern and classical research methods: I International Scientific Conference* (Vol. 1), Boston, February 26, 2021. Boston-Vinnytsia, 2021. P. 81–85.
5. Konovalova V. O., Shevchuk V. M. Innovations in the methodic of teaching criminalistics in modern realities of war. *Modern scientific research*: *achievements, innovations and development prospects*: Proceedings of the

15th International scientific and practical conference (August 14–16, 2022). Berlin, 2022. Pp. 385–396.
6. Latysh, K. K. (2021). Criminalistics Analysis of Cyber Tools for Committing Crimes. Problems of Legality, 153, 165–172.
7. Латиш К. *Цифрова криміналістика* у *період війни* в *Україні: можливості використання спеціальних знань* у *сфері інформаційних технологій. Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika*, 2022,18, 31–37.
8. Paweł Olbe. Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych. Wydawnictwo: Wyższa Szkoła Policji w Szczytnie. 2021. 412 S.
9. Reedy P. Interpol review of digital evidence 2016–2019. Forensic Science International: Synergy. 2020. Vol. 2. P. 489–520.
10. Сайт Офісу Генпрокурора. URL: https://www. gp. gov. ua/ (дата звернення: 20.12.2022).
11. Степанюк Р. Л. Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного ун-ту внутр. справ ім. Е. О. Дідоренка*. 2022. №3 (99). С. 283–294.
12. Shevchuk V. Innovative Essence of Criminalistic and Prospective Directions of its Development. *Developments of criminalistics theory and future of forensic expertology: liber amicorum profesoriui Egidijui Vidmantui Kurapkai.* Collective monograpfy / Malewski H., Matuliene S., Shepitko V., Shevchuk V. and others. Vilnius, Mykolas Romeris University, 2022. Pp. 152–168.
13. Shevchuk V., Vapniarchuk V., Borysenko I., Zatenatskyi D., Semenogov V. Criminalistic methodics of crime investigation: Current problems and promising research areas. *Revista Juridica Portucalense*, 32, 2022. Pp. 320–341.
14. Шепітько В., Шепітько М. Доктрина криміалістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 8, 2021. С. 12–27.
15. Шепітько В. Ю., Коновалова В. О., Шевчук В. М. та ін. Науково-технічне забезпечення слідчої діяльності в умовах змагального кримінального процесу. *Питання боротьби зі злочинністю.* 2021. Вип. 42. С. 92-102.

ЄВРОПЕЙСЬКІ ПРИНЦИПИ ТА РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ СУДОЧИНСТВІ

Крицька Ірина Олександрівна,
кандидат юридичних наук, старший викладач кафедри кримінального процесу, Національний юридичний університет імені Ярослава Мудрого

Попри всі перешкоди та виклики, які постали перед Україною через військову агресію, наша держава прагне до розвитку, який, зокрема, стосується сфери цифровізації. Одним із найбільш прогресивних напрямків такого діджитал-розвитку є розширення використання технологій штучного інтелекту (далі – ШІ) на різноманітні сфери суспільного життя, серед яких важливе місце займає й царина правосуддя. Важливо відмітити, що здійснення судочинства, особливо кримінального, нерозривно пов'язано із втручанням в основоположні права та свободи людини та прийняттям нерідко визначальних для долі людини рішень. А тому використання технологій ШІ у цій сфері має бути чітко регламентованим, контрольованим та відповідати певним стандартам, оскільки несе на собі ризики дискримінації, обмеження права особи на справедливий суд, права на приватність тощо. Зважаючи на те, що сьогодні Україна вже перебуває на шляху інтеграції до Європейського Союзу, пропонуємо зупинитися на окремих нормативних документах, що відіграють ключову роль в регламентації основних принципів, підходів та рекомендацій щодо застосування ШІ у сфері кримінальної юстиції для європейських держав.

Відправною точкою нашого аналізу, як убачається, має стати Висновок №14 (2011) «Судочинство та інформаційні технології» [1], підготовлений Консультативною радою європейських суддів ще у 2011 р. Указаний документ ще не згадує ШІ, а концентрує увагу на перевагах застосування інформаційних технологій у судочинстві, зокрема, на можливому покращенні процесу розгляду та руху судових справ, підвищенні рівня діяльності суду взагалі, спрощенні доступу до інформації про хід та результати судового розгляду для учасників процесу та третіх осіб. Підкреслимо, що вже у цьому Висновку відмічалося важливе засадниче положення, яке стосується особливої ролі людини при використанні цифрових технологій у відправленні правосуддя – йдеться про обов'язкову участь судді у прийнятті всіх рішень стосовно використання та розвитку ІТ у судовій системі, а також про неможливість за-

міни інформаційними технологіями повноважень судді стосовно вивчення та оцінки доказів, інакше це порушило б ідеї верховенства права та гарантії, закріплені у ст. 6 Європейської конвенції з прав людини. Як можна буде простежити далі, цей принцип проходить «червоною ниткою» у наступних європейських нормативних документах з цього аспекту. Тобто, хоча зазначений Висновок ще безпосередньо не регламентував питання, пов'язані з використанням штучного інтелекту, однак в загальному вигляді визначив орієнтири для подальшого використання цього різновиду цифрових технологій.

Наступним, надзвичайно важливим етапом щодо визначення орієнтирів у векторі використання технологій штучного інтелекту в правосудді, стало прийняття у 2018 р. Європейською комісією з питань ефективності правосуддя (СЕРЕЈ), що функціонує при Раді Європи, Європейської хартії етичного використання ШІ у судових системах та суміжному середовищі [2]. Цей документ не тільки містить визначення пріоритетних напрямків використання ШІ в судових системах, але й передбачає відмінності в межах його застосування при прийнятті рішень у цивільних, господарських та адміністративних справах, з одного боку, та кримінальних провадженнях – з іншого. До того ж, в Хартії акцентується увага на ключовому значенні проголошених Європейською конвенцією з прав людини і Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних фундаментальних прав людини, які обов'язково мають бути враховані при використанні ШІ та які, загалом, спрямовують його використання.

Але особливе значення Хартії полягає в тому, що вона, по-перше, містить дефініції категорії «штучний інтелект», а також понять, базових для сфери ІТ, зокрема: «дані», «мета-дані», «база даних», «алгоритм», «чат-бот», «дата-майнінг», «машинне навчання» тощо. А, по-друге, закріплює п'ять основоположних принципів застосування технологій штучного інтелекту в судових системах та суміжному середовищі. Йдеться про такі принципи: (1) *поваги та врахування фундаментальних прав людини*; (2) *заборони дискримінації* (сутність цього принципу базується на основах роботи алгоритмів штучного інтелекту, які можуть використовуватися ще на фазі розробки, та виходить із ідеї про недопустимість закладення даних, що апріорі є упередженими відносно певних груп осіб – за расою, віком, статтю тощо); (3) *якості та безпеки* (стосується вимог щодо необхідності використання сертифікованих джерел для механізму машинного навчання та забезпечення вимог щодо захищеного середовища, які поширюються на збереження та використання створених моделей і алгоритмів); (4) *відкритості (транспарентності)* (цей

принцип ґрунтується на підходах, що передбачають використання доступних і зрозумілих способів обробки даних, а також здійснення зовнішніх перевірок); (5) *контрольованості* (користувач у будь-який момент повинен мати доступ до перегляду судових рішень та даних, які використовуються ШІ, а також можливість внесення необхідних коректив до прийнятого рішення чи його скасування).

На основі зазначеної Хартії та Європейської конвенції з прав людини, а також відповідного вторинного законодавства ЄС (Загальний регламент захисту даних (GDPR), Регламент (ЄС) 2018/172521 (EUDPR), Директива про електронну конфіденційність і Директива про правоохоронні органи (LED)) та практики, Експертна група високого рівня зі ШІ 8 квітня 2019 р. опублікувала Етичні рекомендації щодо надійного ШІ [2]. Рекомендації визначають сім ключових вимог, яким мають відповідати системи ШІ: 1) людське представництво та нагляд; 2) технічна надійність і безпечність; 3) приватність і керування даними; 4) транспарентність; 5) недискримінація та справедливість; 6) суспільний та навколишній добробут; 7) підзвітність і відповідальність.

Наступною сходинкою на шляху контрольованого запровадження штучного інтелекту в процеси відправлення правосуддя можна визнати «Білу книгу зі штучного інтелекту. Європейський підхід до досконалості і довіри» [3], що була опублікована 19 лютого 2020 р. Цей документ не присвячений безпосередньо проблемам використання відповідних алгоритмів у кримінальному провадженні, однак, по суті, його можна розглядати як певну «дорожну карту» необхідних нормативних корекцій, оскільки Біла книга містить пропозиції та рекомендації щодо можливих змін до європейського законодавства, які б могли сприяти надійному та безпечному розвитку штучного інтелекту в Європі з усією повагою до цінностей і прав громадян ЄС, зокрема, права на повагу до людської гідності і захисту приватності. Цей європейський документ визначає певні напрямки вдосконалення законодавчої бази ЄС для вирішення можливих ризиків і ситуацій: а) ефективне застосування та виконання чинного законодавства ЄС та національного законодавства; б) обмеження сфери дії чинного законодавства ЄС; в) зміна функціональності систем ШІ та ін. При цьому основну увагу має бути сконцентровано на застосунках штучного інтелекту з високим рівнем ризику, тобто тих, які можуть найбільше посягнути на фундаментальні права людини, зокрема, права на приватність та повагу до людської гідності.

Вимоги до них, згідно з Білою книгою, мають включати певні характеристики: 1) якість вихідних навчальних даних, що закладені в основу алго-

ритмів навчання; 2) здійснення контрольованого обліку та збереження даних і записів, в тому числі і щодо роботи алгоритмів і проблем в обробці даних; 3) проактивне надання необхідної інформації користувачам щодо використання систем ШІ високого ризику, зокрема, і з метою сприяння відповідальному використанню ШІ, зміцнення довіри та сприяння відшкодуванню, якщо це необхідно; 4) надійність і точність високоризикових програм ШІ –такі системи потрібно розробляти відповідально та з попереднім належним урахуванням ризиків, які вони можуть створити (включає вимоги, що забезпечують відтворюваність результатів, гарантують, що системи ШІ зможуть адекватно справлятися з помилками або невідповідностями на всіх етапах життєвого циклу та ін.); 5) обов'язковість нагляду з боку людини (ШІ не повинен підривати автономію людини, оскільки надійне, етичне та людиноцентричне використання ШІ може бути лише шляхом забезпечення відповідної участі людей у роботі з високоризиковими програмами ШІ).

Надалі, на продовження розглядуваного вектору роботи, Європейський парламент 6 жовтня 2021 р. прийняв Резолюцію щодо ШІ у кримінальному праві та його використання поліцією та судовими органами у кримінальних справах. У Резолюції підтверджено такі ключові аспекти: (а) усі рішення ШІ для правоохоронних органів і судової системи повинні повністю поважати принципи людської гідності, недискримінації, свободи пересування, презумпції невинуватості та права на захист тощо – інакше використання технологій штучного інтелекту має бути заборонено; (б) безпечність використання систем ШІ, які мають бути надійними та стійкими, щоб запобігти потенційно катастрофічним наслідкам зловмисних атак на них; (в) спеціальний людський контроль перед запуском певних критично важливих додатків ШІ; (г) використання лише тих систем ШІ, які дотримуються принципу конфіденційності та захисту даних (без допущення повзучого функціонування). На виконання вказаної Резолюції у грудні 2021 р. Європейською комісією було прийнято дві пропозиції: по-перше, Регламенту, що встановлює правила цифрового зв'язку в процедурах судової комунікації в цивільних, комерційних і кримінальних справах, і, по-друге, Директиви, яка узгоджує існуючі правила комунікації з правилами запропонованого Регламенту.

Список використаної літератури:

1. Висновок № 14 (2011) Консультативної ради європейських суддів до уваги Комітету міністрів Ради Європи про правосуддя та інформаційні

технології (IT). URL: https://rm.coe.int/opinion-n-14–2011-on-justice-and-information-technologies-it-/16806a1fc0
2. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c
3. Ethics Guidelines for Trustworthy Artificial Intelligence (European Commission, 2019). URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
4. White Paper on Artificial Intelligence: a European approach to excellence and trust. URL: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en
5. Digitalisation of cross-border judicial cooperation. URL: https://commission.europa.eu/publications/digitalisation-cross-border-judicial-cooperation_en

АКТУАЛЬНІ ПИТАННЯ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНОЇ ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ

Марочкін Олексій Іванович,
кандидат юридичних наук, старший науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

З початку 90-х років минулого століття цифрові інструменти та Інтернет докорінно змінили способи отримання, збирання та поширення інформації в усіх сферах суспільного життя, у тому числі й у сфері кримінальної процесуальної діяльності. Адже без перебільшення можна зазначити, що новації, запроваджені цифровим середовищем, значною мірою змінили й обличчя вітчизняного кримінального процесу.

Цифрове середовище призвело до розмаїття таких процесуальних джерел інформації, як речові докази та документи, які можуть допомогти у виявленні та розслідуванні не тільки правопорушень у сфері кібербезпеки. На порядку денному з'явилася нова категорія злочинів, з одного боку, проти миру, безпеки людства та міжнародного правопорядку, а з іншого – проти основ національної безпеки України – державна зрада, колабораційна діяльність, пособництво державі-агресору тощо.

Серед змін – новацій – залучення до кримінального провадження «продуктів штучного інтелекту» – цифрових (електронних) доказів та подальший відступ від принципу безпосереднього дослідження судом доказів шляхом використанням інформаційно-комунікаційних технологій.

У зв'язку з цим науковому обґрунтуванню підлягають, наприклад, такі питання, як природа електронних документів як доказів у кримінальному провадженні та особливості їх використання. Чи є вони новим процесуальним джерелом доказів, чи вони є документами з притаманними їм властивостями та особливостями доступу до них тощо.

Характерною ознакою Е-документа є його двоїстість – з одного боку він складається з інформації, а з іншого – з матеріального носія, на якому ця інформація фіксується. Якщо ж проаналізувати погляди вчених, то можна зазначити, що вчені – процесуалісти дискутують щодо їх місця у системі процесуальних джерел доказів, а вчені – криміналісти – до якого виду доказів – речових чи письмових їх треба відносити. Актуальним

залишається також питання про зберігання таких доказів з огляду на забезпечення їх надійності, достовірності, справжності та цілісності.

Одним із важливих елементів справедливого кримінального судочинства є принцип безпосередності дослідження доказів судом. За висновком ЄСПЛ йдеться про право обвинуваченого мати можливість протистояти свідку у присутності судді, який остаточно вирішує справу.

За загальним правилом суд може обґрунтовувати свої висновки лише на показаннях, які він безпосередньо сприймав під час судового засідання, або отриманих в порядку, передбаченому ст. 225 КПК. Йдеться про виняткові випадки, коли за певних обставин, що можуть унеможливити їх допит в суді (існування небезпеки для життя і здоров'я, тяжка хвороба, інші обставини) свідок, потерпілий у певному процесуальному порядку можуть бути допитані слідчим суддею. Порушення цих положень закону позбавляє суд права обґрунтовувати судові рішення показаннями, наданими слідчому, прокурору або посилатися на них.

