DOI: 10.31359/2079-6242-2022-44-69
УДК 343.3/.7

М. В. Шепітько, доктор юридичних наук,
старший науковий співробітник,
професор кафедри кримінального права
Національного юридичного університету
імені Ярослава Мудрого

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ЗДІЙСНЕННЯ ПРАВОСУДДЯ

Постановка проблеми. Здійснення судової реформи в Україні та приведення до міжнародних стандартів його здійснення, а також діджиталізація державних інституцій в Україні, призвело до здійснення автоматизації правосуддя, використання можливостей відеозв'язку (онлайн), створення інформаційних систем, які спрямовані на спрощення доступу до правосуддя, а також збільшення використання електронної сфери. Разом із позитивними змінами, які безумовно здійснюються в Україні щодо забезпечення захисту прав та інтересів людини та громадянина шляхом здійснення правосуддя, нажаль, слід, констатувати наявність негативних проявів у цій сфері. Одним із таких негативних проявів стає незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя (ст. 376–1 КК України), яка ще в 2009 р. була включена до КК України в попередній редакції.

За статистичними даними Офісу Генерального прокурора було зареєстровано злочинів, передбачених ст. 376–1 КК України: у 2016 р. – 37; у 2017 р. – 60; у 2018 р. – 83; у 2019 р. – 34; у 2020 р. – 30; у 2021 р. – 32[1]. За цими ж статистичними даними тільки за цей період до суду з обвинувальними актами було передано 31 кримінальне провадження (справ), з яких постановлено 4 обвинувальні вироки[2]. Фіксація такої значної кількості втручань до Єдиної судової інформаційно-телекомунікаційної системи (раніше – автоматизованої системи документообігу суду), достатньо великої кількості складених обвинувальних актів та наявності обвинувальних вироків за цією категорією проваджень свідчить про істотне бажання зацікавлених осіб вплинути на результати здійснення правосуддя на свою користь, одержати бажане, а не законне та справедливе рішення суду.

Посягання на автоматизовані системи в органах та установах правосуддя може бути здійснено через умисне внесення неправдивих відомостей чи несвоєчасне внесення відомостей до Єдиної судової інформаційно-телекомунікаційної системи, іншої автоматизованої системи, що функціонує в суді, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів, Державній судовій адміністрації України, їх органах, несанкціоновані дії з інформацією, що міститься в таких системах, чи інше втручання в роботу таких систем, вчинене службовою особою, яка має право доступу до цієї системи, або іншою особою шляхом несанкціонованого доступу до таких систем. Зрозуміло, що механізм такого впливу може бути різним та скерованим як зсередини (професійними учасниками провадження та технічного забезпечення діяльності системи), так і ззовні (зацікавленими особами).

Аналіз останніх досліджень і публікацій. Дослідження кримінально-правової охорони інформаційної безпеки під ча здійснення правосуддя не були предметом окремих монографічних досліджень. Разом із цим набуває все більшої значущості забезпечення такої кримінально-правової охорони через притягнення до кримінальної відповідальності за вчинення незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя (ст. 376–1 КК України). До даної проблеми зверталися у своїх дослідженнях В. С. Батиргареєва[3], А. С. Беніцький[4], В. А. Ко-

[1] Див.: 'Офіс Генерального прокурора' <https://new.gp.gov.ua/ua/posts/statistika> (дата звернення: 13.09.2022)

[2] Див.: 'Єдиний державний реєстр судових рішень' <https://reyestr.court.gov.ua> (дата звернення: 13.09.2022)

[3] Батиргареєва В. С. 'Концептуальна модель захисту інформаціного простору України засобами кримінального права' (2020) 1 (32) Інформація і право 110–119

[4] Дудорова О. О., Письменського Є. О. (ред) *Кримінальне право (Особлива частина): підручник* Т. 2. (Елтон-2, 2012) 533–535

зак[1], А. С. Нерсесян[2], В. І. Тютюгін та М. В. Шепітько[3]. Також дані дослідження корелюються із розвитком науково-технічного прогресу, пов'язаного із застосуванням автоматизованих систем, великих даних та штучного інтелекту в сфері кримінальної юстиції.

