УДК 343.9
DOI https://doi.org/10.32782/yuv.v3.2025.10

Я. Неділько,
доктор філософії в галузі права,
асистент кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка

ІСТОРІЯ СТАНОВЛЕННЯ ТА РОЗВИТКУ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

Постановка проблеми. Стрімке впровадження інформаційних комп'ютерних технологій (планшетів, ноутбуків, персональних комп'ютерів тощо) у всі сфери нашого суспільного життя сприяє не лише автоматизації важливих процесів, а й надає можливість особам використовувати їх у своїх протиправних цілях.

Згідно зі статистичними даними Офісу Генерального прокурора, серед кримінальних правопорушень, передбачених ст. ст. 361–363-1 розділу XVI КК України, спостерігається тенденція щодо збільшення їх вчинення. Якщо впродовж 2021 року обліковано 3310 (до суду з обвинувальним актом направлено 1947 (58,82%)), то вже 2022 року їх було 3415 (2435), 2023-го – 3841 (2455), 2024-го – 4055 (2647) [1]. Таким чином, з 2021 по 2024 рік кількість вчинених кримінальних правопорушень зазначеної категорії збільшилась приблизно на 22.5%.

Однак, дана статистична інформація не повністю відображає ситуацію щодо вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій в Україні, оскільки обмежується лише розділом XVI КК України та залишає поза увагою інші кримінальні правопорушення, що можуть вчинятися з використанням інформаційних комп'ютерних технологій.

Наведені статистичні показники дають підстави стверджувати про низьку результативність розслідування зазначених кримінальних правопорушень, обумовлені специфікою виявлення, фіксування, вилучення, зберігання, дослідження, оцінки та використання електронних доказів.

На нашу думку, сприяти ефективному розслідуванню кримінальних кіберправопорушень, повинні положення цифрової криміналістики, яка почала формуватися у результаті стрімкого розвитку засобів інформаційно-комп'ютерних технологій, що зумовило появу нових видів доказів – електронних і потребу в розробці сучасних методів їх виявлення, фіксації, вилучення, зберігання, дослідження, оцінки та використання.

Також, слід враховувати інтенсивний розвиток штучного інтелекту, який може бути використаний як злочинцями при вчиненні кримінальних правопорушень, так і правоохоронними органами для профілактики, виявлення, запобігання та їх розслідування. Тому саме на цифрову криміналістику повинно покладатися дослідження й аналіз та розробка дієвих методик і рекомендацій по ефективному використанню штучного інтелекту у кримінальному провадженні.

І хоча дослідження цифрової криміналістики привертає на себе увагу низки вітчизняних вчених-криміналістів, певні її структурні (системні) елементи, зокрема історія становлення та розвитку, яка відіграла важливу роль у її формуванні, залишаються малодослідженими.

Метою статті є аналіз становлення та розвитку цифрової криміналістики як окремої криміналістичної теорії (вчення), що спрямований на систематизацію ключових етапів її формування як у світі, так і в Україні. Це дозволить не лише збагатити її теоретичні положення, але й визначити основні виклики й перспективи розвитку в умовах стрімкого поширення інформаційно-комп'ютерних технологій та штучного інтелекту, забезпечуючи ефективне проведення розслідувань кримінальних правопорушень.

Виклад основного матеріалу. Уперше електронно-обчислювальні машини (ЕОМ) з'явилися у другій половині XX століття. Дату створення першого комп'ютера прийнято пов'язувати з розробкою та впровадженням Електронного цифрового інтегратора та комп'ютера (ENIAC) у 1943 році. Повністю робочим ENIAC вдалося зробити тільки у листопаді 1945 року. На той час він міг виконувати п'ять тисяч додавань та віднімань за секунду, був тридцять метрів завдовжки та два з половиною метри заввишки, займав площу 167 квадратних метри, а також важив близько тридцяти тон [2, с. 76].

У наш час комп'ютери є меншими за розмірами та вагою, мають швидкісний процесор і можуть поміщатися у кишені людини.