Введення в нашій державі воєнного стану внесло істотні корективи в механізм реалізації принципу безпосередності дослідження доказів судом. Потреба у підвищені ефективності досудового розслідування «за гарячими слідами» та протидії злочинам, які вчиняються в умовах воєнного стану, удосконалення порядку здійснення кримінального провадження у нових умовах існування нашої держави, обумовила необхідність подальшого розширення переліку виключень із принципу безпосередності дослідження доказів судом.

Тому Законами України від 15.03.2022 р. та від 14.04.2022 р. ст. 615 КПК було доповнено положеннями про те, що показання, отримані під час допиту свідка, потерпілого, що здійснюються 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. Що стосується показань, отриманих під час допиту підозрюваного, то вони можуть бути використані як докази в суді виключно у випадку, якщо у такому допиті брав участь захисник. Більше того, передбачена можливість дистанційної участі захисника і перекладача у кримінальному провадженні у разі неможливості їх явки для безпосередньої участі у справі. Тож джерелами доказової інформації у кримінальних провадженнях все частіше стають цифрові, у яких відображаються обставини кримінального правопорушення та проведені процесуальні дії.

Зрозуміло, що такі відступи від принципу безпосередності стають можливими завдяки запровадженню цифрового (електронного) правосуддя, яке з появою новітніх технологій може порушувати єдність часу, місця та процедури в процесі дослідження доказів. В свою чергу, роз'єднання простору та часу, які раніше були поєднані у доцифровому процесі, тягне порушення неперервності між спілкуванням учасників судового процесу у формі змагальності сторін, та електронною (цифровою) інформацією, що має доказове значення і може бути покладена в основу судового рішення.

Особливістю електронної (цифрової) інформації є те, що вона існує в електронно-цифровій формі. Такий її характер вимагає обов'язкового перетворення цих даних для їх подальшого дослідження та використання. Тобто, на відміну від доказів, у яких фактичні дані містяться у природному, некодованому вигляді, для сприйняття інформації, що зберігається на цифровому джерелі, обов'язковою має бути процедура її перетворення (перекодування) в іншу форму, доступну для її безпосереднього сприйняття.

Сучасні технології, які використовуються під час здійснення електронного правосуддя, а саме: комп'ютерні системи для дослідження електронних та відеодоказів, системи віддаленої участі в процесі (платформи відеозв'язку тощо), суттєво змінюють його просторові межі. З іншого боку, актуалізується дослідження у сфері впливу таких технологій на якість правосуддя. Зокрема, якщо суд відбувається за допомогою відео-конференц-зв'язку, виникає чимало процесуальних питань. Наприклад, будь-яке переривання зв'язку, викривлення звуку чи відео ставить питання про законність усього засідання. А якщо сторона не побачила, не почула будь-що під час процесу через технічний брак, чи є це підставою для скасування судового рішення? Як бути із дослідженням доказів, якщо один учасник надав їх у залі судового засідання, а інші – шляхом відеозв'язку? Відповідь на ці питання міститься у Керівних принципах Комітету міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних провадженнях, прийнятих 30 січня 2019 р. на 1335 засіданні заступників Міністрів (далі – Керівні принципи). Вони мають слугувати практичним інструментом для держав-членів, допомагати адаптувати функціонування своїх судових та інших механізмів врегулювання спорів для вирішення питань, що виникають у зв'язку з електронними доказами у судових провадженнях. Йдеться, перш за все,

про усні свідчення, отримані засобами дистанційного зв'язку. Так, *по-перше,* такі свідчення можуть бути отримані дистанційно шляхом використання технічних пристроїв, якщо характер доказів це дозволяє; *по-друге,* при вирішенні питання, чи можуть усні свідчення бути прийняті дистанційно, суди повинні враховувати, зокрема, такі фактори: значимість свідчення; статус особи, яка дає свідчення; безпека та надійність відеозв'язку, через який мають передаватися свідчення; витрати та труднощі доставлення відповідної особи до суду; *по-третє,* при дистанційному прийнятті доказів необхідно забезпечити таке: a) передача усних свідчень має бути побачена та почута особами, які беруть участь у провадженні, та представниками громадськості, якщо провадження проводиться публічно; b) особа, яка була дистанційно заслухана, може бачити та чути провадження, за необхідності для забезпечення справедливості та ефективності; *по-четверте,* процедура та технології, які застосовуються для отримання свідчень дистанційно, не повинні ставити під загрозу прийняття таких доказів та здатність суду встановити особистість таких осіб; *по-п'яте,* незалежно від того, чи передаються свідчення шляхом стаціонарного чи мобільного зв'язку, слід забезпечити належну якість відеоконференції та зашифрувати відеосигнал для захисту від перехоплення.

Важливими висновками Керівних принципів є наступні: 1) питання вирішення потенційної доказової цінності електронних доказів належить судам відповідно до національного законодавства; 2) електронні докази повинні оцінюватися так само, як і інші види доказів, зокрема, стосовно допустимості, достовірності, точності та цілісності.

В підсумку зазначимо, що докази та доказування є основою будь-якого процесу, і від того, наскільки якісно та повно під час досудового розслідування та судового розгляду будуть зібрані та досліджені докази, залежить ефективність розгляду кримінального провадження в суді та швидкість досягнення мети правосуддя. Тому електронні докази мають бути зібрані у належний та безпечний спосіб і подані до суду з використанням надійних послуг відповідно до встановленої процедури вилучення та збору електронних доказів.

ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ НА ШЛЯХУ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНОГО ПРОЦЕСУ

Метелев Олексій Павлович,
доктор філософії в галузі права, завідувач спеціальної кафедри Інституту підготовки юридичних кадрів для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого

Цифровізація – це не тільки логічний етап розвитку технологічної частини життя суспільства, яке з кінця 20-го століття перетворилось з індустріального в інформаційне, але й виклик до змін для всієї правової і соціально-політичної реальності. В Україні, яка реалізує європейський шлях розвитку правової держави, на якому цифровізація функцій усіх інституцій – важливе завдання та вимога Європейського Союзу, не дивлячись на воєнний стан і збройну агресію рф, здійснюється поступове законодавча та практична інтеграція цифрових та інформаційних технологій у всі сфери нашого життя, у тому числі і в кримінальне судочинство.

Основними причинами впровадження інформаційних технологій у кримінальний процес, а також автоматизації діяльності судів законодавець визначив у Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки, №276/2015, а згодом, у Стратегії розвитку системи правосуддя та конституційного судочинства на 2021–2023 роки [1, 2]. Зокрема, це відсутність належної ІТ-інфраструктури та можливостей використання інформаційних систем і системи електронного правосуддя; недостатній рівень дотримання принципу змагальності в кримінальному провадженні, відсутність професійної відповідальності за порушення прав людини й ігнорування принципу змагальності; розбіжності між новими процесуальними повноваженнями та реальними інституційними функціями суб'єктів досудового та судового етапів слідства; відсутність належної динаміки у наближенні до стандартів Європейського Союзу тощо.

Розглядаючи процес цифровізації, необхідно враховувати той факт, що будь-які інформаційні технології, інтегровані у систему кримінального судочинства, складаються з двох взаємопов'язаних складових: технічної (сукупності цифрових засобів, електронних комунікаційних мереж та електронних інформаційних систем) і соціальної (спільнота користувачів, більшість з яких є правниками). І якщо в питаннях забез-

печення роботи технічної складової все зрозуміло: необхідно забезпечити безперебійне живлення, професійне сервісне та інженерне обслуговування, надійне збереження цифрових даних в т.п., то з користувачами інформаційних систем необхідно проводити додаткову роз'яснювальну роботу та навчання з підвищення комп'ютерної грамотності та основ інформаційної та кібернетичної безпеки.

Також, актуальним проблемним питанням на шляху цифровізації кримінального процесу є забезпечення термінологічної єдності нових для кримінального процесу понять з технічної та інформаційної сфери знань. Як відомо, знання є найважливішою складовою змісту освіти, її ядром. На основі знань формуються вміння, навички, розумові і практичні дії. Знання ж наукові, як основа картини світу, від решти знань вирізняються ознаками загальності, перевіреності та стійкості, тобто такою глибиною опрацювання гіпотези, яка запобігає швидкому старінню знань. У сучасних умовах ми зіткнулись з ситуацією, коли обґрунтований консерватизм юридичної науки, зокрема доказового права, науки кримінального процесу, зустрічається з об'єктивною реальністю швидкої зміни парадигми сприйняття навколишнього світу, в якому реальність все більше стає цифровою.

Зміст, який ще кілька років назад вкладався в такі поняття як «комп'ютери», «документи», «докази», «інформаційний простір», «кіберпростір», «телекомунікаційна мережа» тощо – сьогодні вже не відповідають дійсності. Так, електронний документ кардинально відрізняється від традиційного документу не тільки за формою відображення інформації, але й за самою сутністю. Наприклад, якщо відірвати частину аркушу паперу – документ не загубить свого доказового значення, проте, втрата частини файлу цифрового (електронного) документу, призведе до його повного знищення. Комп'ютери, які раніше були єдиним інструментом вводу, виводу та відображення цифрової інформації, сьогодні лише маленька частина цифрових «гаджетів». Цифрові докази за своєю природою вже мають всі ознаки окремого виду доказів у кримінальному процесі. Межі інформаційного та кібернетичного просторів стають «розмитими» і незабаром, з урахуванням того, що все більше даних зберігаються у «хмарних» сховищах та в мережі Інтернет, вони скоро мають об'єднатись…

Все це, в свою чергу, говорить про те, що система законодавства, як основна юридична форма права, має відповідати ознакам узгодженос-

ті та понятійної (термінологічної) єдності. І особливо актуально це на фоні цифровізації кримінального судочинства.

Для прикладу, аналіз норм Кримінального процесуального кодексу України (далі – КПК) і, зокрема, його недавніх змін від 15 травня 2022 (Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 року №2137-IX) показали, що з термінологічною єдністю в частині, що стосується інформаційних технологій, в кодексі є певні проблеми, які потребують не тільки наукової дискусії, але й змін [3].

Зокрема, потребує узгодження термінологія щодо цифрових пристроїв, систем та мереж, деякі з яких вже застарілі (як, наприклад, «комп'ютерні дані»), дублюють один одного («електронна інформаційна система» і «інформаційно-комунікаційна система», «комп'ютерна система» і «інформаційна система», «електронна комунікаційна мережа» і «комп'ютерна мережа»), або вживаються не в тому контексті («комп'ютерні дані» замість «цифрові (електронні) дані») тощо.

Водночас, при внесенні змін у КПК, які безпосередньо стосуються кіберзлочинності і доказових відомостей у цифровій (електронній) формі, хотілося щоб законодавець був послідовним і все ж таки вирішив проблематику цифрових (електронних) доказів. Так, ще у 2017 році в трьох процесуальних кодексах: Господарському процесуальному кодексі України (далі – ГПК), Цивільному процесуальному кодексі України (далі – ЦПК) та Кодексі адміністративного судочинства України (далі – КАСУ), з'явилася нова категорія – електронні докази. Під електронними доказами законодавцем розуміється 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), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі (ст. 96 ГПК, ст. 100 ЦПК, ст. 99 КАСУ відповідно) [4, 5, 6]. Проте, у КПК і в Кодексі України про адміністративні правопорушення їх визначення досі відсутнє.

Отже, цілком очевидно, що в умовах воєнного стану та збройної агресії рф проти нашої країни, внесення суттєвих змін до таких систе-

моутворюючих законодавчих актів як КПК – досить проблематичне. Здається, саме тому, законодавець, виходячи із нагальної необхідності забезпечення повного та неупередженого розслідування кримінальних проваджень, поки демонструє поступовий, але, водночас, не завжди послідовний підхід до змін в КПК на шляху цифровізації кримінального процесу та судочинства.

Список використаної літератури:

1. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки: Указ Президента Україні від 20 травня 2015 року № 276/2015. URL: https://zakon.rada.gov.ua/laws/show/276/2015#Text (дата звернення: 19.12.2022).

2. Про Стратегію розвитку системи правосуддя та конституційного судочинства на 2021–2023 роки: Указ Президента Україні від 11 червня 2021 року № 231/2021. URL: https://zakon.rada.gov.ua/laws/show/276/2015#Text (дата звернення: 19.12.2022).

3. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам: Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137–20 (дата звернення: 19.12.2022).

4. Господарський процесуальний кодекс України: Закон України від 06.11.1991 № 1798-XII (редакція від 06.11.2022). URL: https://zakon.rada.gov.ua/laws/show/1798–12 (дата звернення: 18.12.2022).

5. Цивільний процесуальний кодекс України: Закон України від 18.03.2004 № 1618-IV (редакція від 06.11.2022). URL: https://zakon.rada.gov.ua/laws/show/1618–15 (дата звернення: 22.12.2022).

6. Кодекс адміністративного судочинства України: Закон України від 06.07.2005 № 2747-IV (редакція від 06.11.2022). URL: https://zakon.rada.gov.ua/laws/show/1618–15 (дата звернення: 22.12.2022).

ВИСНОВОК СПЕЦІАЛІСТА У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЩОДО КІБЕРЗЛОЧИНІВ: НОРМАТИВНА ДУАЛЬНІСТЬ ТА ПРАКТИЧНА ДОЦІЛЬНІСТЬ

Неділько Ярослав Валентинович,
аспірант кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка

Одним із важливих видів використання спеціальних знань під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій (кіберзлочинів), є висновок спеціаліста.

Згідно ч. 1 ст. 71 КПК України спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками і може надавати консультації, пояснення, довідки та висновки під час досудового розслідування з питань, що потребують відповідних спеціальних знань і навичок. В етимологічному розумінні поняття «висновок» тлумачиться як остаточна думка про що-небуть, логічний підсумок, зроблений на основі спостережень, міркувань або розгляду певних фактів [1, с. 112]. У кримінальному процесуальному законодавстві відсутнє положення, що розкриває зміст терміну «висновок спеціаліста». Натомість, законодавець у ст. 300 КПК України зазначає, що висновок спеціаліста повинен відповідати вимогам, що ставляться до висновку експерта, зазначеним в ст. ст. 101–102 КПК України. Отже головна різниця між висновком експерта та спеціаліста полягає у суб'єкті надання такого висновку.

На особливу уваги заслуговують положення ст. 298–1 КПК України «Процесуальні джерела доказів у кримінальних провадженнях про кримінальні проступки», де зазначається, що процесуальними джерелами доказів у кримінальному провадженні про кримінальні проступки, крім визначених ст. 84 КПК України, на ряду з поясненням осіб, результатами медичного освідування, показаннями технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, є і висновок спеціаліста.

Далі законодавець застерігає, що зазначені у абз. 1 наведеної статті процесуальні джерела доказів, у тому числі і висновок спеціаліста, не мо-

жуть бути використані у кримінальному провадженні щодо злочину. При цьому зауважує, що *на підставі ухвали слідчого судді*, винесеної за клопотанням прокурора, висновок спеціаліста може використовуватися і у кримінальному провадженні щодо злочину,

Доречно зазначити, що віднесення законодавцем висновка спеціаліста до джерел доказів визвало бурхливу критику такого нововведення серед українського наукового співтовариства [2], [3], [4].

Вчені звертають увагу на процесуальні недосконалості, що стосуються висновка спеціаліста як джерела доказів за приписами ст. 298–1 КПК України. Насамперед порушується структура та логіка кодифікації норм кримінального процесуального законодавства: зазначені положення про джерело доказів вступають в протиріччя з главою 4 розділу І КПК України (докази і доказування), в якій чітко визначенні поняття та види доказів, критерії їх належності та допустимості [3, с. 92].