Мета статті – дослідити межі кримінально-правової охорони інформаційної безпеки під час здійснення правосуддя та можливості протидії таким втручанням.

Виклад основного матеріалу. Стаття 376–1 Кримінального кодексу України (далі – КК України) захищає *від умисного внесення неправдивих відомостей чи несвоєчасного внесення відомостей до Єдиної судової інформаційно-телекомунікаційної системи, іншої автоматизованої системи*, що функціонує в суді, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів, Державній судовій адміністрації України, їх органах, несанкціоновані дії з інформацією, що міститься в таких системах, чи інше втручання в роботу таких систем, вчинене службовою особою, яка має право доступу до цієї системи, або іншою особою шляхом несанкціонованого доступу до таких систем. Це кримінальне правопорушення проти правосуддя (розділ XVIII Особливої частини КК України) визнається нетяжким злочином. Таку норму слід вважати спеціальною по відношенню до втручання в діяльність судових органів (за умови її широкого тлумачення найменування кримінального правопорушення, передбаченого ст. 376 КК України).

Слід відзначити, що кваліфікація зазначених суспільно небезпечних діянь передбачених ст. 376–1 КК України є ускладненою бланкетністю норми і відсиланням до положення Вищої ради правосуддя про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи від 17.08.2021 р. № 1845/0/15–21. Відповідно до п. 3 цього положення Єдина судова інформаційно-телекомунікаційна система (ЄСІТС) – сукупність інформаційних та телекомунікаційних підсистем (модулів), які забезпечують автоматизацію визначених законодавством та цим Положенням процесів діяльності судів, органів та установ в системі правосуддя, включаючи документообіг, автоматизований розподіл справ, обмін документами між судом та учасниками судового процесу, фіксування судового процесу та участь учасників судового процесу у судовому засіданні в режимі відеоконференції, складання оперативної та аналітичної звітності, надання інформаційної допомоги суддям, а також автоматизацію процесів, які забезпечують фінансові, майнові, організаційні, кадрові, інформаційно-телекомунікаційні та інші потреби користувачів ЄСІТС.

Оголошенням Вищої ради правосуддя від 04.09.2022 було повідомлено, що відповідно до п. 2 § 2 розд. 4 Закону України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» окремі підсистеми (модулі) Єдиної судової інформаційно-телекомунікаційної системи починають функціонувати після опублікування оголошення про створення та забезпечення функціонування відповідної підсистеми (модуля) ЄСІТС, яке має містити інформацію про підпункти, пункти цього розділу, які вводяться в дію у зв'язку з початком функціонування відповідної підсистеми (модуля) ЄСІТС.

Відповідно до ст. 35 КПК України у суді функціонує Єдина судова інформаційно-телекомунікаційна система, що забезпечує, зокрема: 1) об'єктивний і неупереджений розподіл матеріалів кримінального провадження між суддями з додержанням принципів черговості та однакової кількості проваджень для кожного судді; 2) визначення присяжних для судового розгляду з числа осіб, які внесені до списку присяжних; 3) надання фізичним та юридичним особам інформації про стан розгляду матеріалів кримінального провадження у порядку, передбаченому цим Кодексом; 4) реєстрацію вхідної і вихідної кореспонденції та етапів її руху; 5) участь учасників судового процесу у судовому засіданні в режимі відеоконференції. Подібні норми з визначенням особливостей функіонування та застосування ЄСІТС в різних вормах судочинства та проваджень прийняті і в інших процесуальних кодексах України (див. ст. 14 ЦПК України, ст 6 ГПК України, ст. 18 КАС України). При цьому «Єдина судова інформаційно-телекомунікаційна система

[1] Козак В. А. 'Кримінальна відповідальність за незаконне втручання в роботу автоматизованої системи документообігу суду: аналіз основного слкаду злочину'(2013) 122 Проблеми законності 151–158.