Аналізуючи історію створення електронно-обчислювальних машин за видами інструментарію технологій, науковці виокремлюють декілька етапів їх становлення:

1) «ручний» (з давніх часів до другої половини XIX ст.), який вирізняється ручною обробкою інформації (за допомогою пера й рахівниць), а зв'язок відбувався шляхом пересилання листів і пакетів;

2) механічний (з кінця XIX ст.), що ознаменувався винайденням друкарської машинки й телефону, вдосконаленням системи поштового зв'язку;

3) електричний (з 1940-х років XX ст. до 1960 років XX ст.) – розроблення перших електронно-обчислювальних машин (ЕОМ) і створення електричних писальних машинок, копіювальних технічних пристроїв тощо;

4) електронний (з початку 70-х років XX ст.) – створення на базі ЕОМ автоматизованих систем управління та інформаційно-пошукових систем, що оснащені широким спектром базових і програмних комплексів;

5) комп'ютерний етап (із середини 80-х рр. XX ст.) – «комп'ютерна» («нова») технологія, головним обладнанням якої є персональний комп'ютер [3].

Саме з виникненням і розвитком персональних комп'ютерів більшість вітчизняних та зарубіжних вчених пов'язують появу «комп'ютерних злочинів», що привело до подальшого формування цифрової криміналістики.

З цього приводу, Марк Полліт зазначав, що у період з 1985–1995 рік відбувається зародження цифрової криміналістики як окремої галузі. З'являються перші організації, зокрема Міжнародна асоціація комп'ютерних слідчих спеціалістів, яка починає займатися питаннями дослідження електронних доказів [4, с. 6].

У національних законодавствах зарубіжних країн появляються відповідні норми, що криміналізують «комп'ютерні злочини». Наприклад, Федеративна Республіка Німеччина у травні 1986 року внесла зміни в КК ФРН та закріпила кримінальну відповідальність за комп'ютерне шахрайство (§263a); незаконне отримання відомостей, які можуть бути відтворені або передані електронним або магнітним шляхом (§ 202a); комп'ютерний саботаж (§ 303b) [5].

У жовтні того самого року в США прийнято федеральний закон «Про комп'ютерне шахрайство та зловживання», головна мета якого полягає

в захисті секретної, фінансової та кредитної інформації, що розміщена в комп'ютерах уряду чи фінансових установ. Цей нормативний акт вніс низку поправок у 18-й звід законів США, главу 41, § 1030, а саме криміналізував такі дії: крадіжку майна за допомогою комп'ютера, що здійснюють у формі обману; змінення, пошкодження або знищення даних, що належать іншим особам, і незаконний продаж паролів [6].

1990 року прийнято закон про неправомірне використання комп'ютерів у Великій Британії [7]. Також 1994 року набув чинності КК Франції, у якому містився окремий розділ «Порушення в роботі автоматизованої системі обробки даних» [8].

Також, у даний період створюються відповідні комп'ютерні програми для дослідження електронних слідів, які дозволяли виготовлювати судово-криміналістичні образи-дисків [4 с. 7].

Отже, саме у цей час починає зароджуватися цифрова криміналістики, оскільки набувають активного поширення «комп'ютерні злочини», вчинення яких залишає за собою «електронні сліди», що послуговує створенню та вдосконаленню засобів виявлення, вилучення й дослідження таких слідів.

Далі можна зазначити про активне становлення цифрової криміналістики у світі (1995–2005), що обумовлено трьома факторами: 1) розвитком технологій – активного поширення набуває мережа Інтернет, вдосконалення телефонів і комп'ютерів, у більшості людей з'являється електронна пошта тощо; 2) розвитком злочинності, зокрема збільшенням випадків розповсюдження дитячої порнографії за допомогою мережі Інтернет, що призвело до необхідності вилучення електронних доказів; 3) використанням терористами комп'ютерів як знарядь вчинення злочинів, що зумовило правоохоронний та військовий сектор активізувати розвиток цифрової криміналістики на потребу часу [4, с. 9–10].

Вказані чинники змушують удосконалювати криміналістичні програми для роботи з електронними доказами, які використовують під час судово-комп'ютерних експертиз.

Саме у даний час, починає вперше застосовуватися та набуває широкого поширення в наукових колах термін «кіберзлочин» [9, с. 477], а також відбувається прийняття Конвенції про кіберзлочинність (Будапештська конвенція), яка стала першим міжнародним документом, спрямованим на боротьбу з «комп'ютерними злочинами» [10] та Додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [11].

Третій період тривав з 2005 по 2010 рік і характеризувався глобальним поширенням використання мережі Інтернет [4, с. 11]. Так, за статистичними даними з 2005 по 2010 рік кількість користувачів мережі Інтернет збільшилась з 1 до 2 мільярдів людей [12].