Крім того, таке нововведення ставить під сумнів доказове значення висновку спеціаліста у кримінальному провадженні, оскільки згідно ч. 2 ст. 298–4 КПК України висновок спеціаліста може бути перевірений висновком експерта за клопотанням прокурора про проведення експертизи. Тобто перевага надається висновку експерта [3, с. 91].

Не зважаючи на наведену критику з боку вітчизняних вчених, на нашу думку, враховуючи специфіку розслідування зазначених кримінальних правопорушень, висновок спеціаліста варто використовувати на вихідному етапі (до внесення відомостей до ЄРДР). Це сприятиме встановленню обставин, що можуть свідчити про вчинення кримінального правопорушення, а також слугувати підґрунтям для прийняття рішення про початок досудового розслідування. Вбачається за доцільне використовувати висновок спеціаліста і на наступних етапах розслідування.

У контексті зазначеного наведемо позицію ЄСПЛ щодо висновку спеціаліста. Зокрема, у справі «Пічугін проти Росії» Суд констатував, що відмова національних судів визнати звіти, підготовлені спеціалістами як докази, порушує принцип рівності сторін (п. 33). У зв'язку з несправедливим дослідженням доказів допущено порушення ст. 6 Конвенції [5].

У ході проведеного опитування прокурорів 55% із них вважають, що нехтування залученням спеціаліста та використанням його консультацій, пояснень, довідок та висновків негативно впливає на результати ефективного досудового розслідування зазначеної категорії кримінальних правопорушень [6].

Таким чином, під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), використання висновку спеціаліста суб'єктом розслідування дасть змогу проводити досудове розслідування в розумні строки та отримувати без зволікань необхідні докази.

Список використаної літератури:

1. Великий тлумачний словник сучасної української мови. Київ; Ірпінь, 2001. 1440 с.
2. Черненко А. П., Шиян А. Г. Висновок спеціаліста як процесуальне джерело доказів у кримінальному провадженні. *Матеріали науково-практичного семінару (ДДУВС, 29.05.2020).* С. 149–152.
3. Антонюк П. Є., Свобода Є. Ю., Михальчук Т. В. Висновок спеціаліста як джерело доказів у кримінальному провадженні: аналіз процесуальної спроможності. *Криміналістика і судова експертиза. Випуск 66.* С. 88–95. DOI: https://doi.org/10.33994/kndise.2021.66.10 (дата звернення 10.12.2022).
4. Коваленко А. В. Висновок спеціаліста як нове процесуальне джерело доказів у кримінальному провадженні (проблеми та перспективи). *Актуальні питання розвитку права та законодавства: наукові дискусії: матеріали міжнародної науково-практичної конференції*, м. Львів, 18–19 грудня 2020 р. Львів: Західноукраїнська організація «Центр правничих ініціатив», 2020. Ч. 2. С. 187–190
5. Case Pichugin v. Russia №38958/07. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–174061%22]} (дата звернення 101.2.2022)
6. Результати опитування прокурорів, що проводилось з 15 по 25 липня 2022 року. URL: https://forms.gle/pSPC5mdMt8qpwwSb8.).

КІБЕР-ІНФОРМАЦІЙНІ ПОСЯГАННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Нетеса Наталія Володимирівна,
кандидат юридичних наук, вчений секретар НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Стрімкий розвиток інформаційно-комунікаційної сфери, прискорення темпів цифрової трансформації держави, очікувана тенденція до зростання інтелектуальної складової комп'ютерних технологій попри значний корисний суспільно-економічний ефект, на жаль, має зворотний бік, що виявляється в активному використанні новітніх досягнень науки і техніки у кримінально протиправній діяльності, що безперечно підвищує технічний рівень реалізації інформаційних загроз.

Інформаційні кримінальні правопорушення – це достатньо великий масив кримінально протиправних діянь, що можуть вчинятися як з використанням кіберсередовища, так і поза ним. Саме тому, не зважаючи на всю привабливість пропозиції систематизувати правопорушення в інформаційній сфері шляхом об'єднання їх в один розділ Кримінального кодексу України «Кримінальні правопорушення проти інформаційної безпеки особи, суспільства, держави» [1, с. 16–18], виникає закономірне питання щодо практичної реалізації такої пропозиції. Вбачається, що тут важливого значення набуває правильне визначення пріоритетності об'єктів кримінально-правової охорони з урахуванням ступеня важливості тих чи інших інтересів та встановлення адекватних цьому ступеню важливості засобів їх кримінально-правового забезпечення [3, с. 127], адже цілком очевидно, що інформаційний простір і надалі буде ущільнюватися за рахунок потужних інформаційних потоків та подальшого розвитку новітніх інформаційно-комунікаційних технологій. Відповідно зростатиме й кількість кримінально протиправних посягань в інформаційному просторі. Підтвердженням цьому є зокрема те, що традиційні форми кримінально протиправної діяльності швидко адаптуються до сучасних можливостей, набуваючи ознак кіберзлочинності. Як зазначається у Стратегії кібербезпеки України однією із загроз кібербезпеці є поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень,

пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо [4]. Як наслідок, понад 80% кримінальних правопорушень містять цифровий компонент [2].

Викладене дає підстави говорити про те, що в масиві кримінально протиправних посягань, що вчиняються в інформаційному просторі, окрему відносно автономну групу становлять так звані кібер-інформаційні посягання, які можуть бути охарактеризовані як група кримінальних правопорушень, що містять певний кіберкомпонент, але при цьому пов'язані з різного роду обігом інформації, а також з інформаційним впливом на окремих осіб, їх групи, населення країни чи навіть світову спільноту. Методологічним підґрунтями для виокремлення такої групи діянь є уявлення про співвідношення базових категорії «кіберпростір» та «інформаційний простір». Визнаючи те, що кіберпростір є складовою інформаційного простору, при цьому вважаємо, що їх взаємодія не вичерпується уявленнями про співвідношення «частки» та «цілого». За низки обставин кіберпростір виступає своєрідним операційним базисом, що створює умови для вчинення діянь в інформаційному просторі, а отже, взаємозв'язок може бути представлений як система двох кіл, що перетинаються, і саме в області перетину якраз і перебувають ці так звані «кібер-інформаційні» посягання. Якщо перенести цю модель у систему координат кримінально-правової матерії, то можна говорити про випадки, коли предикатне діяння вчиняється у кіберпросторі і в такий спосіб забезпечує вчинення основного кримінального правопорушення – посягання на інформаційну безпеку. Наочним прикладом наведеного може бути ситуація, коли в результаті кібератаки на інформаційні медіаресурси на них розміщується інформація, змістом якої є виправдовування, визнання правомірною, заперечення збройної агресії рф проти України, а також глорифікація її учасників. Очевидно, що у цьому випадку кібератака є не самоціллю, а способом вчинення іншого кримінального правопорушення, поєднаного зі здійсненням деструктивного інформаційного впливу з метою викривлення уявлення громадськості про реальні події та посилення соціальної напруги серед населення України. Звісно, що і ця група кримінальних правопорушень так само не є одно-

рідною, і в ній можна виокремити принаймні дві підгрупи – це кібер-інформаційні діяння, що спрямовані на здійснення інформаційно-психологічного впливу, та кібер-інформаційні посягання, що не пов'язані з ним.

Розпочнемо аналіз спочатку з другої із названих груп кібер-інформаційних посягань. Класичним їх прикладом в умовах збройної агресії рф проти України може слугувати так званий кібершпіонаж, за якого у кіберпросторі або з його використанням здійснюється збір інформації щодо тих об'єктів, заподіяння шкоди яким матиме найбільший за масштабом руйнівний ефект. Сьогодні з упевненістю можна стверджувати, що інформацією, виток якої становить загрозу національній безпеці і відповідно предмет кібершпіонажу, є: відомості щодо розміщення, передислокації та просування підрозділів ЗС України; інформація стосовно наданих Україні державами-партнерами новітніх зразків озброєння, місць їх перебування та зберігання, складів боєприпасів до них; точні координати розміщення логістичних вузлів, якими здійснюється перекидання озброєння на передову; точні координати об'єктів критичної інфраструктури, об'єктів ВПК (у тому числі, які задіяні у ремонтно-відновлювальних роботах, модернізації та переобладнання як української, так захопленої російської військової техніки) тощо. При цьому найпоширенішими механізмами отримання та подальшої передачі вказаної вище інформації є: здійснення кібератак (причому як на державні інформаційно-комунікаційні ресурси, так і на персональні електронні пристрої користувачів), на які припадає понад 50%, а також активне використання можливостей такого компоненту кіберпростору, як соціальні мережі (насамперед «Facebook», «Instagram» і «Twitter») із заздалегідь створеними «фейковими» акаунтами і так званими «бот-мережами», а також мессенджери («Telegram», «Viber» та ін.). Так само до цієї групи кібер-інформаційних посягань, якщо вони вчиняються за допомогою інструментарію кіберпростору, можуть бути віднесені окремі форми державної зради (зокрема, шпигунство та надання допомоги в проведенні підривної діяльності проти України (ст. 111 КК)), несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення ЗСУ чи інших утворених відповідно до законів України військових формувань (ст. 114^2 КК) та ін.

Що ж стосується кібер-інформаційних діянь, що спрямовані на здійснення інформаційно-психологічного впливу, то їх існування здебільшого

зумовлене тими унікальними можливостями, що відкриваються внаслідок поєднання сучасних інформаційно-комунікаційних технологій з методами соціальної інженерії, що дозволяє маніпулювати не лише думкою окремих осіб, їх груп і цілих спільнот, а навіть процесом сприйняття та пізнання ними тих чи інших суспільних явищ. Поширеність таких кібер-інформаційних діянь суттєво зросла в умовах військової гібридної агресії рф проти України, невід'ємною складовою якої є інформаційна війна, яка спрямована проти інформаційного простору не лише України, а й фактично має транснаціональний характер, оскільки має своїм призначенням вплив на суспільну думку світової спільноти. При цьому основним середовищем ведення цієї війни, звісно, виступає кіберпростір як її операційний базис, який створює широкі можливості для протиправного впливу, що зумовлено такими його властивостями, як швидкість та масштабність одночасного поширення інформації, складність ідентифікації особи зловмисника та виявлення місця його знаходження, відсутність територіальних кордонів, відносно невелика затратність здійснених кібероперацій та ін. Як приклад, можна навести перші дні війни, коли операції інформаційного впливу, поєднані з потужними кібератаками, які фактично паралізували роботу державних інформаційних ресурсів і заблокували доступ населення до офіційних даних, стали чи не одним із головних засобів дестабілізації ситуації в Україні, оскільки були спрямовані на поширення паніки серед населення шляхом нав'язування думки про неможливість протистояти військовій агресії, зраду української влади власному народові, масову співпрацю прифронтових населених пунктів та прийняття ними «руського миру». Активно використовується кіберпростір й для деструктивної пропаганди та дезінформації шляхом розміщення відповідних матеріалів деструктивного та антидержавного характеру. Для цього так само можуть вчинятися попередні злами медійних вебсайбів або вебсайтів та інформаційних систем інтернет-провайдерів, але найчастіше використовуються ті ж самі соціальні мережі та мессенджер-канали, які об'єднують багатотисячну аудиторію підписників, що дозволяє ефективно поширювати інформацію деструктивного (маніпулятивного) характеру, яка викликає бурхливе обговорення порушених питань серед їх учасників, провокує панічні настрої, загострює соціальні протиріччя, викривляє погляди на перебіг бойових дій на окремих територіях України. У такий спосіб можуть вчинятися, зокрема, публічні заклики до повалення конституційного ладу

або захоплення державної влади (частини 2 та 3 ст. 109 КК); публічні заклики до посягань на територіальну цілісність України (ст. 110 КК); певні форми колабораційної діяльності (в частині публічного заперечення здійснення збройної агресії проти України та публічних закликів до різного роду співпраці з окупаційною владою (ч. 1 ст. 111^1 КК), а також освітній колабораціонізм в частині пропаганди подібних форм співпраці з державою-агресором (ч. 3 ст. 111^1 КК)); пропаганда війни (ст. 436 КК); виправдовування, визнання правомірною, заперечення збройної агресії РФ проти України та глорифікації її учасників (ст. 436^2 КК), публічні заклики до геноциду (ч. 2 ст. 442 КК) та ін.

Список використаної літератури:

1. Батиргареєва В. С. Модернізація кримінально-правової охорони інформаційного простору України. *Питання боротьби зі злочинністю*: зб. наук. пр. / редкол. : В. С. Батиргареєва та ін. Харків: Право, 2022. Вип. 43. С. 11–23.
2. Міжнародні експерти з протидії кіберзлочинності скоординували зусилля на форумі в Києві. URL: https://www.euam-ukraine.eu/ua/news/global-cybercrime-law-enforcement-experts-gathered-in-ukraine-to-share-knowledge-and-coordinate-efforts/.
3. Нетеса Н. В. Суспільні та приватні інтереси у кримінальному праві: до питання пошуку балансу. *Питання боротьби зі злочинністю*: зб. наук. пр. / редкол. : В. І. Борисов та ін. Харків: Право, 2017. Вип. 33. С. 123–137.
4. Про рішення Ради безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

НЕОДНОРІДНІСТЬ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ НА КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНУ ФОРМУ

Пашковський Микола Іванович,
кандидат юридичних наук, доцент, науковий співробітник
НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Оцифрування, цифровізація, діджиталізація та цифрова трансформація суспільного життя, зокрема кримінального судочинства – поняття, які ми чуємо практичного кожного дня, є новими для правової сфери і знаходяться в динамічному розвитку. Разом з тим, вони позначають різні явища. Розуміння їх змісту та розмежування є важливим для з'ясування форм (можливих форм) їх реалізації в кримінальному провадженні, а головне – меж такої реалізації, що позначається на стані правового регулювання.

Найпростішим поняттям є «оцифрування» (англ. – Digitization), під яким розуміється процес переходу від аналогової форми інформації до цифрової [1].

Поняття «цифровізація» (англ. – Digitalization) розуміється як процес використання цифрових технологій та інформації для трансформації бізнес-операцій: «Цифровізація – це використання цифрових технологій для зміни бізнес-моделі та надання нових можливостей для отримання прибутку та збільшення вартості; це процес переходу до цифрового бізнесу» [2]. Ключовими ознаками у цьому визначені є оцифрування процесу, а не інформації; отримання внаслідок цього додаткової вартості (додаткових можливостей); зміна звичайного порядку ведення діяльності (моделі), соціальної комунікації, що вимагає відповідних цифрових компетентностей. Одним із класичних проявів цифровізації є автоматизація окремих процесів за допомогою цифрових технологій (далі – ЦТ) та інформації.

Стосовно цифрової трансформації позиції розбіжні. Існує позиція, що оцифрування та цифровізація є двома типами цифрової трансформації [3] і з цієї позиції цифрова трансформація розуміється як будь-які зміни, що відбуваються в суспільстві або в окремому сегменті суспільної діяльності під впливом застосування цифрових технологій через оцифрування

та цифровізацію. Існує й інший погляд на цифрову трансформацію як на переосмислення певної структури на основі ЦТ, в такому випадку цифрова інформація мислиться як інший рівень, ніж оцифрування та цифровізація і знаходиться поза їх межами, оскільки вимагає наскрізних організаційних, а можливо і світоглядних змін, що має наслідком створення нової організаційної моделі, повністю заснованої на цифрових технологіях [4].