[2] Нерсесян А. С. 'Автоматизована система документообігу суду як обгєкт кримінально-правової охорони' (2018) 29 Правова держава 275–281

[3] Тютюгін В. І., Шепітько М. В. *Кримінальні правопорушення, які посягають на відносини, що забезпечують реалізацію конституційних принципів правосуддя і належне виконання особами, що його здійснюють своїх професійних (службових) обов'язків. Кримінальне право. Особлива частина.* За ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна (Право, 2020) 642–652.

підлягає захисту із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю» (ст. 35 КПК України).

Регламентація діяльності *інших автоматизованих систем*, що функціонують в суді, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів, Державній судовій адміністрації України, їх органах, разом із цим не є такою визначеною. Це означає необхідність прийняття окремого положення, яке б відображало дію таких «інших» автоматизованих систем. Дослідження цього питання дозволило встановити, наприклад, Положення Вищої ради правосуддя про автоматизовану систему розподілу справ (визначення члена Вищої ради правосуддя – доповідача) та визнання такими, що втратили чинність, деяких рішень Вищої ради юстиції та Вищої ради правосуддя від 16.11.2017 р. №3689/0/15–17. Такий підхід законодавця фактично унеможливлює застосування будь-яких «інших» автоматизованих систем в суді, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів, Державній судовій адміністрації України, їх органах, оскільки вони прямо (на відміну від ЄСІТС) не визначені в КК України.

У статті 7 Конвенції Ради Європи про захист прав і основоположних свобод від 04.11.1950 р. наголошується, що «нікого не може бути визнано винним у вчиненні будь-якого кримінального правопорушення на підставі будь-якої дії чи бездіяльності, яка на час її вчинення не становила кримінального правопорушення згідно з національним законом або міжнародним правом. Також не може бути призначене суворіше покарання ніж те, що підлягало застосуванню на час вчинення кримінального правопорушення».

Принцип передбачення законом злочинів і покарань вимагає, або правопорушення і покарання за їх скоєння були чітко визначені у законі. Поняття «закон» у розумінні статті 7, як і в інших статтях Конвенції, передбачає якісні умови, зокрема щодо доступності і передбачуваності (Cantoni проти Франції, § 29; Kafkaris проти Кіпру, § 140; Del Rio Prada проти Іспанії, §91; Perincek проти Швейцарії, §134). Якісні умови мають бути виконані як щодо визначення правопорушення (Jorgic проти Німеччини, §§ 103–114), так і щодо покарання за його скоєння або щодо його міри Kafkaris проти Кіпру, § 150; Kamilleri проти Мальти, §§ 39–45)… Відсутність «яксоті закону» щодо визначення правопорушення або покарання, котре має за нього застосовуватись, спричиняє порушення статті 7 Конвенції (Kafkaris проти Кіпру, § § 150 і 152)[1]. Таким чином, можливість застосування ст. 376–1 КК України щодо посягань на «інші» автоматизовані системи, що діють в судових органах ставиться під сумнів.

Проблема застосування автоматизованих систем в органах правосуддя (в широкому розумінні відповідно до чинної Конституції України) ставиться достатньо давно і пов'язується, перш за все, із підвищенням ефективності діяльності органів правосуддя, діджиталізацією держави та її правових інституцій, а також захистом даних, які знаходяться в обігу під час досудового розслідування, судового розгляду та виконання рішень (покарань).

Історично застосування автоматизованих систем здійснювалося з метою використання сучасних інформаційних технологій для підвищення якості або оптимізації слідчої діяльності (В. Ю. Шепітько, В. В. Білоус, Г. К. Авдєєва, Л. І. Керик)[2], алгоритмізацією слідчої діяльності (В. Ю. Шепітько, Г. К. Авдєєва)[3], програмування розслідування (В. А. Журавель)[4], техніко-криміналістичного забезпечення органів досудового слідства (В. Ю. Шепітько)[5], використання криміналістичних технологій (В. В. Тіщенко, А. А. Барцицька[6], В. В. Семеногов[7]) або наукової організації управлінської праці (В. М. Плішкін)[8].