До того ж, відбувається масове поширення пристроїв Apple, зокрема телефонів iPhone на операційній системі iOS, а також швидкого розповсюдження набувають засоби інформаційно-комп'ютерних технологій на базі Android, що змушує експертів у галузі цифрової криміналістики створювати нові програми по роботі з електронними доказами.

Також, відбувається розвиток веб-сервісів таких як YouTube, Facebook, Reddit, Twitter тощо, які змінюють способи передачі інформації між людьми, а електронна пошта стає основним джерелом доказової інформації у кримінальних правопорушеннях, вчинених з використанням інформаційних комп'ютерних технологій.

Четвертий період (2010–2022) характеризується високим рівнем зростання кіберзлочинності, який

вже набуває світового масштабу. Сюди можна віднести викриття даних 2010 року, зроблені WikiLeaks, масштабні кібератаки на приватні та урядові веб-ресурси, викрадення секретних даних тощо. Особливо характерним для даного періоду є те, що починають з'являтися потужні віруси, такі як Stuxnet і WannaCry. Крім того, цей період відзначився активним формуванням та діяльністю кіберзбройних угруповань, значним зростанням випадків використання програм-вимагачів і розвитком методів соціальної інженерії. Також на світову арену кіберзлочинності вийшов Даркнет, який став основним інтернет-середовищем для торгівлі викраденими даними, наркотиками, зброєю тощо.

Міжнародна спільнота гостро реагує на дані протиправні виклики, створюючи стратегії по боротьбі з кіберзлочинами, а також керівні принципи та рекомендації щодо роботи з електронними доказами та розслідуванням кримінальних кіберправопорушень.

Варто зазначити про створення у 2020 році протоколу Берклі. Даний документ є практичним посібником, який окреслює мінімальні стандарти та надає загальні міжнародні вказівки щодо пошуку, збирання, зберігання, перевірки та аналізу інформації з відкритих цифрових джерел для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права [13].

Окрім цього, активно впроваджуються та використовуються штучні нейронні мережі у різних сферах, у тому числі й правоохоронній, які надалі стануть ключовим елементом у формуванні сучасних систем штучного інтелекту [14].

П'ятний період розпочинається з прийняттям Другого додаткового протоколу до Конвенції про кіберзлочинність (2022) [15] та стрімким поширенням штучного інтелекту.

У Другому додатковому протоколі [15] зазначено, що поштовхом для його створення слугувало:

– зростання рівня кіберзлочинності у сфері інформаційно-комунікаційних технологій та інтернеті, що ставить під загрозу демократію, верховенство права та права людини;

– збільшення кількості жертв кіберзлочинів;

– необхідність держави нести відповідальність за захист осіб не тільки офлайн, а й онлайн, зокрема шляхом здійснення ефективного досудового розслідування та судового розгляду;

– докази кримінального правопорушення зберігаються в електронній формі в комп'ютерних системах, які знаходяться в юрисдикції іноземних держав.

До того ж, даний період характеризується активним створенням, зміною та доповненням міжнародних нормативних актів у сфері боротьби з кримінальними кіберправопорушеннями. Зокрема, варто зауважити про Регламент ЄС 2023/1543 від 12 липня 2023 року «Про європейські ордери на надання доказів та європейські ордери на збереження електронних доказів у кримінальному провадженні та для виконання покарань, пов'язаних з позбавленням волі, за результатами кримінального провадження» [16] та Директиву ЄС, що встановлює гармонізовані правила щодо визначення визначених установ та призначення законних представників з метою збору електронних доказів у кримінальному провадженні [17].

Як зазначає прокурор Міжнародного кримінального суду Карім Хан, засоби для вчинення серйозних міжнародних злочинів постійно розвиваються – від куль і бомб до соціальних мереж, інтернету та штучного інтелекту. Оскільки держави та інші суб'єкти все частіше вдаються до операцій у кіберпросторі, цей новий засіб ведення війни може бути використаний для вчинення воєнних злочинів, злочинів проти людяності, геноциду

та навіть агресії однієї держави проти іншої [18]. Тому відбувається й вдосконалення положень Римського Статуту відповідно до загроз, що несуть в собі кримінальні кіберправопорушення.