Якщо дивиться практичний аспект кримінального провадження, то стає зрозумілим, що усі три підходи наразі рідко застосовуються ізольовано. Як правило, оцифрування та цифровізація поєднуються. Тому можна надавати характеристику певного впливу на кримінальне провадження ЦТ через більшу ємність у ній того чи іншого рівня.

Так, близькими до оцифрування є такі інститути (субінститути) кримінального провадження, пов'язані з застосуванням ЦТ:

– електронна форма початку досудового розслідування через внесення інформації про вчинення кримінального правопорушення до ЄРДР (ст. 214 КПК);

– внесення до ЄРДР процесуальних рішень у кримінальному провадженні (ч. 4 ст. 218, ч. 4 ст. 278, ч. 4 ст. 280, ч. 3 ст. 282, ч. 2 ст. 281, ст. 283 КПК);

– застосування технічних засобів фіксування кримінального провадження (ст. 107 КПК);

– використання електронних документів як джерела доказів (ст. ст. 84, 99 КПК);

– використання сучасних телекомунікаційних засобів для виклику особи (ст. ст. 134 КПК);

– проведення ряду слідчих (розшукових) дій, судових засідань у режимі відео або телефонної конференції (ст. 232, 336, 615 ч. 12 КПК);

– оприлюднення судових рішень в ЄДРСР (ст. 535 КПК).

Так, близькими до цифровізації є такі інститути (субінститути) кримінального провадження, пов'язані з застосуванням ЦТ та автоматизацією (оцифруванням процесуальних алгоритмів):

– розподіл матеріалів кримінальних проваджень між суддями, визначення присяжних, надання особам інформації про стан розгляду матеріалів кримінального провадження, реєстрація руху кореспонденції через ЄСІТС (ст. 35 КПК);

– автоматизація окремих контрольних механізмів на основі ІТКСДР (ст. 106–1 КПК), лише застосовно до НАБУ, САП, ВАКС;

– автоматизація кримінальної статистики та окремих контрольних механізмів на основі ЄРДР (ст. 214 КПК).

Вияви цифрової трансформації в кримінальному провадження полягають у зміні парадигми кримінального судочинства, наприклад, шляхом заміни частини функцій, властивих слідчому, прокурору чи судді, ЦТ, зокрема алгоритмічними системами, наприклад, штучним інтелектом. Прикладом реалізації може бути застосування штучного інтелекту в діяльності судів КНР [5].

Підхід до відмежування трьох рівнів застосування ЦТ в суспільному житті, зокрема в кримінальному судочинстві: оцифрування, цифровізація та цифрова трансформація уявляється більш правильним, ніж об'єднання оцифрування та цифровізації під «парасолькою» цифрової трансформації, оскільки дозволяє більш правильно відобразити процеси застосування ЦТ, їх цілі (досяжність) та межі.

Проведені дослідження вказують, що у кожній національній правовій системі існує свій вектор використання цифрових технологій у кримінальному судочинстві та набір інструментів, що використовуються, цей вектор, а також набір інструментів можуть з часом змінюватися, що впливає на правову регламентацію процесуальної діяльності [3].

Різні рівні застосування ЦТ в кримінальному провадженні вимагають відмінного підходу до їх правової регламентації в КПК. Очевидно, що цифровізація кримінального провадження через використання автоматизації неможлива без упорядкування кримінально-процесуальної діяльності як відповідних алгоритмів, що можуть бути оцифровані. Обумовлена алгоритмічністю природи кримінального провадження автоматизація має позитивно вплинути на ефективність кримінально-процесуальної діяльності та негативно на корупційні ризики, які супроводжують судочинство [6, с. 28, 193; 7].

Міжнародний збройний конфлікт, викликаний агресією російської федерації проти України, супроводжується масовим вчиненням російськими військовими міжнародних злочинів, документування та розслідування яких (як і в ситуаціях інших сучасних масштабних збройних конфліктів) засновано на широкому використанні інформаційних технологій (мова йде не лише про використання інформації з відкритих джерел). Надзвичайно великий обсяг насамперед цифрової та оцифрованої інформації, що генерується збройним конфліктом (навколо нього) та збирається під час розслідувань, вимагає належного забезпечення її збері-

гання, аналізу та обміну між зацікавленими правоохоронними органами. Очевидно, що спроможність України розслідувати міжнародні злочини залежить від належного технологічного забезпечення таких розслідувань та адекватної правової регламентації (зокрема, щодо електронних доказів та поводження з ними, використання ІТ в процесуальній діяльності). Результати досудових розслідувань кримінальних проваджень в Україні за ст. 438, 442 КК (докази) можуть бути використані іноземними юрисдикціями або МКС, тому документування подій відповідних подій повинно відбуватися з урахуванням міжнародних стандартів (як загальних стандартів, наприклад Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних, так і стандартів, запропонованих МКС), що вимагає напрацювання відповідних алгоритмів процесуальної діяльності з можливістю інтеграції таких алгоритмів до інформаційно-телекомунікаційної системи досудового розслідування.

Список використаної літератури:

1. Definition of Digitization – Gartner Information Technology Glossary. *Gartner*. URL: https://www.gartner.com/it-glossary/digitization/ (date of access: 28.12.2022).
2. Definition of Digitalization – Gartner Information Technology Glossary. *Gartner*. URL: https://www.gartner.com/en/information-technology/glossary/digitalization (date of access: 28.12.2022).
3. Seepma A. P., de Blok C., Van Donk D. P. Designing digital public service supply chains: four country-based cases in criminal justice. *Supply Chain Management: An International Journal*. 2020. Ahead-of-print, ahead-of-print. URL: https://doi.org/10.1108/scm-03-2019-0111 (date of access: 28.12.2022).
4. Definition of Digital Business Transformation – Gartner Information Technology Glossary. *Gartner*. URL: https://www.gartner.com/en/information-technology/glossary/digital-business-transformation (date of access: 28.12.2022).
5. Усіх суддів Китаю підключили до штучного інтелекту. *Газета «Закон і Бізнес». Законодавство, влада, права людини*. URL: https://zib.com.ua/ua/152143.html (дата звернення: 28.12.2022).
6. Каланча І. Г. Електронне кримінальне судочинство: передумови виникнення, сучасний стан та перспективи розвитку: монографія. Харків : Право, 2018. 240 с.
7. Шило О. Г., Глинська Н. В. Алгоритмізація кримінального провадження як антикорупційний стандарт кримінального процесуального законодавства. *Митна справа*. 2013. №2. С.137–145.

ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ ПРИ ПРОВЕДЕННІ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ СЛІДЧИМИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ (ПРОБЛЕМНІ ПИТАННЯ)

Погорецький Микола Миколайович,
кандидат юридичних наук, доцент кафедри кримінального права і кримінології Національної академії служби безпеки України

Серед гуманітарних цінностей суспільства у правовій державі, людина та її права займають центральне місце. Конституції демократичних правових держав визнають невідчужуваність і недоторканність прав людини. Підтримуючи цю концепцію, і орієнтуючись на прогресивні європейські ідеї про статус людини, Конституція України закріпила положення про те, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються найвищою соціальною цінністю, а утвердження прав людини є головним обов'язком держави.

Важливе місце у розслідуванні тяжких та особливо тяжких злочинів посідають негласні слідчі (розшукові) дії (НСРД), які є основними засобами отримання доказів у кримінальних провадження про зазначені злочини. Водночас, як свідчать результати аналізу матеріалів практики, НСРД є нерідко й найпоширенішими засобами порушення прав та свобод людини під час проведення досудового розслідування.

Так, відповідно до ч. 1 ст. 290 КПК України, визнавши зібрані під час досудового розслідування докази достатніми для складання обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру слідчий зобов'язаний повідомити підозрюваному, його захиснику, законному представнику та захиснику особи, стосовно якої передбачається застосування примусових заходів медичного чи виховного характеру, про завершення досудового розслідування та надання доступу до матеріалів досудового розслідування.

Відповідно до зазначеної статті прокурор, або слідчий за його дорученням, зобов'язаний надати доступ до матеріалів досудового розслідування, які є в його розпорядженні, у тому числі будь-які докази, які самі по собі або в сукупності з іншими доказами можуть бути використані для доведення невинуватості або меншого ступеня винуватості обвинуваченого, або сприяти пом'якшенню покарання.

Водночас, прокурор або слідчий за його дорученням зобов'язаний надати доступ та можливість скопіювати або відобразити відповідним чином будь-які речові докази або їх частини, документи або копії з них. При цьому, надання доступу до матеріалів включає в себе можливість робити копії або відображення матеріалів.

Однак, відповідно до ч. 3 ст. 254 КПК України Заходи щодо захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій» виготовлення копій протоколів про проведення негласних слідчих (розшукових) дій органами Служби безпеки України та додатків до них не допускається.

Зазначена норма у статті 254, частинах 2 та 3 передбачає лише можливість ознайомлення з матеріалами НСРД в порядку, передбаченому статтею 290 КПК України, а також попередження особи, захисника, інших осіб, які мають право на ознайомлення з протоколами НСРД про кримінальну відповідальність за розголошення отриманої інформації.

Як приклад, ухвалою Комсомольського районного суду м. Херсона (справа №667/4283/14-к) відмовлено у задоволенні скарги ОСОБА_1, на бездіяльність слідчого відділу прокуратури Херсонської області щодо ненадання скаржнику можливості копіювання матеріалів негласних слідчих (розшукових) дій, проведених органами Служби безпеки України, та додатків до них, які містяться у матеріалах кримінального провадження №42014230000000066.

Суд обґрунтував відмову у задоволенні скарги тим, що КПК України забороняє роботи копії або відображення матеріалів НСРД, проведених органами Служби безпеки України відповідно до ст. 254 КПК України. При цьому суд вважає, що вказана стаття, виходячи з її змісту, також регулює відносини сторін кримінального провадження на стадії досудового розслідування, зокрема передбачені ст. 290 КПК України.

Водночас, суд приходить до переконання, що норми ст. 254 КПК України є спеціальними нормами, порівняно із положеннями ст. 290 КПК України, що регулюють спірні, розглядувані судом правовідносини, а тому саме норми ст. 254 КПК України і підлягають застосуванню у розглядуваному судом випадку. Таким чином, суд приходить до переконання про відсутність правових підстав до задоволення розглядуваної судом скарги.

Другою обставиною, що призводить до порушення прав людини, є допущені помилки при складанні протоколів про проведення НСРД

органами Служби безпеки України. Так, відповідно до ч. 1. ст. 252 КПК України фіксація ходу і результатів НСРД повинна відповідати загальним правилам фіксації кримінального провадження, передбаченим КПК України. При цьому, як проведення, так і оформлення результатів НСРД може фіксуватися за допомогою технічних та інших засобів, проте, про фіксування ходу і результатів НСРД за допомогою технічних засобів зазначається у протоколі, який складається за результатами проведення НСРД.

До протоколу за результатами проведення НСРД, в разі необхідності долучаються додатки, якими можуть бути спеціально виготовлені копії, зразки об'єктів, речей і документів; письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії; стенограма, аудіо-, відеозапис процесуальної дії; фото-таблиці, схеми, зліпки, носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу.

Особливу увагу слід звернути на оформлення додатків, адже вони є невід'ємною частиною протоколу, а тому повинні бути належним чином виготовлені, упаковані з метою надійного збереження, а також засвідчені підписами слідчого, прокурора, спеціаліста, інших осіб, які брали участь у виготовленні та/або вилученні таких додатків.

На практиці, у порушення прав людини, досить часто при складанні протоколів про проведення НСРД виявляються наступні помилки: невідповідність дати і часу проведення НСРД фактичним обставинам справи, тобто складання протоколу про проведення НСРД не в день їх фактичного проведення; розбіжності або неточності в анкетних даних учасників, в тому числі понятих; відсутність у протоколі про проведення НСРД окремих із перед- бачених ст. 104 КПК України відомостей.

По-третє, не повідомлення осіб, щодо яких проводилися НСРД. На практиці, у 75% проведення НСРД особи, конституційні права яких були тимчасово обмежені під час проведення НСРД, а також підозрюваний, його захисник, у порушення ст. 253 КПК України, не були письмово повідомлені прокурором або за його дорученням слідчим про таке обмеження, або були повідомлені із порушенням строків повідомлення.

Наприклад, Южноукраїнським міським судом Миколаївської області при розгляді кримінального провадження №12013160080000047 по обвинуваченню ОСОБА_1, ОСОБА_2, у вчиненні кримінального правопорушення за ч. 2 ст. 28, ч. 1 ст. 203–2 КК України було відмовлено

у задоволенні клопотання прокурора про призначення у кримінальному провадженні №12013160080000047 комп'ютерно-технічної експертизи та експертизи звуку та відеозапису.

Дане клопотання прокурор мотивує тим, що в ході розгляду кримінального провадження ним долучено в якості доказів протокол №63/11-2419т від 27.05.2013 за результатами проведення негласних слідчих (розшукових) дій – зняття інформації з транспортних телекомунікаційних мереж (електронних інформаційних систем) за абонентським номером, яким користується ОСОБА_1, а також додаток до цього протоколу – диск для лазерних систем зчитування DVD-R №75т/13 від 18.03.2013.

Однією із причин відмови слідчого судді у задоволенні клопотання стало не залучення в якості письмового доказу прокурором і письмового повідомлення обвинуваченому ОСОБА_2 та його захиснику щодо втручання в його особисте та сімейне життя з приводу тимчасових обмежень, які гарантуються Конституцією України та ст. 8 Європейської Конвенції з прав людини і основоположних свобод, що не відповідає практиці ЄСПЛ.

По-четверте, відсутність у матеріалах кримінального провадження ухвал слідчого судді про надання дозволу на проведення НСРД.

Слід зазначити, що на практиці, як правило, матеріали кримінального провадження не містять ухвали суду про надання дозволу на проведення негласних слідчих (розшукових) дій, а отже, вони і не відкриваються стороною обвинувачення стороні захисту.

Крім того, трапляються випадки, коли навіть протокол про проведення НСРД не містить інформації про дату ухвали суду про надання дозволу на проведення НСРД, прізвище, ім'я та по батькові слідчого судді, що надав цю ухвалу, тобто інформацію про законні підстави проведення НСРД.

В результаті цього підозрюваному, обвинуваченому та його захисникові досить складно побудувати лінію захисту та перевірити законність проведення НСРД, а також чи були порушені його права, адже вони навіть не в змозі перевірити зміст ухвали слідчого судді про дозвіл на проведення НСРД органами Служби безпеки України.

Список використаної літератури:

1. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія. Х.: Арсіс, ЛТД, 2007. 576 с.

2. Погорецький М. А., Сергєєва Д. Б. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи : поняття, сутність і співвідношення. Боротьба з організованою злочинністю і корупцією (теорія і практика) : науково-практичний журнал. К., 2014. Спеціальний випуск 2 (33). С. 137–141.
3. Шерудило В. О. Процесуальний порядок проведення негласних слідчих (розшукових) дій, пов'язаних з втручанням у приватне спілкування Процесуальний порядок проведення негласних слідчих (розшукових) дій, пов'язаних з втручанням у приватне спілкування. автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, НАВС. 2018. 20 с.
4. Нечай В. В. Проведення негласних слідчих (розшукових) дій під час розслідування податкових злочинів, що вчиняються організованими групами: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» Харків, 2019. 20 с.