---

[1] Див.: п 22 *Довідника із застосування статті 7 Європейської конвенції з прав людини «Ніякого покарання без закону: принцип встановлення законом кримінальних правопорушень і покарань».* <https://www.echr.coe.int/Documents/Guide_Art_7_UKR.pdf> (дата звернення: 13.09.2022)

[2] Шепітько В. Ю., Білоус В. В., Керик Л. І. 'Роль інформаційних технологій в підвищенні якості слідчої діяльності' (2008) 17. Питання боротьби зі злочинністю 252–264; Шепітько В. Ю., Авдєєва Г. К. 'Інформаційні технології в криміналістиці та слідчій діяльності' (2010) 19. Питання боротьби зі злочинністю 194–202.

[3] Шепітько В. Ю., Авдєєва Г. К. 'Проблеми алгоритмізації слідчої діяльності' (2008) 44 Актуальні проблеми держави і права 46–50.

[4] Журавель В. А. 'Програмування як засіб підвищення якості розслідування' *Теоретичні основи забезпечення якості кримінального законодавства та правозастосовчої діяльності у сфері боротьби зі злочинністю в Україні*. Матеріали науково-практична конференція. (15 трав. 2009, м. Харків) 175–178.

[5] Шепітько В. Ю. 'Техніко-криміналістичне забезпечення органів досудового слідства та якості слідчої діяльності' *Теоретичні основи забезпечення якості кримінального законодавства та правозастосовчої діяльності у сфері боротьби зі злочинністю в Україні*. Матеріали наукової конференції (15 трав. 2009 р., м. Харків) 33–36.

[6] Тіщенко В. В., Барцицька А. А. *Теоретичні засади формування технологічного підходу в криміналістиці: монограф* (Фенікс, 2012) 198

[7] Семеногов В. В. 'Поняття й види криміналістичних технологій під час розслідування злочинів' (2014) 6. Порівняльно-аналітичне право 334–337.

[8] Плішкін В. М. *Теорія управління органами внутрішніх справ: підруч.* за ред. Ю. Ф. Кравченка. (Національна академія внутрішніх справ, 1999) 670–690

Необхідність впровадження автоматизованих сисетм також підтверджується і загальним науково-технічним прогресом, викликами сучасності. Так, реальністю став обіг таких термінів як цифровий доказ (інформація в електронній (цифровій) формі, що має значення для досудового розслідування та судового розгляду й надається стороною провадження (справи) для її оцінки слідчим, прокурором аюо судом), цифровий слід (слід активності користувача комп'ютером або гаджетом, що збирається з його відома або без такого), цифрова криміналістика (окрема криміналістична теорія та вид судової експертизи, що ставить своїм завданням дослідження цифрових доказів з використанням криміналістичної техніки та наявних методик в цілях досудового розслідування та судового розгляду)[1].

