

УДК 343.2/.7+004.9

**РАДУТНИЙ О.Е.**, доктор філософії (*Ph.D.*) в галузі права, доцент, доцент кафедри кримінального права Національного юридичного університету імені Ярослава Мудрого.  
ORCID: <http://orcid.org/0000-0002-6521-3977>.

## МАНІФЕСТ ЄДНАННЯ ПРАВНИЧИХ ТА ІТ-ПРОФЕСІЙ НА ПРИКЛАДАХ ВИКОРИСТАННЯ У КРИМІНАЛЬНО-ПРАВОВОМУ ЦИКЛІ ОДНОРІДНИХ ПРАКТИК СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

DOI: [https://doi.org/10.37750/2616-6798.2025.2\(53\).334053](https://doi.org/10.37750/2616-6798.2025.2(53).334053)

**Анотація.** В статті розглядаються ознаки, які є спорідненими для сфери права та інформаційних технологій (ІТ), у зв'язку з чим виникають підстави для їх взаємопроникнення та синтезу, в тому числі, через використання міждисциплінарних прийомів, методів і засобів, однакового програмного та апаратного забезпечення тощо. Доведено, що інструментарій ІТ, зокрема, системну аналітику, інженерію даних, машинне навчання, аналітику даних, оброблення природної мови тощо, можливо використовувати у сфері права за багатьма напрямками. Ними можуть бути розслідування кримінальних правопорушень, аналіз правової ситуації, побудова карт злочинності, виявлення аномалій, аналіз потокових даних та патернів кримінальних правопорушень, оцінка та прогнозування ризиків, розподіл ресурсів та обов'язків, візуалізація статистики та руху кримінального провадження, оперативна комунікація та координація, планування, автоматизація рутинних процесів, створення баз знань та даних, управління внутрішніми регламентами тощо. Обґрунтовано, що ключовими аспектами впровадження зазначеного інструментарію в сферу права мають бути: безпека даних, в тому числі, шифрування чутливої інформації, контроль доступу, аудит дій користувачів, резервне копіювання тощо; інтеграція, в тому числі об'єднання різних джерел даних, автоматизація обміну інформацією, стандартизація форматів, забезпечення сумісності систем тощо; навчання персоналу, в тому числі регулярні тренінги, створення інструкцій, технічна підтримка, обмін досвідом тощо. Розглянуто приклади практичного застосування методів та засобів ІТ в сфері права. Наведено додаткові аргументи щодо корисності опанування правниками сучасних технологічних інструментів та(або) розуміння принципів їх роботи. Зокрема, ними визначено стрімку цифрову трансформацію самої правової сфери, зростаючі масштаби використання штучного інтелекту та машинного навчання, появу нових видів кримінальних правопорушень, які безпосередньо пов'язані з розвитком технологій та нових віртуальних просторів тощо. Викладений матеріал надає підстави для висновку, що до трьох основних навичок сучасної культурної людини, як то вміння читати (так, щоб зрозуміти особисто і вміти пояснити іншим), писати (так, щоб лаконічно та переконливо викладати свої думки), а також рахувати, невдовзі будуть додані обізнаність в сучасних технологіях та оволодіння однією з базових ІТ компетентностей. Процеси навчання юриспруденції та програмуванню мають багато спільного, тому навчальні програми повинні формуватися у тісному міждисциплінарному зв'язку між ними.

**Ключові слова:** інформація, інформаційні відносини, інформаційні технології, Великі Дані, право, кримінальне право, кримінальне правопорушення, криминологія, криміналістика, штучний інтелект, машинне навчання, кримінально-правова характеристика, формальна мова, природна мова, прецедент, алгоритмічний підхід, програмування, мова програмування, принцип правової визначеності, принцип технічної визначеності, планування, системний аналіз, нейронна мережа, платформа, предикативна аналітика, візуалізація, база даних, безпека даних.