УЧАСТЬ ОРГАНІВ ПРОКУРАТУРИ В ПРОЦЕСАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ (ОРГАНІЗАЦІЙНИЙ АСПЕКТ)

Подкопаєв Сергій Васильович
доктор юридичних наук, доцент, старший науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

У сучасних умовах стрімкого розвитку інформаційних технологій одним із стратегічних векторів удосконалення кримінальної процесуальної діяльності є перехід на електронну форму кримінального провадження. Втім питання полягає не лише в модернізації робочих процесів, підвищенні ефективності процесуальної діяльності, але й в реальній здатності до опрацювання великих масивів інформації, яка зберігається в паперовому вигляді в територіально різних регіонах країни. В ситуації наявного військового протистояння виключається можливість оперативного вивчення матеріалів кримінального провадження, дослідження формальних вимог до оформлення процесуальних документів та дотримання необхідних процесуальних вимог, порушення яких може нівелювати результати проведених слідчих дій та отриманих доказів. До того ж складними, а інколи й неможливими залишаються координація роботи великих груп слідчих та прокурорів у кримінальних провадженнях щодо воєнних злочинів; дослідження ефективності діяльності як окремих працівників, так і сформованих за напрямками роботи груп; відслідковування строків та якості виконання поставлених завдань, аналіз перспективності кримінальних проваджень з точки зору подальшого обвинувачення в національних та міжнародних судах.

У листопаді поточного року, під час засідання міжвідомчої робочої групи, яка опікуватиметься розробленням плану реформування органів правопорядку (як частини сектору безпеки й оборони України – *С. П.*), Генеральний прокурор назвав цифровізацію та впровадження електронної системи управління кримінальними провадженнями однією з стратегічних задач такої реформи [1]. Раніше, запровадження системи електронного кримінального провадження та інших актуальних інформаційних технологій визначено в якості одного із завдань у Стратегії розвитку прокуратури на 2021–2023 роки, затвердженій наказом Генерального

16.10.2020 р. № 489. Фактично це стратегічний пріоритет розвитку прокуратури, що розглядається в контексті «удосконалення методів і заходів забезпечення високого рівня якості реалізації конституційних функцій прокуратури» (п. 2.1.2. Стратегії) [2].

Органи прокуратури не залишаються осторонь процесів модернізації своїх робочих процесів. Конкретні кроки, спрямовані на розробку та впровадження системи електронного кримінального провадження були зроблені ще до доповнення Кримінального процесуального кодексу України (далі – КПК України) новою ст. 106[1] (Інформаційно-телекомунікаційна система досудового розслідування) [3].

Першим кроком до впровадження системи електронного кримінального провадження в країні було створення з 20.11.2012 р. на виконання п. 22 Перехідних положень КПК України Єдиного реєстру досудових розслідувань [3]. Ним переведено в електронний формат початок досудового розслідування, запроваджено фіксацію, прийнятих у кримінальному провадженні процесуальних дій та рішень, у тому числі з можливістю прикріплення копій документів в електронному вигляді. Власником і розпорядником цієї системи є держава в особі Офісу Генерального прокурора [4].

Наказом Генерального прокурора України від 13.03.2018 р. № 41 з метою забезпечення єдності інформаційного поля органів кримінальної юстиції та підвищення ефективності взаємодії між сторонами кримінального провадження в Генеральній прокуратурі України була створена робоча група з розробки заходів щодо запровадження електронного кримінального провадження. Перед нею стояло завдання з підготовки відповідного плану заходів [5].

Слід відмітити, що фактично відповідні робочі групи (як відомчі, так і міжвідомчі) останнім часом створювалися кожним із Генеральних прокурорів. Це може бути пов'язано з особливостями протікання процесу реформи прокуратури в країні, зміною керівництва системи прокуратури тощо.

З метою підготовки пропозицій щодо шляхів запровадження електронного кримінального провадження наказом Генерального прокурора від 21.02.2020 р. № 104 створено міжвідомчу робочу групу з питань запровадження електронного кримінального провадження. Перед нею стояли завдання щодо підготовки та ухвалення концепції запровадження електронного кримінального провадження; сприяння підготовці технічного

завдання, розробки та запровадження в роботу електронного кримінального провадження [6].

Такі ж завдання були покладені і на міжвідомчу робочу групу з питань запровадження електронного кримінального провадження, створену наказом Генерального прокурора від 12.01.2021 р. №2 [7]. Результатом її роботи стала підготовка проєкту Концепції запровадження інформаційно-телекомунікаційної системи досудового розслідування, єдиної для усіх органів досудового розслідування. Він донедавна розглядався в якості стратегічного документа та перебував на вивченні і опрацюванні в галузевих підрозділах Офісу Генерального прокурора, відповідних органах досудового розслідування, а спільно з ДП «Інфотех» розроблювалося технічне завдання для реалізації його положень.

Поряд із цим, спільним наказом Національного антикорупційного бюро України (далі – НАБУ) та Офісу Генерального прокурора від 24.11.2021 р. затверджено Тимчасове положення про інформаційно-телекомунікаційну систему досудового розслідування «іКейс» та розпочато спільну дослідну експлуатацію системи в НАБУ і Спеціалізованій антикорупційній прокуратурі (далі – САП) Офісу Генерального прокурора [8]. Невдовзі, спільним наказом НАБУ, Офісу Генерального прокурора, Ради суддів України та Вищого антикорупційного суду від 15.12.2021 р. розпочато використання цієї системи в НАБУ і САП та затверджено Положення про інформаційно-телекомунікаційну систему досудового розслідування «іКейс» [9].

І нарешті наказом Генерального прокурора від 12.12.2022 р. №279 в Офісі Генерального прокурора була утворена нова робоча група, на яку покладено завдання забезпечити підготовку концепції цифрової трансформації процесів організації роботи органів прокуратури та досудового розслідування, а також підготовку проєктів нормативних документів для впровадження цієї концепції.

Підсумовуючи можна констатувати, що до останнього часу в органах прокуратури існувало декілька паралельних процесів, пов'язаних із розробкою (або впровадженням) системи електронного кримінального провадження:

(а) пілотний запуск системи управління кримінальним провадженням *(eCase)* (з 30 квітня 2020 року) у САП (а також у НАБУ та Вищому антикорупційному суді) [10]. Розробка цієї системи розпочалася ще у 2019 році за технічної, експертної та фінансової підтримки Антикорупційної

ініціативи Європейського Союзу в Україні (EUACI), а 16.12.2021 р. детективи НАБУ та прокурори САП зареєстрували перше кримінальне провадження в eCase [11]. Ця система побудована на базі вже готових модулів пропрієтарного програмного продукту вірменської компанії Synergy [12, с. 7]

(б) опрацювання проєкту Концепції запровадження інформаційно-телекомунікаційної системи досудового розслідування, єдиної для усіх органів досудового розслідування (крім НАБУ), розробленого міжвідомчою робочою групою створеною згідно наказу Генерального прокурора від 12.01.2021 року №2 [7], розробку технічного завдання на основі якої здійснювало ДП «Інфотех»;

(в) опрацювання проєкту Концепції системи електронного кримінального провадження (єдиної електронної Системи управління кримінальними провадженнями «СМЕРЕКА» – *С. П.*), розробленого консалтинговою компанією CIVITTA на замовлення Консультативної місії Європейського Союзу (EUAM Ukraine) [12; 13]. Остання на сьогодні розглядається в якості найбільш вірогідної для впровадження системою, робота над якою триває.

Список використаної літератури:

1. В Офісі Генпрокурора обговорили підготовку стратегічного плану реформування органів правопорядку як частини сектору безпеки й оборони України. 17.11.2022. URL: https://www. gp. gov. ua/ua/posts/v-ofisi-genprokurora-obgovorili-pidgotovku-strategicnogo-planu-reformuvannya-organiv-pravoporyadku-yak-castini-sektoru-bezpeki-i-oboroni-ukrayini
2. Стратегія розвитку прокуратури на 2021–2023 роки: затверджено наказом Генерального прокурора 16 жовтня 2020 року №489. URL: https://www. gp. gov. ua/ua/posts/strategiya-rozvitku-prokuraturi-na-2021–2023-roki
3. Кримінальний процесуальний кодекс України від 13 квітня 2012 року №4651-VI. URL: https://zakon. rada. gov. ua/laws/show/4651–17#Text
4. Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення: затверджено наказом Генерального прокурора від 30 червня 2020 року №298. URL: https://zakon. rada. gov. ua/laws/show/v0298905-20#n11
5. Про утворення робочої групи з розробки заходів щодо запровадження електронного кримінального провадження: наказ Генерального прокурора України від 13 березня 2018 року №41. URL: https://old. gp. gov. ua/ua/file_downloader. html?_m=fslib&_t=fsfile&_c=download&file_id=204339

6. Про створення міжвідомчої робочої групи з питань запровадження електронного кримінального провадження: наказ Генерального прокурора від 21 лютого 2020 року № 104. URL: https://www. gp. gov. ua/userfiles/1_nakaz__104_vid_21_02_2020. docx
7. Про створення міжвідомчої робочої групи з питань запровадження електронного кримінального провадження: наказ Генерального прокурора від 12 січня 2021 року № 2. URL: https://old. gp. gov. ua/ua/file_downloader. html?_m=fslib&_t=fsfile&_c=download&file_id=210920
8. Тимчасове положення про інформаційно-телекомунікаційну систему досудового розслідування «іКейс»: затверджено наказ Національного антикорупційного бюро України, Офісу Генерального прокурора від 24 листопада 2021 року № 164/378. URL: https://old. gp. gov. ua/ua/file_downloader. html?_m=fslib&_t=fsfile&_c=download&file_id=214899
9. Положення про інформаційно-телекомунікаційну систему досудового розслідування «іКейс»: наказ Тимчасово виконуючого повноваження Директора Національного антикорупційного бюро України, Генерального прокурора, Голови Ради суддів України, Голови Вищого антикорупційного суду від 15 грудня 2021 року № 175/390/57/72. URL: https://old. gp. gov. ua/ua/file_downloader. html?_m=fslib&_t=fsfile&_c=download&file_id=215240
10. Кримінальні провадження в Україні переводять в електронний формат. 06.04.2020 р. URL: https://www. rbc. ua/ukr/news/ugolovnye-proizvodstva-ukraine-perevodyat-1586169699. html
11. НАБУ та САП зареєстрували перше кримінальне провадження в системі eCase: URL: https://nabu. gov. ua/novyny/nabu-ta-sap-zareyestruvaly-pershe-kryminalne-provadzhennya-v-systemi-ecase
12. CIVITTA. Концептуальна записка. 2022. 12 с.
13. Розробка системи електронного кримінального провадження для Офісу Генерального прокурора. Липень 2022. CIVITTA. Alkalon. EUAM Ukraine. 14 с.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ СУДОЧИНСТВІ УКРАЇНИ

Рєпіна Юлія Сергіївна,
кандидат економічних наук, доцент, науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України

Стрімкий розвиток інформаційних технологій (далі – ІТ) у другій половині минулого століття та винаходи, які пов'язані з їх впровадженням, що з'явились протягом останніх трьох-чотирьох десятиліть повсюдно поширюють занадто великі очікування від використання Штучного інтелекту (далі ШІ) – однієї із них, зокрема у судах. Проте при дослідженні потенціалу і ризиків ШІ для правосуддя слід спиратися на поточний рівень досягнень інформатики у цьому напрямі. І ще одне зауваження стосується того, шо застосування ІТ, у тому числі ШІ, не є однаковим для всіх судових справ. Втім використання ШІ сприяє зменшенню складності, що є основою судових процесів, незалежно від предмета судового розгляду [1]. Надзвичайно важливо визначити напрями використання ШІ при роботі судів і суддів, які б відповідали стандартам права на справедливий суд, наприклад, в контексті статті 6 Конвенції про захист прав людини і основоположних свобод. Також вимагають вивчення ризиків для правосуддя в результаті використання ШІ та винаходу механізму їх запобігання.

У науковій літературі зустрічається багато визначень поняття ШІ, при цьому кожне із них виділяє певний аспект відповідно до теми дослідження, але більшість зорієнтовані навколо концепції створення комп'ютерних програм або машин, здатних до поведінки, яку ми вважали б розумною, якби її демонстрували люди [2, с. 1]. ШІ офіційно з'явився в 1956 р. в Дармутському університеті, коли вчені спробували змоделювати нейрони за допомогою математичних функцій. Головна ідея полягала в тому, що нейронні мережі дозволять створити штучний мозок. Д. Маккарті, який вважається автором терміну ШІ , описав цей процес у 1955 році як процес, що полягає в тому, «щоб змусити машину поводитися у спосіб, який можна назвати розумним, ніби це поведінка людина» [2, с. 1; 3]. Однак, на думку Л. Джулія – експерта в галузі ШІ, «люд-

ський мозок так не працює, дослідження було засноване на хибному припущенні. Ці вчені створили не штучний інтелект (як його назвали), а доповнений інтелект, тобто інструмент поліпшення нашого власного інтелекту. З цього погляду ШІ з'явився в 1642 р., коли Б. Паскаль винайшов паскаліну (Калькулятор Паскаля)» [4].

При цьому важливо встановити, визначаючи людський інтелект як міру того, шо виконує ШІ. Інтелект – це здатність до абстрактного, логичного і послідовного міркування, до відкриття, встановлювення і бачення кореляції, до вирішування проблеми, відкриття правил в здавалося б невпорядкованому матеріалі за допомогою наявних знань, до вирішування нових завдань, гнучкого адаптування до нових ситуацій й самостійного навчання, без потреби у чітких та повних настановах [1].

Втім Л. Джулія, який є також співатором Сірі (Siri) (на тепершній час, можливо, найбільшого проекту ШІ в світі (принаймні, за кількістю користувачів), заперечує існування ШІ. Наприклад, на його думку, коли у 1997 р. машина (Deep Blue) вперше обіграла людину в шахи, то це не інтелект, а розрахунок та пам'ять [4]**.** Проте ШІ привертає великий інтерес спеціалістів із різних галузей знань, які наголошують на його існуванні в багатьох різних формах, наприклад, розпізнавання мови або розпізнавання зображень. Л. Джулія пропонує взяти за приклад розпізнавача котів: скільки зображень котів потрібно нам як людям, щоб розпізнавати їх увесь час, навіть у темряві чи намальовані Пікассо? Зважаючи на все, нам потрібно всього два, тоді як машині потрібно близько 100 000 [4]. Тобто, ШІ, щоб працювати, потребує «Великих даних (Big Data)». Ми спостерігаємо, шо внаслідок розвитку Інтернету було створено величезні бази даних, які вимагають машинного навчання. Але глибоке навчання, при якому сама технологія навчається, все що належить до майбутнього.