Такий підхід підтвердження загальну цифровізацію суспільства та держави й створює підстави для створення автоматизованих систем, а також в перспективі штучного інтелекту. Одразу слід зазначити, що в чинному та проєкті нового КК України проблема застосування із кримінальною протиправною метою штучного інтелекту (далі – ШІ) та встановлення механізму кримінальної відповідальності не вирішена. Однак 6 жовтня 2021 р. Європейський парламерт прийняв резолюцію з штучного інтелекту в кримінальному праві та його застосування поліцією та судовими органанми в кримніальних цілях (2020/2016(INI))[2]. Зокрема, на нашу думку, важливо звернути увагу на деякі акценти, здійснені в даній резолюції Європейського парламенту. Підкреслюється наявність силової асиметрії між тими, хто використовує технології ШІ, та тими, хто їх підкоряється; наголошується, що вкрай важливо, щоб використання інструментів ШІ правоохоронними та судовими органами не стало фактором нерівності, соціального розколу чи ізоляції; підкреслюється вплив використання інструментів ШІ на права захисту підозрюваних, проблеми з отриманням значної інформації про них. Також приймається до уваги ризики, пов'язані, зокрема, з витоками даних, порушеннями безпеки даних та несанкціонованим доступом до персональних даних та іншої інформації, пов'язаної, наприклад, із кримінальними розслідуваннями або судовими справами, що обробляються системами ШІ; підкреслюється, що аспекти безпеки систем ШІ, що використовуються у правоохоронних органах та судових органах, мають бути ретельно розглянуті правоохоронними та судовими органами використовувати лише додатки ШІ, які дотримуються принципу конфіденційності та захисту даних, щоб уникнути повзучості функцій. Наголошується і на тому, що жодна система ШІ, яка використовується правоохоронними чи судовими органами, не повинна завдавати шкоди фізичній недоторканності людей, а також розподіляти права або накладати юридичні зобов'язання на окремих осіб. Так само наголошується, що жодна система ШІ, яка використовується правоохоронними чи судовими органами, не повинна завдавати шкоди фізичній недоторканності людей, а також розподіляти права або накладати юридичні зобов'язання на окремих осіб. Європейський парламент визнає проблеми правильного визначення юридичної відповідальності та відповідальності за потенційні збитки, враховуючи складність розробки та експлуатації систем ШІ; вважає за необхідне створити чіткий та справедливий режим для розподілу юридичної відповідальності та відповідальності за потенційні несприятливі наслідки, викликані цими передовими цифровими технологіями; підкреслює, однак, що мета повинна полягати, перш за все, у запобіганні будь-яким таким наслідкам; тому закликає застосовувати принцип обережності у всіх застосуваннях ШІ у контексті правоохоронної діяльності; наголошує, що юридична відповідальність та відповідальність завжди повинні пов'язуватися з фізичною або юридичною особою, яка завжди має бути ідентифікована для прийняття рішень, що приймаються за підтримки ШІ; тому наголошує на необхідності забезпечення прозорості корпоративних структур, які виробляють та керують системами ШІ (п.10–13 резолюції Європейського парламенту).

У контексті дослідження впливу ШІ на кримінальну відповідальність останнім часом здійснено достатні серйозні спроби досліджень, які були здійснені через підготовку до чергового XXI Міжнародного конгресу карного права 2024 «Штучний інтелект та кримінальна юстиція» Міжнародної асоціації карного права. В плані підготовки до нього національним групам було запропоновано підготувати відповіді на питання, пов'язані із особливостями відображення проблем кримінального відповідальності в Загальній та Особливій частині Кримі-

[1] Див.: Шепітько В., Шепітько М. *Кримінальне право, криміналістика та судові науки: енциклопедія.* (Право, 2021) 129–130.

[2] Див.: 'Європейський парламент' <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html> (дата звернення: 13.09.2022)

нального права, а також особливостей правового регулювання данної сфери предиктивним здійсненням полійцейської діяльності та правосуддя, а також особливостей впливу ШІ на судову взаємодію та Міжнародне кримінальне /гуманітарне право[1].

Паралельно із підготовкою до XXI Міжнародного конгресу карного права 2024 був підготовлений окремий том Міжнародного огляду карного права, присвячений проблемам ШІ, великих даних, автоматизованих систем, які застосовуються в сфері кримінальної юстиції[2]. Г. Вермеулен, Н. Першак та Н. Реккіа звертають увагу, що підготовка цього випуску пов'язана із зростаючою інформаованістю про можливості та лімітованість систем ШІ в сфері кримінальної юстиції і потрібно для того, щоб бути краще підготовленим для майбутнього, яке у нас вже настало[3]. Підтвердженням такого погляду в майбутнє є дослідження й вітчизняних вчених, які вже ставлять питання про штучний інтелект як суб'єкта злочину (О. Радутний)[4].

[1] Див.: 'Міжнародної асоціації карного права' <https://www.penal.org/en/information> (дата звернення: 13.09.2022)

[2] Див.: International Review of Penal Law. Vol. 92, is. 1, 2021. 244 p.