Крім того, проходить активне впровадження штучного інтелекту для автоматизації аналізу великих обсягів даних, прогнозування та ідентифікації кібератак, а також у допомозі в розслідуванні кримінальних правопорушень.

У 2024 Рада Європи відкрила для підписання Рамкову конвенцію про штучний інтелект та права людини, демократію та верховенство права. Дана конвенція забезпечує правову базу, що охоплює весь життєвий цикл систем штучного інтелекту. Він сприяє прогресу та інноваціям у сфері штучного інтелекту, водночас управляючи ризиками, які він може становити для прав людини, демократії та верховенства права [19].

Таким чином, постійне вдосконалення інформаційних комп'ютерних технологій та штучного інтелекту, призводить до подальшого розвитку та вдосконалення положень цифрової криміналістики, розширюючи її можливості у сфері виявлення, дослідження, вилучення та використання електронних доказів, розслідуванні кримінальних кіберправопорушень, а також у галузі по використанню штучного інтелекту в кримінальному провадженні.

Проаналізувавши становлення та розвиток цифрової криміналістики у світі, варто зауважити про її виникнення та вдосконалення в Україні. Досліджуючи формування цифрової криміналістики в України, на нашу думку, можна виокремити наступні чотири періоди.

І період – 1991–2005 роки. Відбувається законодавче закріплення відповідальності за вчинення «комп'ютерних злочинів». Так, КК України 1960 року був доповнений ст. 198-1 «Порушення роботи автоматизованих систем» [20]. Надалі, у новому КК України 2001 року вже було передбачено окремий розділ XVI [21].

Попри те, що в Україні в кінці XX ст. «комп'ютерна злочинність» не була таким масовим явищем (протягом 1997–2001 років зареєстровано 52 посягання, що належали до «комп'ютерних злочинів») [22], українські вчені різних галузей права зосереджували увагу як на теоретичних, так і на практичних аспектах цього криміногенного явища.

Вагомим кроком у боротьбі з кіберзлочинністю стала ратифікація Україною Конвенції про кіберзлочинність у 2005 році [23]. Окрім цього, в експертних установах починає проводитися експертиза комп'ютерної техніки та програмних продуктів як один з видів експертиз [24].

Таким чином, даний період можна охарактеризувати як створення та закріплення нормативної бази, яка послугує основним підґрунтям для подальшого розвитку цифрової криміналістики в Україні.

ІІ період – 2005–2014 роки. У даний період відбувається збільшення використання інтернету в Україні. Зокрема у 2005 році тільки 16% населення України використовувало Інтернет, а вже у 2012 році даний показник сягнув 43% [25].

Зі збільшенням кількості користувачів інтернету, кіберзлочинність в Україні еволюціонувала від поодиноких випадків до чітких організованих форм. Основними видами протиправних діянь даного періоду було розповсюдження шкідливого програмного забезпечення, крадіжка номерів кредитних карт і банківських рахунків (кардинг), злом паролів, порушення авторських прав (піратство) тощо.

Це все змусило нашу державу швидко та ефективно реагувати на відповідні загрози. Тому, у липні 2009 року в структурі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми МВС, було створено окремий відділ боротьби

з кіберзлочинністю. Наприкінці 2012 року у складі кримінальної міліції МВС України створюється вже самостійний структурний підрозділ – Управління боротьби з кіберзлочинністю [26].

У структурі СБУ відповідно до Указу Президента України від 25 січня 2012 року було створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, який почав відповідати за стан державної безпеки в кібернетичній та інформаційній сферах [27].

Отже, II період можна охарактеризувати створенням відповідних правоохоронних органів по боротьбі з кіберзлочинністю в України, що зумовлено стрімким розвитком кіберзлочинності.

III період відноситься до 2014–2022 років. Даний етап характеризується активною реакцією України на зростаючу кіберзлочинність та гібридні загрози, що особливо загострилися після збройного вторгнення 2014 року.

Однією з найважливіших подій стало створення Департаменту кіберполіції Національної поліції України у жовтні 2015 року. Даний орган зосередився на запобіганні, виявленні, припиненні та розкритті кіберзлочинів, а також на техніко-криміналістичному забезпеченні їх розслідування.

Створення Департаменту кіберполіції виявилось своєчасним та необхідним кроком, оскільки протягом наступних років рівень кримінальних кіберправопорушень суттєво збільшувався.