Робота суда і судді полягає в обробці інформації, незалежно від спеціалізації та інстанційності суда. Проте не вся інформація потребує складної кастомизації [1]. В адміністративних і цивільних справах (не складних, з передбачуваним результатом, коли суддя затверджує домовленість сторін, наприклад, у справах про розлучення, про припинення трудових відносин тощо) судове рішення створюється переважно на комп'ютері на основі наданих даних. Обробку таких справ принаймні часткову можна автоматизувати за допомогою ШІ. Для будь-якої категорії справ, включаючи кримінальні, необхідність використання електро-

нних базах даних (знань), які надають швидкий та легкий доступ до нормативно-правових актів, судової практики, рішень Європейського суду з прав людини тощо із застосуванням ШІ для пошуку, сортування важливої для вирішення справи інформації здатне значною мірою спростити роботу судді.

Наприклад, «Розумний суд SoS» (система систем) – система, заснована на технології машинного навчання підключається до робочого столу кожного працюючого судді у Китаї, автоматично переглядає судові справи на наявність посилань, рекомендує закони та постанови, складає проекти юридичних документів та виправляє передбачувані людські помилки, якщо такі є у судовому рішенні [5].

Ще один приклад використання ШІ, але вже у кримінальному судочинстві, також із Китаю. Китайська академія наук на замовлення прокурора Шанхаю розробила програму, яка використовуючи ШІ може вивчати кримінальні справи та висувати звинувачення. Для того, щоб натренувати алгоритми розробники створили модель з використання 17 тис. справ, що розглядалися прокуратурою з 2015 по 2020 рік. Розробники заявляють, що програма може ухвалити правильне рішення про висунення звинувачення у 97% випадків на підставі знайомства з матеріалами справи. Для цього вона аналізується приблизно по тисячі параметрів. Поки що програма натренована для роботи з вісьмома типами злочинів, які найчастіше трапляються в Шанхаї, до них відносяться, зокрема, дрібні крадіжки, незаконні азартні ігри, навмисні тілесні ушкодження, шахрайство та ін. Розробники програми планують, що в майбутньому вона навчиться розпізнавати й менш розповсюджені злочини, а також висувати одразу кілька звинувачень одному підозрюваному [6].

Отже питання, яке постає перед правосуддям, стосується передачі повноважень від людини машинам. Величезна кількість публікацій про ШІ постійно використовує риторичну фігуру пролепсису: вимагається вірити сьогодні в реальність делегування повноважень машинам, яке відбудеться тільки завтра [7, с. 110–111]. «Якщо машина буде здатною завтра «розкопати» в декілька секунд сукупність схожих випадків та винесених рішень, пристосовуючи в максимально точний спосіб своє рішення до окремих випадків, чи не зможемо зекономити на неповоротких процедурах та усунути роки відтерміновування справи? В дійсності штучний інтелект судитиме краще, ніж особа, піддана впливу своєї ідеології та контексту виголошення рішення. В науці царює критерій від-

творюваності досліду. Чи не має бути критерієм правосуддя критерій відтворюваності судового рішення? Останнє не має залежати ні від особи, яка судить, ні від обставин» [7, с. 110–111].

Проте є інша точка зору, за якою звинувачення, висунуті ШІ навченим лише на прецедентах, можуть бути помилковими, адже не враховують динаміку соціального життя. На думку Д. Рейлінг – судді у відставці та незалежного судового консультанта з ІТ, «алгоритм не може використовуватися як рецепт (припис), тобто комп'ютер нічого не призначає та не може приймати самостійне рішення. Користувачі мають знати та розуміти, що робить ШІ, також вони повинні контролювати вибір, який вони роблять. Це означає, що користувачі повинні мати здатність без труднощів відхилитися від машинного результату» [1].

ШІ та його використання в сфері правосуддя та кримінальному судочинстві активно обговорюється правничою спільнотою як в Україні, так і в світі. Проявом серйозного ставлення до проблеми використання ШІ є наразі понад двадцять п'ять документів присвячені етичним принципам використання ШІ, які підготовлені, зокрема, IEEE – найбільшою в світі технічною професійною асоціацією по просуванню технологій, Європейським Союзом та Радою Європи. Європейська комісія з ефективності правосуддя Ради Європи у грудні 2018 р. прийняла Європейську хартію етичного використання ШІ у судових системах та суміжному середовищі. У грудні 2020 р. була схвалена Концепція розвитку штучного інтелекту в Україні, в т.ч. в сфері правосуддя. Резюмуючи, відмітимо, що використання ШІ видається перспективним напрямом розвитку вітчизняного судочинства, в тому числі і кримінального, проте потребує подальших практичних розробок і наукових досліджень.

Список використаної літератури:

1. Reiling A. D. (Dory) Courts and Artificial Intelligence. *International Journal for Court Administration 8,* 2020, 11 (2) (November 24, 2020). DOI: https://doi.org/10.36745/ijca.343, Available at SSRN: https://ssrn.com/abstract=3736411 (дата звернення: 12.02.2022)

2. Kaplan J. Artificial Intelligence: What Everyone Needs to Know. Oxford University Press USA, 2016. 192 p.

3. McCarthy J., Minsky M. L., Rochester N. and Shannon C. E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine*. 27, 4 (Dec. 2006), 12. DOI: https://doi.org/10.1609/aimag.

v27i4.1904. URL: https://ojs.aaai.org//index.php/ aimagazine/article/view/1904 (дата звернення: 12.02.2022)

4. Julia L. There is no such thing as Artificial Intelligence! *BRAINCITIES* (Sep. 10, 2019). URL: https://medium.com/braincities/there-is-no-such-thing-as-artificial-intelligence-586482ca494d (дата звернення: 12.02.2022)

5. В Китае искусственный интеллект полностью интегрировали в правовую систему. *Судебно-юридическая газета*. 17.07.2022. URL: https://sud.ua/ru/news/abroad/244322-v-kitae-iskusstvennyy-intellekt-polnostyu-integrirovali-v-pravovuyu-sistemu (дата звернення: 12.02.2022)

6. Міщенко Т. Товариш штучний інтелект: у Китаї розробили програму, яка заміняє прокурора та може висувати обвинувачення. URL: https://mezha.media/2021/12/27/tovarysh-shtuchnyy-intelekt/ (дата звернення: 12.02.2022)

7. Гарапон А., Ласег Ж. Цифрове правосуддя. Переклад з фр., передмова, примітки В. Омельянчика. Київ: Стилос, 2021. 302 с.

ПРОБЛЕМИ ЦИФРОВІЗАЦІЇ КРИМІНАЛІСТИКИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

***Шевчук Віктор Михайлович*,**
доктор юридичних наук, професор,
провідний науковий співробітник НДІ ВПЗ ім. акад. В. В. Сташиса
НАПрН України, професор кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого,
Заслужений юрист України
ORCID: http://orcid.org / 0000-0001-8058-3071

Цифрові технології сьогодні – це невід'ємний компонент, інтегрований у всі сфери людської діяльності. *У сучасних умовах цифровізація стає найважливішим фактором економічного зростання економіки будь-якої країни і взагалі є сучасним трендом розвитку сучасного суспільства*, забезпечуючи практично всю цінність та інновації цифрового сектору держави. Процеси цифровізації виступають як нова реальність перспективного розвитку передових держав Європи та світу, у тому числі й України, яка обрала європейський вектор розвитку. Нова цифрова реальність ставить перед юридичною практикою і наукою безліч принципово нових завдань, пов'язаних з розробкою ефективних інструментів і моделей правового регулювання різних сфер життя суспільства, у тому числі й у сфері протидії злочинності.

Сьогодні цифрова реальність пов'язана із появою нових форм злочинності – кіберзлочинів, інформаційного шахрайства, великою кількістю кібернетичних атак на різні підприємства та установи, що потребує спеціального вивчення та дослідження. Цифрова інформація, як невід'ємний атрибут сучасної злочинної й діяльності органів кримінальної юстиції, визначає перспективи розвитку юридичної науки, у тому числі й криміналістики [9, с. 98], яка знаходиться на передньому краю боротьби зі злочинністю в сучасних умовах цифровізації суспільства.

У сучасних реаліях криміналістика відповідає розвитку цифрових технологій, створюючи засоби та методи можливості вилучення криміналістичної значимої інформації з нового виду носіїв. Завдяки науково-технічному прогресу з'являється можливість використання цифрових технологій у правоохоронній діяльності, що підвищує ефективність та прискорює процес досудового розслідування, дозволяє більш повно

формувати доказову базу при розслідуванні кримінальних правопорушень, а у подальшому і забезпечує якість судового розгляду матеріалів кримінальних проваджень.

В сучасних реаліях гостро постає питання про підвищення ролі криміналістики в сучасних умовах війни, у тому числі і за допомогою цифрових технологій, зокрема формування та застосування нового наукового напрямку – *цифрової криміналістики*. Як бачимо, у сучасному світі практично вся діяльність людини, у тому числі і злочинців, супроводжується своєрідною «слідовою картиною», серед якої особливе місце набувають *цифрові сліди* [1; 5; 8], як важливе джерело криміналістично-значущої інформації. Саме цифрові, а не електронні сліди на сьогоднішній день становлять основу доказової бази під час розслідування та розгляду кримінальних правопорушень.

Цифровими слідами в криміналістиці є матеріальні невидимі сліди, які містять криміналістично-значущу інформацію (відомості, дані), зафіксовану в цифровій формі на матеріальних носіях і можуть бути виявлені, зафіксовані й досліджені за допомогою певних цифрових пристроїв [1, с. 91]. Сьогодні такими слідами є файли та їх уривки, накопичувачі оперативної пам'яті та трафиків, службова інформація про ці файли, що утворюються цифровими пристроями (англ. digital device) – технічними пристроями або пристосуваннями, призначеними для отримання й оброблення інформації в цифровій формі з використанням цифрових технологій. Це може бути також певна різновиди комп'ютерних засобів, зокрема програмні продукти, текстові та графічні документи; файли мультимедіа; бази даних; файли програм; системні звіти та журнали додатків тощо. Як правило, вони застосовуються злочинцями при вчиненні кримінальних правопорушень, залишаючи своєрідну «слідову картину» із цифрових слідів.

Варто зауважити, що цифровий слід має певну систему ознак та властивостей, серед яких особливого значення набуває неможливість сприйняття такого сліду безпосередньо органами почуттів, а лише за допомогою спеціальних пристроїв та програм, тобто робота з ними потребує застосування спеціальних знань, вимагають нових нетрадиційних, способів, методів та процедур щодо їх виявлення, фіксації, дослідження та оцінки як доказів у майбутньому. Отже, *цифровий слід* являє собою криміналістично значиму комп'ютерну інформацію про події (дії) кримінального правопорушення, відображені у цифровій інформації

в матеріальному середовищі, у процесі її виникнення, обробки, зберігання та передачі.

Вбачається, що цифрові сліди є слідами матеріальними, оскільки, залишаючись у результаті певних подій, відбиваються на матеріальних об'єктах, хоча в деяких випадках період їх існування досить невеликий. За походженням цифрові сліди є технологічними, оскільки формування даних слідів обумовлено специфікою реалізації інформаційних технологій, і для їх перетворення в доступну для сприйняття форму також використовуються інформаційні технології. За механізмом слідоутворення вони можуть бути віднесені до електронних чи електро-магнітних залежно від носія, у якому вони відображені – твердотільному чи магнітних дисках. Можуть бути й механіко-оптичні цифрові сліди, які утворюються у структурі матеріалу оптичного диска під впливом лазерних променів.

Більше того, виявлення ознак кримінальних правопорушень в умовах цифровізації в кожному конкретному випадку мають свої особливості та специфіку, повязану із наявними цифровими слідами та механізмом слідоутворення, який буде різнитися способами вчинення та використовуваними технічними засобами та специфічним програмним забезпеченням. Успіх розкриття та розслідування такої злочинної діяльності буде можливим тільки при інтегруванні криміналістичних та спеціальних знань у галузі ІТ технологій, програмування та рівня підготовки слідчого і відповідного спеціаліста, який буде залучатися до проведення розслідування та процесу збору цифрової інформації.

У свою чергу цифрові докази вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження під час доказування у кримінальному провадженні. Під «цифровим доказом» у криміналістиці розуміють фактичні дані, представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ та 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 [7, с. 259].

В умовах воєнної агресії РФ проти України традиційні криміналістичні засоби та форми збирання доказів воєнних злочинів можуть працювати обмежено через небезпеку для всіх учасників слідчих (розшукових) дій, а також через неможливість безпосереднього доступу до місця

події [4, с. 897]. Тому виникає потреба у застосуванні інструментів цифрової криміналістики [6, с. 165]. Цифрова криміналістика, зокрема, має відношення до процесу збору, отримання, збереження, аналізу та подання електронних (цифрових) з метою отримання оперативно-розшукових відомостей, доказової інформації і здійснення розслідування та кримінального переслідування по відношенню до різних видів кримінальних правопорушень [3], включаючи кіберзлочини та воєнні злочини, що вчиняються військовими РФ на території України.

Сучасні можливості розслідування воєнних злочинів дозволяють визначити джерел цифрової інформації, які визначають напрями збирання та дослідження цифрових слідів, до яких можна віднести: отримання інформації з мобільних пристроїв вилучених телефонів в учасників кримінального провадження; отримання інформації з персональних комп'ютерів фізичних та юридичних осіб; отримання інформації із серверів та інших накопичувачів інформації в організаціях та установах; отримання інформації щодо радіочастотних ідентифікаторів, GPS-трекерам, датчикам, стаціонарним і мобільним вимірювальним пристроям з використанням систем геопозиціонування, відеоспостереження та позиціонування; отримання інформації з мережевих сервісів, що встановлюють голосовий та відеозв'язок між комп'ютерами через інтернет, такі як ICQ, Skype, WhatsApp, Viber, Telegram та інші; отримання інформації з банківських систем на відповідних цифрових носіях (SD-диски, флеш-картки та ін.); отримання інформації від стільникових операторів зв'язку щодо деталізації абонентського зв'язку та встановлення місцезнаходження абонента з геолокації; отримання інформації з камер відеоспостереження різних комерційних та державних структур; отримання інформації з вилучених у учасників кримінального провадження фотоапаратів та відеокамер.

Вважаємо, що треба чітко розрізняти цифрову криміналістику як окрему галузь криміналістичних знань, спрямовану на дослідження цифрових слідів, з одного боку, та з іншого – застосування цифрових технологій у розслідуванні та судовому розгляді, тобто процес *цифровізації криміналістики* як закономірний сучасний етапу її розвитку та формування, який передбачає впровадження цифрових технологій у різні галузі криміналістичної техніки та судової експертизи, до самого процесу досудового розслідування [8, с. 288].

Підсумовуючи, варто зазначити, що процеси цифровізації в криміналістиці [2; 10] в сучасних умовах є актуальними та потребують

подальших наукових досліджень. Для правильного розуміння та вирішення існуючих теоретичних та практичних проблем необхідно сконцентрувати зусилля не тільки криміналістів, а й представників інших наук, оскільки розглядувана проблематика має міждисциплінарний характер. В реаліях сьогодення та умовах воєнного стану гостро постає необхідність формування концепції цифрової криміналістики та вдосконалення освітніх програм із врахуванням інноваційних підходів криміналістичної дидактики та євроінтеграційних процесів, спрямованих на сучасний розвиток криміналістики як європейської науки.