[3] Vermeulen G., Peršak N., Recchia N. 'Preface: capabilities and limitations of AI in criminal justice' Vol. (2021) 92, (1) International Review of Penal Law. P. 7.

[4] Радутний О. Е. 'Штучний інтелект як суб'єкт злочин' (2017) 4 (23) Інформація і право 106–115.

Висновки. На нашу думку, застосування ст. 376–1 КК України, яка фактично одноосібно забезпечує захист інформації під час здійснення правосуддя потребує певного уточнення. Перш за все, це стосується надання точного переліку автоматизованих систем, які потребують такого захисту. Наступном необхідним етапом є розширення такої цифрової інформації в бік діяльності не тільки судових органів, але й органів, які здійснюють досудове розслідування та виконання покарань (рішень), що викликано створенням відповідних електронних проваджень і загальним поступовим переходом від паперових до електронних справ. Аналогічною є тенденція щодо все більшої зростаючої необхідності застосування дистанційних засобів проведення опитування та допиту з дотриманням відповідних процесуальних, криміналістичних та технічних стандартів. Важливу роль у сфері забезпечення інформаційної безпеки під час здійснення правосуддя стане впровадження штучного інтелекту в найближчому майбутньому, що зробить необхідним здійснити обмеження його застосування та особливостей кримінальної відповідальності не тільки за втручання, а і за його діяльність, що опосередковано вказується у вищеназваній резолюції Європейського парламенту.

REFERENCES

Bibliography

Authored books

1. Dudorova O. O., Pysmenskoho Ye. O. (red) *Kryminalne pravo (Osoblyva chastyna): pidruchnyk* [Criminal law (Special part): textbook] T. 2. (Elton-2, 2012) 704 (in Ukrainian)
2. Tiutiuhin V. I., Shepitko M. V. *Kryminalni pravoporushennia, yaki posiahaiut na vidnosyny, shcho zabezpechuiut realizatsiiu konstytutsiinykh pryntsypiv pravosuddia i nalezhne vykonannia osobamy, shcho yoho zdiisniuiut svoikh profesiinykh (sluzhbovykh) obov'iazkiv. Kryminalne pravo. Osoblyva chastyna.* [Criminal offenses that encroach on relations that ensure the implementation of constitutional principles of justice and the proper performance by persons performing their professional (official) duties. Criminal Law. A special part] Za red. V. Ya. Tatsiia, V. I. Borysova, V. I. Tiutiuhina (Pravo, 2020) 642–652 (in Ukrainian)
3. Tishchenko V. V., Bartsytska A. A. *Teoretychni zasady formuvannia tekhnolohichnoho pidkhodu v kryminalistytsi: monohraf* [Theoretical foundations of the formation of a technological approach in criminology: a monograph] (Feniks, 2012) 198 (in Ukrainian)
4. Plishkin V. M. *Teoriia upravlinnia orhanamy vnutrishnikh sprav: pidruch.* [Theory of management of internal affairs bodies: tutorial] za red. Yu. F. Kravchenka. (Natsionalna akademiia vnutrishnikh sprav, 1999) 702 (in Ukrainian)
5. Shepitko V., Shepitko M. Kryminalne pravo, kryminalistyka ta sudovi nauky: entsyklopediia [Criminal law, criminology and forensic sciences: an encyclopedia] (Pravo, 2021) 508 (in Ukrainian)

Non-authored books

6. *Dovidnyk iz zastosuvannia statti 7 Yevropeyškoï konventsiï z prav liudyny «Niiakoho pokarannia bez zakonu: pryntsyp vstanovlennia zakonom kryminalnykh pravoporushen i pokaran»* [Handbook on the application of Article 7 of the European Convention on Human Rights «No punishment without law: the principle of establishing criminal offenses and punishments by law».] <https://www.echr.coe.int/Documents/Guide_Art_7_UKR.pdf> (in Ukrainian)