Так, кількість кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, у 2015 році становила 598 випадків. Протягом наступних років їх обсяг значно зріс: у 2016 році було обліковано 865 кримінальних правопорушень, у 2017 – 2573, у 2018 – 2301, у 2019 – 2204, у 2020 – 2498, у 2021 – 3310, а у 2022 році їх кількість склала 3415 правопорушень [1].

Таким чином, в умовах постійного збільшення кримінальних правопорушень зазначеної категорії, виникла необхідність удосконалити нормативно-правове регулювання для забезпечення ефективної боротьби та розслідування даних протиправних діянь.

Тому, у 2017 році було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» [28].

До того ж, для формування потенціалу стримування кіберзагроз у нашій державі та запобігання їхнім небажаним наслідкам Указом Президента України від 26 серпня 2021 року № 477/2021 було введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про стратегію кібербезпеки України» [29].

Крім того, з метою імплементації положень Ланцаротської конвенції 2021 року, Кримінальний кодекс (КК) України доповнено ст. ст. 156-1, 301-1, 302-1, у яких встановлено відповідальність за вчинення будь-яких дій сексуального характеру щодо дітей, зокрема з використанням інформаційних комп'ютерних технологій.

У даний час відбувається й становлення штучного інтелекту, який також починає використовуватися у правоохоронній діяльності, зокрема в розпізнаванні обличь, аналізу великих обсягів даних для прогнозування злочинності, моніторинг поведінки осіб у соціальних мережах тощо.

З 2022 року починається IV період, який триває по наш час. Повномасштабне вторгнення Російської Федерації на територію України стало поштовхом до змін у сфері кібербезпеки та значним розвитком цифрової криміналістики. Зокрема, постала нагальна потреба в отриманні «воєнних доказів», які зберігаються в електронній формі та можуть знаходитися в юрисдикції іноземних держав.

Це зумовило нагальну потребу в подальшому розширенні міжнародного співробітництва у сфері збору електронних доказів у кримінальному провадженні, що знайшло своє відображення у підписанні Україною Другого додаткового протоколу до Конвенції про кіберзлочинність (2022).

Окрім цього, даний період характеризується стрімким поширенням штучного інтелекту, який змінює як засоби вчинення кримінальних правопорушень, так і підходи до їх розслідування. З'являються нові моделі штучного інтелекту (ChatGPT, GPT-4, Gemini тощо), які здатні генерувати текст, відео, музику та зображення, а також виконувати інші завдання. Тому у травні 2025 року Україна підписала Рамкову конвенцію Ради Європи про штучний інтелект, права людини, демократію та верховенство права [30], де визначені принципи, які держава повинна дотримуватися у формуванні законодавства щодо застосування штучного інтелекту.

Варто зазначити, що у цей час активно відбуваються наукові дискусії стосовно місця та ролі цифрової криміналістики у системі вітчизняної криміналістики. Загалом, у науковій літературі під цифровою криміналістикою слід розуміють окрему криміналістичну теорію, що спрямована на розробку засобів і методів з виявлення, фіксування, вилучення, зберігання, дослідження, оцінки та використання електронних доказів, а також надання рекомендацій з виявлення, розслідування та профілактики кримінальних кіберправопорушень [31, с. 232].

Таким чином, Україна продовжує активно працювати над розбудовою стійкої системи кіберзахисту, ефективним проведенням розслідувань кримінальних кіберправопорушень та розвитком експертного потенціалу для ефективної протидії сучасним викликам у кіберпросторі, а також законодавчою базою для врегулювання та використання штучного інтелекту у цих сферах.

Висновки. Підсумовуючи, варто зазначити, що аналіз історії становлення та розвитку цифрової криміналістики свідчить про її постійний динамічний характер формування, який зокрема зумовлений удосконаленням процесів виявлення, фіксування, вилучення, зберігання, дослідження, оцінки та використання електронних доказів, а також засобів і методів розслідування кримінальних кіберправопорушень. Становлення цифрової криміналістики як окремої криміналістичної теорії (вчення) та подальше її вдосконалення є відповіддю на виклики, пов'язані з виникненням нових видів протиправних діянь у кіберпросторі, обумовлених стрімким розвитком засобів інформаційно-комп'ютерних технологій та штучного інтелекту.