Список використаної літератури:

1. Авдєєва Г. К. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики* : зб. матеріалів міжнар. наук.-практ. конфер.(Харків, 10–11 жовт. 2018 р.). Харків, 2018. С. 90–93.
2. Думчиков М. О. Процеси діджиталізації і криміналістика: ретроспективний аналіз. *Криміналістика і судова експертиза,* 2020, 65, 100–108.
3. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*, 2022, (1), 176–180.
4. Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: Proceedings of the 5th International scientific and practical conference (August 7–9, 2022). Sci-conf.com.ua‖. Lviv, Ukraine. 2022. Pp. 896–903.
5. Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні. *Цифрові трансформації України 2020: виклики та реалії*: зб. наук. пр. НДІ ПЗІР НАПрН України, 18 вересня 2020 р. Харків, 2020. С. 92–97.
6. Latysh, K. V. Criminalistics Analysis of Cyber Tools for Committing Crimes. *Probs. Legality*, *153*, 165.
7. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юриспруденція. 2013. № 5.С. 256–260.
8. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського держ. ун-ту внутр. справ ім. Е. О. Дідоренка*. 2022. № 3 (99). С. 283–294.
9. Шепітько В. Ю., Коновалова В. О., *Шевчук В. М.* та ін. Науково-технічне забезпечення слідчої діяльності в умовах змагального кримінального процесу. *Питання боротьби зі злочинністю.* 2021. Вип. 42. С. 92–102.

10. Shevchuk V. Innovative optimization directions of investigative (detective) activity in modern condition. *Theory and Practice of Forensic Science and Criminalistics*: Collection of Scientific Papers. Kharkiv : NSC «Hon. Prof. M. S. Bokarius FSI», 2021. Issue 2 (24). Pp. 8–25

ЦИФРОВА ТРАНСФОРМАЦІЯ ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНИХ ЗНАНЬ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ ПІД ЧАС ВОЄННОГО СТАНУ

Яремчук Вікторія Олегівна,
кандидат юридичних наук, старший науковий співробітник, НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України, лабораторія «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю»

В умовах воєнного стану змінюється діяльність органів правопорядку. Частково піддаються змінам і процедури проведення розслідування кримінальних правопорушень. Окремої уваги приділяється використанню спеціальних, криміналістичних знань в умовах війни.

Нині зафіксовано понад 16 тисяч проваджень по воєнних кримінальних правопорушень. Поліція, СБУ, ДБР, НАБУ, прокуратура зараз мають свою ділянку роботи з розслідування. Збирається доказова база для національних судів. Паралельно з цим збираються докази для Міжнародного кримінального суду, для майбутнього спеціального трибуналу з агресії [1].

Так, збиранням фактів про воєнні кримінальні правопорушення в Україні займаються працівники Офісу Генерального прокурора. Окремі держави активно допомагають Україні. Так, влада Німеччини направила своїх експертів до України. Українські судово-медичні експерти також отримають для судово-медичної експертизи з Німеччини необхідний матеріал. Люксембург передав Україні тридцять 3D-сканерів, які можуть бути використані для реконструкції місць подій, для фіксації травм загиблих та ін. [2]

Сьогодні Україна намається разом із Польщею та Литвою проводити рослідування воєнних злочинів створивши спільну міжнародну групу. Однак є певні проблеми у розслідуванні. Так, в Київську область, звільнену в кінці березня 2022 р., слідчі почали працювати лише в середині квітня. А огляд одного зі сильно постраждалих міст провели швидше, ніж за один робочий день. Крім того, в різних органах підходи до документування воєнних злочинів відрізняються. Так, Офіс Генерального прокурора реєструє кримінальні правопорушення під час війни тільки за статтею «воєнні злочини». А поліцейські фіксують ці кримінальні правопорушення як вбивство чи зґвалтування [3].

Використання цифрових технологій у розслдідуванні воєнних кримінальних правопорушень стає можливм завядки європейській підтримці. Так, Франція передала Україні унікальну мобільну ДНК-лабораторію, яка надала можливість здійснювати дослідження на місцях ексгумації тіл, економлячи час та ресурси[4]. Крім того, команда технологічної американської компанії «Hala Systems», що спеціалізується на аналітиці даних і штучному інтелекті допоможе Україні систематизувати накопичену доказову базу щодо російських кримінальних правопорушень. Слід зазначити, що дана інноваційна компанія відома створенням системи попередження про авіаудари цивільного населення у Сирії, а також впровадженням мобільного додатку з використанням штучного інтелекту дозволить сьогодні структурувати та пріоритезувати воєнні злочини на території України [5].

Отже, рослідування воєнних кримінальних правопорушень, вчинених на території України, потребує застосування цифрових інновацій у розслідуванні. Суттєву підтримку в цьому надають європейські держави. Необхідно надалі впроваджувати цифрові криміналістичні технології при розслідуванні тисяч військових кримінальних правопорушень.

Список використаної літератури:

1. Воєнні злочини росії: як допомогти зібрати докази URL: https://gre4ka.info/suspilstvo/71878-voienni-zlochyny-rosii-iak-dopomohty-zibraty-dokazy

2. Розслідування воєнних злочинів Росії: чому МКС ініціює відкриття офісу в Україні? URL: http://www.nrcu.gov.ua/news.html?newsID=98868

3. Перші кримінальні справи та сотні фігурантів: як Україна розслідує воєнні злочини росіян і чому виникають складнощі URL: https://www.pravda.com.ua/articles/2022/05/17/7346641/

4. Коломієць В. Місія французьких експертів допомогла розслідувати злочини росіян в Ізюмі, Курилівці та біля Куп'янська URL: https://hromadske.ua/posts/misiya-francuzkih-ekspertiv-dopomogla-rozsliduvati-zlochini-rosiyan-v-izyumi-kurilivci-ta-bilya-kupyanska

5. Масив інформації про кожен факт воєнних злочинів, вчинених рф, важливо структурувати та пріоритезувати, – Катерина Павліченко. URL: https://www.kmu.gov.ua/news/masiv-informaciyi-pro-kozhen-fakt-voyennih-zlochiniv-vchinenih-rf-vazhlivo-strukturuvati-ta-prioritezuva

ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN LAW ENFORCEMENT AND JUSTICE: UKRAINIAN AND EUROPEAN EXPERIENCE

Baltrūnienė Jurgita,
Mykolas Romeris University, Academy of Public Security, Lector, Department of Police Activities, Kaunas District Prosecutor's Office, Prosecutor
ORCID ID: 0000-0001-8323-0570

Shevchuk Viktor,
Doctor of Legal Sciences, Professor, Professor of Criminalistics Yaroslav Mudryi National Law University, leading Researcher Academician Stashis Scientific Research Institute for the Study of Crime Problems
ORCID ID: 0000-0001-8058-3071

In modern conditions, the XXI century is often called the era of innovation, in which artificial intelligence (AI) has become one of the most urgent and significant problems. Today, artificial intelligence technologies are widely used in everyday and professional life. In particular, artificial intelligence is used in medicine, economics, business, industry, agriculture, public administration, cyber security, education, science, defense and military, including legal. In today's realities, AI is not just a technological trend, a buzzword, or a temporary fad, in fact it is the third computer era based on innovation and advanced technologies.

We are now at a stage of fundamental change, unlike that experienced by the generation of the first industrial revolution. The head of Google, (Sundar Pichai), noting the importance of artificial intelligence in modern society, indicated that achievements in the field of artificial intelligence would do more for humanity than the discovery of fire or electricity [3]. Today, smartphones recognize the faces of their owners, autopilot drives cars, virtual assistants answer our questions, street cameras recognize criminals, «cyber judges» make court decisions, surgical operations are performed with the help of robots, high-precision military weapons and unmanned aerial vehicles are being created [1, p. 356] and it's far is not an exhaustive list of cases when modern AI technologies help a person to solve various complex tasks. AI as the latest scientific breakthrough is included in new forensic ideas and methods related to its use in the fight against crime [14].

The military aggression of the Russian Federation and the introduction of martial law in Ukraine significantly affected all spheres of our lives. On the territory of Ukraine, the Russian military commits mass murders of civilians, destruction of infrastructure facilities and citizens' homes, rape of women and children, and looting [4, p. 898]. In such conditions, the main task of criminalistic is the development and application of means, techniques and methods that allow collecting, researching, and using evidentiary information in the conditions of war and global threats of the XXI century [11, p. 9–20].

According to the official statistics of the Office of the Prosecutor General, among the crimes committed during the full-scale invasion of the Russian Federation, the following are the most widespread: a) crimes of aggression and war crimes – 54 898 crimes were registered (as of December 20, 2022); b) crimes against national security – 18 438 crimes; c) crimes against children – 450 children were killed, 863 children were injured; 4) the city case of aggression of the RF – 633 examined representatives of the military leadership of the RF (military command, officials, ministers, heads of political law enforcement agencies, etc.) [7].

Peculiarities of the formation and application of forensic knowledge in the conditions of martial law. In such conditions, the main task of criminalistic is the development and application of means, techniques and methods that allow collecting, researching, and using evidentiary information in the conditions of war and global threats of the 21st century [10, p. 175]. Now, in the realities of wartime, the question of increasing the role of criminalistics in modern conditions, including with the help of artificial intelligence technologies, is acute.

How does artificial intelligence help us in war and accelerate our victory? The main ones are as follows: 1) Identification of Russian occupiers in social networks and on video cameras; 2) Searches for saboteurs, spies and war criminals; 3) Listens to the Russian military; 4) Creates pictures about Ukraine; 5) Collects intelligence for the Armed Forces of Ukraine. So, for example, searches for saboteurs, spies and war criminals – facial recognition algorithms have found many terrorists who committed crimes in the Kyiv region, Kharkiv, Izyum, Kupyansk and other cities of Ukraine. Artificial intelligence technologies are also used at checkpoints – such systems have already caught more than two hundred criminals, saboteurs, and deserters [6].

Now, in the realities of wartime, legal science and criminal justice face new challenges and tasks, which, in turn, require the use of the latest approaches

to solve them, including the help of artificial intelligence technologies [12, p. 185–196]. Among such tasks, the: study of the problems of the place of artificial intelligence in the activities of law enforcement and justice; issues related to the elimination of gaps in the regulatory and legal regulation of the use of artificial intelligence; ensuring the protection of the rights and legitimate interests of individuals and legal entities against violations using digital technologies; attracting to liability for damage caused by the use of digital technologies.

Now, in the realities of wartime there are important key areas of state policy in the field of artificial intelligence. To consolidate the efforts of the state, scientists, educators, business, public and expert communities in the field of artificial intelligence, the Ministry of Digital Transformation of Ukraine created the Expert Committee on the Development of AI in Ukraine, which proposed eight key directions of state policy in the field of artificial intelligence: 1) Education and human capital; 2) Science and innovation; 3) Economy and business; 4) Cyber security; 5) Defense and security; 6) State administration; 7) Legal regulation and ethics; 8) Justice. We are primarily interested in the application of artificial intelligence in justice, the activities of law enforcement agencies, and the improvement of legal support for such activities.

First of all, let's find out what is the attitude of Ukrainians to the use of artificial intelligence? A sociological study conducted in Ukraine showed that the majority of surveyed respondents are positive about the consequences of the development of artificial intelligence. They see such positive points primarily in: 1) freeing people from difficult, dangerous and unskilled jobs (69.5%); 2) increase in productivity in all branches of industry (50.4%); 3) prevention of diseases, the extension of human life (19.9%); 4) securing humanity from natural disasters and catastrophes (18.1%); 5) prevention of crime and war (14.1%). At the same time, 35.6% of respondents believe that artificial intelligence should be entrusted with law enforcement functions, 46.0% – the development and improvement of legislation, and 54.9% – consideration of cases in court [9].

The prerequisite for the introduction of artificial intelligence in Ukraine is the launch of a *unified judicial information and telecommunication system* (EUITS), which is a set of information and telecommunication subsystems (modules) that ensure the automation of the processes of activity of courts, bodies and institutions in the justice system determined by legislation and this Regulation.

Can artificial intelligence replace the judge? In Art. 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as the ECHR, the Convention) enshrines the right to review cases by an independent and impartial court. However, not in Art. 6, nor in the comments to it, there is no direct prohibition of the use of artificial intelligence and it is not said that justice is administered only by a human judge. The practice of the European Court of Human Rights considering the violation of Article 6 of the Convention due to the use of AI in decision-making has not yet occurred. Our national law details the norm of the Convention in Art. 127 of the Constitution of Ukraine, which stipulates that justice is administered by judges and that judicial power is vested in them [8]. A similar legal position is contained in Art. 92 of the Basic Law of the Federal Republic of Germany.

Thus, artificial intelligence cannot replace judges, however, nothing prohibits optimizing the work of the judge and the court by involving artificial intelligence. When analyzing the abovementioned issues, attention should be paid to the approach of the European Union to the creation of regulation in certain areas. The Schuman Declaration states «Europe will not be made all at once, or according to a single plan. It will be built through concrete achievements which first create a de facto solidarity» [13].

Thus, it can be concluded that the use of artificial intelligence may violate the rights of a person to ensure his right to a fair trial, and this is not permissible. It is believed that the most important thing in ensuring a person's rights to a fair trial, when artificial intelligence is involved in the decision-making process, is the possibility for judges and other persons involved in the case to check how the artificial intelligence reached this or that conclusion. AI is particularly useful in implementation such a right of individuals in simple cases by eliminating the factor of human error, but the final decision must be reviewed and approved by the judge. Thus, the use of such artificial intelligence is approved, but it is proposed not to eliminate the human factor, that is, it is necessary for a «real» judge to check and confirm the decision made by artificial intelligence [2, p. 216–217].

Already today, law enforcement agencies of Ukraine are actively using AI technologies in the following directions:1) Face recognition; 2) Ensuring road safety; 3) Use of drones; 4) Prevention of criminal offences; 5) Prediction of criminal offenses. So, for example, with the help of drones, police officers can detect poachers, detect illegal mining, illegal logging, find outbreaks

of forest fires, and help search for those lost in the forest or mountains. So, in 2021, police officers from the anti-narcotics crime unit discovered 36 areas planted with hemp in the Dnipropetrovsk region. Drones monitor the road situation on the highways of the Dnipropetrovsk and Kyiv regions and look for stolen vehicles [5, p. 116]. In Ukraine, the widest field of application of drones in military operations.

Summing up the above, the following should be noted: 1) A significant problem from the use of AI technologies today is the violation of human rights in the field of privacy protection of personal data on the Internet and interference with privacy and private life; 2) It is important not to exaggerate the advantages of artificial intelligence, to balance the advantages of artificial intelligence technologies, especially those that only a person can possess when making decisions. At the same time, it is currently impossible to replace the judge with artificial intelligence when conducting judicial proceedings; 3) It is necessary to create global (mandatory) international legislation regarding the development and implementation of artificial intelligence, in particular, to prevent its illegal, i.e. uncivilized use; 4) Prospects for further scientific research should be aimed at developing issues related to the development and use of artificial intelligence as a component of information technologies in law enforcement and justice, considering the international experience and modern practice.

References:

1. Ackermann V. R., Kurapka V. E., Malewski H., Shepitko V. Schaffung eines einheitlichen europaisehen Kriniinalistischen Raumes: Die Tatigkeit offentlicher Organisationen zur Starkung der internationalen Beziehungen. *Kriminalistik*. 2020. Vol. 2020, Iss. 6. P. 355–363.
2. Baltrūnienė Jurgita. Dirbtinis intelektas ir duomenų apsauga kriminalistikos plėtros kontekste. *Kriminalistikos teorijos plėtra ir teismo ekspertologijos ateitis.* Kolektyvinė monografija. Liber Amicorum Profesoriui Vidmantui Egidijui Kurapkai. Vilnius, 2022. Pp. 201–220.
3. Google CEO Sundar Pichai: AI is more important than fire, electricity. URL: https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html
4. Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: 5th International scientific and practical conference (August 7–9, 2022). SPC-Sci-conf.com.ua. Lviv, Ukraine. 2022. Pp. 896–903.