Journal articles

7. Batyrhareieva V. S. 'Kontseptualna model zakhystu informatsinoho prostoru Ukrainy zasobamy kryminalnoho prava' [Conceptual model of protection of the information space of Ukraine by means of criminal law] (2020) 1 (32) Informatsiia i pravo 110–119 (in Ukrainian)
8. Kozak V. A. 'Kryminalna vidpovidalnist za nezakonne vtruchannia v robotu avtomatyzovanoi systemy dokumentoobihu sudu: analiz osnovnoho slkadu zlochynu' [Criminal liability for illegal interference in the operation of the court's automated document management system: analysis of the main sequence of the crime] (2013) 122 Problemy zakonnosti 151–158 (in Ukrainian)
9. Nersesian A. S. 'Avtomatyzovana systema dokumentoobihu sudu yak obgiekt kryminalno-pravovoi okhorony' [Automated court document management system as an object of criminal law protection] (2018) 29 Pravova derzhava 275–281 (in Ukrainian)
10. Shepitko V. Yu., Bilous V. V., Keryk L. I. 'Rol informatsiinykh tekhnolohii v pidvyshchenni yakosti slidchoi diialnosti' [The role of information technologies in improving the quality of investigative activities] (2008) 17. Pytannia borotby zi zlochynnistiu 252–264 (in Ukrainian)
11. Shepitko V. Yu., Avdieieva H. K. 'Informatsiini tekhnolohii v kryminalistytsi ta slidchii diialnosti' [Information technologies in forensics and investigative activities] (2010) 19. Pytannia borotby zi zlochynnistiu 194–202 (in Ukrainian)
12. Shepitko V. Yu., Avdieieva H. K. 'Problemy alhorytmizatsii slidchoi diialnosti' [Problems of algorithmization of investigative activity] (2008) 44 Aktualni problemy derzhavy i prava 46–50 (in Ukrainian)
13. Semenohov V. V. 'Poniattia y vydy kryminalistychnykh tekhnolohii pid chas rozsliduvannia zlochyniv' [Concepts and types of forensic technologies during the investigation of crimes] (2014) 6. Porivnialno-analitychne pravo 334–337 (in Ukrainian)
14. International Review of Penal Law (2021) 92 (1) 244 (in English)
15. Vermeulen G., Peršak N., Recchia N. 'Preface: capabilities and limitations of AI in criminal justice' (2021) 92 (1) International Review of Penal Law 7 (in English)
16. Radutnyi O. E. 'Shtuchnyi intelekt yak subiekt zlochyn' [Artificial intelligence as a subject of crime] (2017) 4 (23) Informatsiia i pravo 106–115 (in Ukrainian)

Conference papers

17. Zhuravel V. A. 'Prohramuvannia yak zasib pidvyshchennia yakosti rozsliduvannia' [Programming as a means of improving the quality of investigation] *Teoretychni osnovy zabezpechennia yakosti kryminalnoho zakonodavstva ta pravozastosovchoi diialnosti u sferi borotby zi zlochynnistiu v Ukraini*. Materialy naukovo-praktychna konferentsiia. (15 trav. 2009, m. Kharkiv) 175–178 (in Ukrainian)
18. Shepitko V. Yu. 'Tekhniko-kryminalistychne zabezpechennia orhaniv dosudovoho slidstva ta yakosti slidchoi diialnosti' [Technical and forensic support of pretrial investigation bodies and the quality of investigative activity] Teoretychni osnovy zabezpechennia yakosti kryminalnoho zakonodavstva ta pravozastosovchoї diialnosti u sferi borotby zi zlochynnistiu v Ukraini. Materialy naukovoi konferentsii (15 trav. 2009 r., m. Kharkiv) 33–36 (in Ukrainian)

Websites

19. 'Ofis Heneralnoho prokurora' [Office of the Prosecutor General] <https://new.gp.gov.ua/ua/posts/statistika> (in Ukrainian)
20. 'Iedynyi derzhavnyi reiestr sudovykh rishen' [Unified state register of court decisions] <https://reyestr.court.gov.ua> (in Ukrainian)
21. 'European Parliament' <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html> (in English)
22. 'Mizhnarodna asotsiatsiia karnoho prava' [International Criminal Law Association] <https://www.penal.org/en/information> (in Ukrainian)