У статті аналізується формування цифрової криміналістики як окремої криміналістичної теорії, наводяться ключові етапи її розвитку як у світі, так і в Україні. Зазначається про інтенсивний розвиток штучного інтелекту, який може бути використаний як злочинцями у протиправних цілях, так і правоохоронними органами для профілактики, виявлення, запобігання та розслідування кримінальних правопорушень. Наводяться періоди становлення цифрової криміналістики у світі: 1) з 1985 по 1995 рік; 2) з 1995 по 2005 рік; 3) з 2005 по 2010 рік; 4) з 2010 по 2022 рік: 5) з 2022 по наш час. Кожен з вказаних етапів демонструє розвиток цифрової криміналістики, зокрема у сферах боротьби з кримінальними кіберправопорушеннями, удосконаленням процесів виявлення, фіксування, вилучення, зберігання, дослідження, оцінки та використання електронних доказів,

а також застосування штучного інтелекту у правоохоронній діяльності. Наголошується, що цифрова криміналістика повинна досліджувати, аналізувати та розробляти дієві методики й рекомендації для ефективного використання штучного інтелекту у кримінальному провадженні. Зауважуються періоди становлення цифрової криміналістики в Україні: 1) з 1991 по 2005 рік; 2) 2005–2014 рік; 3) 2014–2022 рік; 4) з 2022 по наш час. Зазначено, що цифрова криміналістика розуміється як окрема криміналістична теорія, спрямована на розробку засобів і методів виявлення, фіксування, вилучення, зберігання, дослідження, оцінки та використання електронних доказів, а також надання рекомендацій з виявлення, розслідування та профілактики кримінальних кіберправопорушень. Констатовано, що становлення цифрової криміналістики як окремої криміналістичної теорії (вчення) та подальше її вдосконалення є відповіддю на виклики, пов'язані з виникненням нових видів протиправних діянь у кіберпросторі, обумовлених стрімким розвитком засобів інформаційно-комп'ютерних технологій та штучного інтелекту.

Ключові слова: цифрова криміналістика, кримінальні кіберправопорушення, штучний інтелект, електронні докази, інформаційно-комп'ютерні технології, розслідування, кіберзлочинність.

Nedilko Ya. The history of the formation and development of digital forensics

The article analyzes the formation of digital forensics as a separate forensic theory, outlining the key stages of its development both globally and in Ukraine. It notes the intensive development of artificial intelligence (AI), which can be used by criminals for illegal purposes, as well as by law enforcement agencies for the prevention, detection, deterrence, and investigation of criminal offenses. The periods of the establishment of digital forensics worldwide are presented as follows: 1) from 1985–1995; 2) from 1995–2005; 3) from 2005–2010; 4) from 2010–2022; 5) from 2022 to the present. Each of these stages demonstrates the evolution of digital forensics, particularly in the areas of combating cybercrime, improving the processes of detecting, recording, seizing, storing, examining, evaluating, and using electronic evidence, and applying AI in law enforcement activities. It is emphasized that digital forensics should research, analyze, and develop effective methodologies and recommendations for the efficient use of AI in criminal proceedings. The periods of the establishment of digital forensics in Ukraine are identified as: 1) from 1991 – 2005; 2) from 2005–2014; 3) from 2014–2022; 4) from 2022 to the present. It is stated that digital forensics is understood as a separate forensic theory aimed at developing means and methods for the detection, recording, seizure, storage, examination, evaluation, and use of electronic evidence, as well as providing recommendations for the detection, investigation, and prevention of cybercrimes. It is concluded that the establishment of digital forensics as a distinct forensic theory (doctrine) and its further improvement is a response to the challenges associated with the emergence of new types of illegal acts in cyberspace, driven by the rapid development of information and computer technologies and artificial intelligence.

Key words: digital forensics, cybercrimes, artificial intelligence, electronic evidence, information and computer technologies, investigation, cybercrime.

Література:

1. Офіс Генерального прокурора. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL: https://surl.li/pakoxe (дата звернення 12.05.2025).

2. Вольтер Айзексон. Інноватори. Як група хакерів, геніїв та тіків здійснила цифрову революцію. Київ, 2017. 488 с.

3. Інформаційно-комунікаційні технології в бізнесі : навч. посіб. / уклад. М.О. Чупріна. Київ : КПІ ім. І. Сікорського, 2020. 116 с. URL: https://ela.kpi.ua/bitstream/123456789/33703/1/Infor_tech.pdf.