5. Козар А. В. Актуальні питання використання безпілотних літальних апаратів для запобігання незаконному вирощуванню снодійних маків чи конопель. *Правові та організаційні засади забезпечення державою правоохоронної функції*: Всеукр. наук.-практ. конф. (Дніпро, 30 жовт. 2018 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. С. 115–118.
6. War crimes: how technology will help find Russian soldiers for trial after the war in Ukraine / NV). URL: https://techno.nv.ua/ukr/innovations/tehnologiji-proti-viyskovih-zlochinciv-50236139.html
7. Website of the Office of the Attorney General Ukraine. URL: https://www.gp.gov.ua/
8. Petryshyn, O. V., & Hyliaka, O. S. Human rights in the digital age: challenges, threats and prospects. *Journal of the National Academy of Legal Sciences of Ukraine*, 28 (1), 2021,15–23.
9. Майже 50% українців вважають, що штучний інтелект може допомогти забезпечити чесні вибори і перемогти корупцію, опитування.ua https://lb.ua/news/2018/12/11/414638_pochti_50_ukraintsev_schitayut.html
10. Shevchuk V. M. Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine*, 27 (2), 2020, 170–183.
11. Shepitko V. Theoretical and methodological model of criminalistics and its new directions. *Theory and Practice of Forensic Science and Criminalistics*. Issue 3. 2021, 25. Pp. 9–20.
12. Shepitko V. The Formation of Digital Criminalistics as a Strategic Direction for the Development of Science. *17 Medzinarodny Kongres Kriminalistika a Forenzne Vedy: Veda, Vzdelavanie, Prax*. Zbornik. Bratislava, 2021. Pp. 185–196.
13. Schuman declaration May 1950. URL: https://european-union.europa.eu/principles-countries-history/history-eu/1945–59/schuman-declaration-may-1950_en
14. Cody Jackson Artificial Intelligence Changing the World of Forensics Science, June 16, 2021. URL: file://D:/Downloads/EasyChair-Preprint-5815%20(1).pdf)

APPLICATION OF DIGITAL TECHNOLOGIES IN CRIMINALISTICS IN THE CONDITIONS OF WAR

Konovalova Violeta Omelyanivna,
Doctor of Legal Sciences, Professor, Academian National Academy of Legal Sciences of Ukraine, chief researcher Academician Stashis Scientific Research Institute for the Study of Crime Problems

Shevchuk Viktor Mikhailovich,
Doctor of Legal Sciences, Professor, Professor of Criminalistics Yaroslav Mudryi National Law University, leading researcher Academician Stashis Scientific Research Institute for the Study of Crime Problems

In today's realities, the digital age is a modern era in which social, economic and political activity depends on information and communication technologies. It is believed that the world of digital technologies, which we are now entering, is not only a new logical stage in the development of the technological sphere of mankind, but also the entire existing legal and socio-political reality [10, p. 90]. In this era, when the latest high technologies are key, society is moving into a new reality of digitalization, actively using digital technologies in all areas of society. Digital technologies in modern conditions are an integral component integrated into all spheres of human activity, which determines the prospects for the development of the economy, politics, national security and the defense capability of the state.

Today, digitalization is a modern trend in the development of society, becoming the most important factor in the economic, social, political and international growth of any country, including Ukraine, which has chosen the European vector of development. Granting Ukraine the status of an EU candidate has created an additional impetus for the harmonization of approaches to digital transformation. In this regard, an important event was the fact that Ukraine joined the *Digital Europe Program* until 2027, the goal of this program is to activate economic recovery and digital transformation of Ukraine [14]. The formation of a single digital market with the EU and the approximation of the digital sector of Ukraine to the European one are the priorities of the domestic policy of digital transformations in the conditions of war [17].

In this regard, it is worth noting that with the development of society, digitalization of all spheres of life, the system of law enforcement agencies needs constant improvement, in particular, its transition to a new reality – digital. This is a situation where digital information, as an integral attribute of criminal activity and the work of criminal justice bodies, determines the trends in the development of criminology, criminal and criminal procedural law. Digital reality is associated with the emergence of new forms of crime – cybercrimes, information fraud, a huge number of cyberattacks on various enterprises and institutions [1, p. 269]. Moreover, the armed aggression of the Russian Federation and the introduction of martial law in Ukraine had a significant impact on our society. It is obvious that such threats require the development of new countermeasures, updating the system of criminal justice bodies to modern conditions and global threats, including the means of criminalistics [15, p. 12–27].

In such conditions, the main task of criminalistics is the development and application of means, techniques and methods that allow collecting, researching, and using evidentiary information in the conditions of war and global threats of the 21st century [6, p. 898].The system of pre-trial investigation bodies, the prosecutor's office, and criminal justice bodies face new challenges related to the need for quick, comprehensive and high-quality documentation, gathering the evidence base of massive criminal violations of international humanitarian law.

Today, the question of increasing the effectiveness of the investigation of cybercrimes and war crimes with the help of digital technologies is a pressing issue. Under such circumstances, it is now possible to talk about the activation of trends in the formation and application of a new scientific direction – *Digital Forensics (Digital Forensic Science or Digital Criminalistics)* [2, p. 83–84]. Other terms are used to designate this direction – «*Computer Forensic*» [11, p. 29–30], «*Electronic Forensics*» [4, p.79] or «*Forensics in Computer Systems*»[16, p. 189].

Further development of criminalistics in the conditions of the information society, digitization and military realities of today is impossible without the wide use of innovative and fundamental knowledge in the field of *digital criminalistics* – a new field of criminalistics that is dynamically developing today and forms the theoretical and methodological foundations in this field of knowledge [5, p. 80].

Today, criminalistics corresponds to the development of digital technologies, creating means of the possibility of extracting forensically significant information from a new type of media. Thanks to scientific and technical progress, it is possible to use digital technologies in law enforcement activities, which accelerates the process of pre-trial investigation, allows to more fully form the evidence base in the investigation of crimes, and in the future ensures the quality of judicial review of materials of criminal proceedings.

In the special literature [12; 13; 16] there are different approaches to defining the concept of digital criminalistics and its place in the system of criminalistics and forensic sciences. Some scientists point out that digital forensics is a separate branch of forensic science, which is a system of scientific methods for researching digital evidence in order to facilitate the detection and investigation of criminal offenses [13, p. 290]. Others believe that digital forensics is related to the process of collecting, receiving, saving, analyzing and submitting electronic (digital) data for the purpose of obtaining investigative information, evidentiary information and carrying out investigations and criminal prosecutions in relation to various types of criminal offenses [7, p. 179], including cybercrimes and war crimes committed by the occupying forces of the Russian Federation on the territory of Ukraine.

Some sources indicate that digital forensics is «one of the branches of criminalistics that focuses on criminal procedural law and evidence regarding computers and related devices» [9, p.29], such as mobile devices (e.g., phones and smartphones), game consoles, and other Internet-enabled devices (e.g., health and fitness devices and medical devices) [8]. In addition, digital forensics is related to the process of collecting, obtaining, analyzing and presenting electronic (digital) evidence in pretrial and judicial proceedings. Therefore, digital forensics can be a strategic direction in the development of criminalistics [16, p. 192].

In view of the above, it can be stated that the subject of digital forensics is the regularities of detection, recording, preliminary research, use of computer information and means of its processing in order to solve the tasks of detection, disclosure, investigation and prevention of criminal offenses, as well as development based on this knowledge regularities of technical means, techniques, methodical recommendations aimed at optimizing activities in the fight against crimes.The object of digital

forensics is, on the one hand, criminal offenses related to the use of computer technologies and social relations that arise in the course of detection, disclosure and investigation, and criminal offenses when detection, recording, preliminary research is carried out, the use of computer information and means of its processing, and on the other hand, the activity of law enforcement agencies in relation to the investigation of such criminal offenses and the issue of the development and application of criminalistic methods, means of using computer technologies in the fight against crime.

Therefore, *digital forensics* is a branch of criminalistics that studies the patterns of occurrence and use of digital traces and, based on the knowledge of these patterns, develops technical means, techniques and methods for detecting, recording, extracting and researching digital information and means of its processing for the purpose of disclosure, investigation and prevention of crimes.

We believe that it is necessary to clearly distinguish digital forensics as a separate branch of criminalistic knowledge, aimed at the study of digital traces, on the one hand, and on the other – the use of digital technologies in the investigation and judicial procedure, that is, the process of digitization of criminalistics as a natural modern stage of its development and formation, which provides for the implementation of digital technologies in various fields of criminalistics and forensic examination, to the very process of pre-trial investigation [13, p. 288].

In the realities of war, the central place for collecting evidence of war crimes in digital forensics was occupied by artificial intelligence technology [3, p. 107]. In modern conditions of war, the following areas of application of digital forensics are of particular importance: obtaining information from mobile devices of seized phones of participants in criminal proceedings; receiving information from personal, such as Skype, WhatsApp, Viber, Telegram and others; receiving information from banking systems on appropriate digital media (SD disks, flash cards, etc.); receiving information from cellular communication operators regarding the details of subscriber communication and establishing the location of the subscriber from geolocation; obtaining information from video surveillance cameras of various commercial and state structures; obtaining information from cameras and video cameras seized from participants in criminal proceedings.

Thus, the process of digitization of criminalistics is a natural stage of its modern development and formation, which involves the introduction

of digital technologies in various fields of criminalistics, forensic expertise and varieties of legal practice. Today, it is one of the most promising areas of scientific research in criminalistics. Under such circumstances, it is necessary to update the development of the problem of digital forensics and criminalistic didactics in the conditions of digitalization. At the same time, special attention should be paid to the training, retraining, and advanced training of investigators, forensic investigators, and forensic experts in the field of digital technologies, including the initiation and training of a new profession – a digital criminalistic scientist.

References:

1. Авдєєва Г. К. Використання спеціальних знань у боротьбі з комп'ютерною злочинністю. *Вісник Луганського держ. ун-ту внутрішніх справ імені Е. О. Дідоренка.* Сєвєродонецьк, 2016. Вип. 1. С. 268–277.
2. Борисова К. Є., Світличний В. А. Застосування цифрової криміна-ліс-тики. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану*: тези доп. Міжнар. наук.-практ. конф. (м. Харків, 25 листоп. 2022 р.). Харків: ХНУВС, 2022. С. 83–84.
3. Dumchykov M. O. Protsesy didzhytalizatsii i kryminalistyka: rektrospektyvnyi analiz. *Kryminalistyka i sudova ekspertyza Forensics and forensic examination,* issue 65, 2020. Pp. 100–108.
4. Заєць І. С. Перспективи криміналістики в умовах інформатизації суспільства. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід* : Міжнар. наук.-практ. круглий стіл (Київ, 19 лют. 2020 р.). Київ : НАВСУ, 2020. С. 77–81.
5. Kohutych I. I. Zastosuvannia tsyfrovykh tekhnolohii – novyi napriam kryminalistyky. *Naukovi chytannia pamiati Hansa Hrossa: zbirnyk tez mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Chernivtsi, 09 hrudnia 2021 r.) – Scientific readings in memory of Hans Gross: collection of theses of the international scientific conference (Chernivtsi, December 9, 2021). Chernivtsi: Tekhno-druk, 2021.Pp.79–84.
6. Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: Proceedings of the 5th International scientific and practical conference (August 7–9, 2022). Sci-conf.com.ua. Lviv, Ukraine. 2022. Pp. 896–903.
7. Kolodina A. S., Fedorova T. S. Tsyfrova kryminalistyka: problemy teorii i praktyky. *Kyivskyi chasopys prava – Kyiv Journal of Law*, issue 1, 2022. Pp.176–180.

8. Kiberprestupnost. Vvedenie v cifrovuyu kriminalistiku. Modul 4. Vena: OON, 2019. 32 p. URL: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_4_Introduction_to_Digital_Forensics_RU.pdf
9. Maras Marie-Helen. Computer Forensic: Cybercriminals, Laws, and Evidence. Second Edition. Burlington, Jones & Bartlett Learning, 2014. 408 p.
10. Метелев О. П. Окремі проблеми цифровізації у кримінальному процесі. *Прикарпатський юридичний вісник*. Вип. 3 (44). 2022. С. 90–94.
11. Полотай О. І. Комп'ютерна криміналістика: основні завдання та проблеми. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*»: міжн. наук. конф. Тернопіль. Вип. 68. 2022. С. 29–30.
12. Samodin A. V. Suchasne rozuminnia fenomenu «tsyfrova kryminalistyka». Innovatsii v kryminalistytsi ta sudovii ekspertyzi : materialy mizhvidom. nauk.-prakt. konf. (Kyiv, 25 lystop. 2021 r.). *Innovations in criminology and forensic examination:* interdisciplinary materials. science and practice conf. (Kyiv, November 25, 2021). Kyiv : Nats. akad. vnutr. sprav, 2021. Pp. 275–279.
13. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського держ. ун-ту внутр. справ ім. Е. О. Дідоренка*. 2022. №3 (99). С. 283–294.
14. Україна долучилася до Програми «Цифрова Європа»: що це означає | Кабінет Міністрів України. URL: https://www.kmu.gov.ua/news/ukraina-doluchylasia-do-prohramy-tsyfrova-ievropa-shcho-tse-oznachaie
15. Shepitko V., Shepitko M. Doktryna kryminalistyky ta sudovoi ekspertyzy: formuvannia, suchasnyi stan i rozvytok v Ukraini. *Law of Ukraine*, 2021, 8, 12–27.
16. Shepitko V., Shepitko M. The Formation of Digital Criminalistics as a Strategic Direction for the Development of Science. *XVII Criminalistics and Forensic Expertology: Science, Studies, Practice*. (September 16–17), 2021. Pp. 187–198.
17. Shevchuk V. Tasks of criminalistics in modern conditions of war. *Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних та юридичних наук*: міжн. наук.-практ. конф. (Харків-Рига, 31 травня 2022 р.). Харків, 2022. С. 28–30.

Наукове видання

ЦИФРОВА ТРАНСФОРМАЦІЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Матеріали круглого столу,
присвяченого Всеукраїнському тижню права
(м. Харків, 23 грудня 2022 року)

Електронне наукове видання

Комп'ютерна верстка *А. Т. Гринченка*

Підписано до поширення через мережу Інтернет 28.12.2022.
Відповідає формату друкованого видання 60×84/16. Гарнітура Times. Обл.-вид. арк. 8. Об'єм даних 1,69 Мб.
Вид. № 3125

Видавництво «Право» Національної академії правових наук України
та Національного юридичного університету імені Ярослава Мудрого,
вул. Чернишевська, 80-А, Харків, 61002, Україна
Тел./факс (057) 716-45-53
Сайт: https://pravo-izdat.com.ua
E-mail для авторів: verstka@pravo-izdat.com.ua
E-mail для замовлень: sales@pravo-izdat.com.ua
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції – серія ДК № 4219 від 01.12.2011