Шепітько М. В.
Кримінально-правова охорона інформаційної безпеки під час здійснення правосуддя

У статті здійснена спроба дослідження кримінально-правової охорони інформаційної безпеки під час здійснення правосуддя. Здійснено акцент на тому, що розвиток інформаційних технологій, цифрової інформації, дистанційних форматів діяльності надало можливість її застосовувати в сфері кримінальної юстиції. Найбільш

близькими сферами застосування інформаційних технологій в кримінальній юстиції стало впровадження автоматизованих систем, що прослідковується по багатьом роботам криміналістам, а також спробам впровадження Автоматизованих робочих місць професійних учасників кримінального провадження. Разом із цим відслідковується процес впровадження і відповідного захисту Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС), що включає в себе електронний кабінет, електронний суд та відеоконференцзв'язку.

Кримінально-правовий захист автоматизованих систем, що діють в сфері правосуддя, через застосування ст. 376–1 КК України, потребує певного уточнення. Здійснено висновки про необхідність надання точного переліку автоматизованих систем, які потребують такого захисту. Наступном необхідним етапом є розширення такої цифрової інформації в бік діяльності не тільки судових органів, але й органів, які здійснюють досудове розслідування та виконання покарань (рішень), що викликано створенням відповідних електронних проваджень і загальним поступовим переходом від паперових до електронних справ. Аналогічною є тенденція щодо все більшої зростаючої необхідності застосування дистанційних засобів проведення опитування та допиту з дотриманням відповідних процесуальних, криміналістичних та технічних стандартів. Важливу роль у сфері забезпечення інформаційної безпеки під час здійснення правосуддя стане впровадження штучного інтелекту в найближчому майбутньому, що зробить необхідним здійснити обмеження його застосування та особливостей кримінальної відповідальності не тільки за втручання, а і за його діяльність, що опосередковано вказується у вищеназваній резолюції Європейського парламенту.

***Ключові слова**: кримінально-правова охорона, кримінальна відповідальність, інформаційна безпеки, штучний інтелект, кримінальні правопорушення проти правосуддя*

Shepitko M. V.

Criminal law protection of informative security during administration of justice

Author is tried to pay attention to the criminal law protection of information security during the administration of justice in this article. Emphasis is placed on the fact that the development of information technologies, digital information, online mode of activity has made it possible to apply it in the field of criminal justice. The closest areas of application of information technologies in criminal justice were the implementation of automated systems, which is traced to many works of criminalists, as well as attempts to implement automated workplaces of professional participants in criminal proceedings. At the same time, the process of implementation and appropriate protection of the Unified Judicial Information and Telecommunication System, which includes an electronic office, an electronic court, and video conferencing, is monitored.

Criminal legal protection of automated systems operating in the sphere of justice, through the application of Art. 376–1 of the Criminal Code of Ukraine, needs some clarification. Conclusions were made about the need to provide an accurate list of automated systems that will need such protection. The next necessary stage is the expansion of such digital information towards the activities of not only judicial bodies, but also bodies that carry out pre-trial investigation and execution of punishments (decisions), which is caused by the creation of relevant electronic proceedings and the general gradual transition from paper to electronic cases. A similar trend is the growing need to use remote means of conducting interviews and interrogations in compliance with the relevant procedural, criminalistic and technical standards. An important role in the field of ensuring information security during the administration of justice will be the introduction of artificial intelligence (AI) in the near future, which will make it necessary to limit its use and the specifics of criminal liability not only for interference, but also for its activity, which is indirectly indicated in the above-mentioned resolution of the European Parliament.

***Keywords:** criminal law protection, criminal liability, informative security, artificial intelligence, criminal offenses against justice*

Стаття надійшла до редакції:17.10.2022 р.
Прийнята до друку: 5.11.2022 р.