4. Pollitt, M. (2010). A History of Digital Forensics. In: Chow, KP., Shenoi, S. (eds) Advances in Digital Forensics VI. DigitalForensics 2010. IFIP Advances in Information and Communication Technology, vol 337. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15506-2_1 (дата звернення 12.05.2025).

5. Bundesgesetzblatt. Ausgegeben zu Bonn am 23. Mai 1986 Nr. 21. URL: https://surl.li/rydgcl (дата звернення 12.05.2025).

6. Winmill B., Metcalf D., Band M. Cybercrime: issues and challenges in the United States. Digital Evidence and Elecronic Signature Law Review. 2010. Vol. 7. P. 19–34. DOI: https://doi.org/10.14296/deeslr.v7i0.1921/ (дата звернення 12.05.2025).

7. Computer Misuse Act 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/1991-02-01 (дата звернення 12.05.2025).

8. Code pŭnal. Version en vigueur au 25 avril 2022. URL: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070719/ (дата звернення 12.05.2025).

9. Tonry M. The Oxford Handbook of Crime and Public Policy Oxford Handbooks. Oxford Universaty Press, 2009. 640 p.

10. Конвенція про кіберзлочинність : міжнар. док. від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 12.05.2025).

11. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : міжнар. док. від 28 січ. 2003 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення 12.05.2025).

12. How many people use the Internet. URL: https://soax.com/research/how-many-people-use-the-internet (дата звернення 15.05.2025).

13. Протокол Берклі з ведення розслідувань з використання відкритих цифрових даних. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення 15.05.2025).

14. Неділько Я. В. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. Криміналістика і судова експертиза. 2021. Вип. 66. С. 453–461. DOI: 10.33994/kndise.2021.66.43.

15. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. URL: https://rm.coe.int/1680a49dab (дата звернення 15.05.2025).

16. Регламент (ЄС) 2023/1543 Європейського Парламенту та Ради від 12 липня 2023 року про європейські ордери на пред'явлення доказів та європейські ордери на збереження електронних доказів у кримінальному провадженні та для виконання покарань, пов'язаних з позбавленням волі, за результатами кримінального провадження. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng (дата звернення 15.05.2025).

17. Директива (ЄС) 2023/1544 Європейського Парламенту та Ради від 12 липня 2023 року, що встановлює гармонізовані правила щодо визначення визначених установ та призначення законних представників з метою збору електронних доказів у кримінальному провадженні. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj/eng (дата звернення 15.05.2025).

18. ICC Office of the Prosecutor launches public consultation on policy on cyber-enabled crimes under the Rome Statute. URL: https://surl.li/xtmgju (дата звернення 15.05.2025).

19. Council of Europe opens first ever global treaty on AI for signature. URL: https://surl.li/cyhjvm (дата звернення 15.05.2025).

20. Кримінальний кодекс України : Закон УРСР від 28 груд. 1960 р. № 2001-05. URL: https://zakon.rada.gov.ua/laws/show/2002-05#Text (дата звернення 15.05.2025).

21. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 15.05.2025).

22. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. ... канд. юрид. наук : 12.00.08. Київ, 2002. 246 с.

23. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення 15.05.2025).

24. Про затвердження Інструкції про призначення та проведення судових експертиз та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення 15.05.2025).

25. Динаміка проникнення інтернету в Україні. URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=80&page=1 (дата звернення 15.05.2025).

26. Кіберполіція України. URL: https://surl.li/hxhktd (дата звернення 15.05.2025).

27. Про внесення зміни до Указу Президента України від 27 груд. 2005 р. № 1860 : Указ Президента від 25 січ. 2012 р. № 34/2012. URL: https://www.president.gov.ua/documents/342012-13995 (дата звернення 15.05.2025).

28. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163 – 19#Text (дата звернення 15.05.2025).

29. Про рішення Ради національної безпеки і оборони України від 10 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» : Указ Президента України від 1 лют. 2022 р. № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289 (дата звернення 15.05.2025).

30. Ukraine Signs the Council of Europe Framework Convention on AI. URL: https://surli.cc/euuyqj (дата звернення 15.05.2025).

31. Неділько Я. В. Поняття цифрової криміналістики та її місце в системі криміналістики. Криміналістика і судова експертиза. 2024. Вип. 69. С. 228–236. DOI: 10.33994/kndise.2024.69.21.