**Summary:** *The article examines features related to the fields of law and information technology (IT), and thus, there are grounds for their interpenetration and synthesis, including through the use of interdisciplinary techniques, methods, and tools, the same software and hardware, etc. It is proved that IT tools, in particular, system analytics, data engineering, machine learning, data analytics, natural language processing, etc., can be used in law in many areas. These may include criminal investigation, analysis of the legal situation, crime mapping, anomaly detection, analysis of streaming data and patterns of criminal offences, risk assessment and forecasting, allocation of resources and responsibilities, visualization of statistics and criminal proceedings, operational communication and coordination, planning, automation of routine processes, creation of knowledge and databases, management of internal regulations, etc. It is substantiated that the key aspects of the implementation of these tools in the field of law should be: data security, including encryption of sensitive information, access control, audit of user actions, backup, etc.; integration, including combining different data sources, automating information exchange, standardizing formats, ensuring system compatibility, etc.; staff training, including regular training, developing instructions, technical support, exchange of experience, etc. Examples of practical application of IT methods and tools in the field of law are considered. The author provides additional arguments as to the usefulness of lawyers' mastery of modern technological tools and/or understanding of the principles of their operation. In particular, they identify the rapid digital transformation of the legal sphere itself, the growing use of artificial intelligence and machine learning, the emergence of new types of criminal offences that are directly related to the development of technology and new virtual spaces, etc. The material presented above has led to the conclusion that the three basic skills of a modern cultural person, such as the ability to read (so that one can understand personally and be able to explain to others), write (so that one can express one's thoughts concisely and convincingly), and calculate, will soon be supplemented by awareness of modern technologies and mastery of one of the basic IT competencies. The processes of learning law and programming have much in common, so curricula should be developed in close interdisciplinary connection between them.*

**Keywords:** *information, information relations, information technology, Big Data, law, criminal law, criminal offence, criminology, forensics, artificial intelligence, machine learning, criminal law characterization, formal language, natural language, precedent, algorithmic approach, programming, programming language, principle of legal certainty, principle of technical certainty, planning, system analysis, neural network, platform, predictive analytics, visualization, database, data security.*

**Постановка проблеми.** Правники та представники більшості професій у сфері інформаційних технологій (далі – ІТ-професій), зокрема розробники програмного забезпечення, аналітики та спеціалісти з обробки даних, інженери зі штучного інтелекту та машинного навчання, мають набагато більше спільного, ніж може видатися на перший погляд. Обидві розглядувані галузі не розділені такими принциповими відмінностями, щоб це стало перешкодою для їх взаємопроникнення, обміну, або поступового зрощення. На користь цього свідчать численні аргументи та приклади на їх підтвердження, зокрема, щодо спільних вимог відносно структурованої логіки мислення, роботи з символами, образами, прецедентами та формальними мовами, необхідності перманентного пошуку та виправлення помилок, оновлення знань, важливості правил та документації, формулювання та додержання засадничих принципів, важливості командної роботи та ефективної комунікації, творчого підходу у рамках існуючих обмежень тощо.

*Структурована логіка мислення.* Представникам правничих та ІТ-професій критично важливо розвивати чітке логічне мислення. Так, юристи аналізують нормативні акти, документи та правові ситуації, виокремлюють їх складові частини, застосовують певні шаблони та релевантні норми права у їх системному зв'язку між собою. З свого боку, представники ІТ-професій так само деталізують складні завдання шляхом виокремлення більш простих компонентів, застосовують до них відповідні

усталені шаблони та певні алгоритми. Таким чином, структурована логіка алгоритмічного мислення, оптимізація рішень, здатність аналізувати інформацію, будувати чіткі аргументи та ланцюжки для доведення або спростування певної позиції, встановлювати логічні зв'язки та знаходити ефективні рішення, а так само використання дедукції та індукції, умовних операторів, циклів, рекурсії, чітке формулювання тверджень для уникнення двозначностей та інші навички є ключовими для представників розглядуваних професій з урахуванням специфіки контекстів.

*Робота з формальними мовами, образами та символами.* Правники працюють з мовою права, яка має свій символізм, образність, структуру, синтаксис, семантику, термінологію та правила інтерпретації. У свою чергу, розробники та тестувальники програмного забезпечення, аналітики та спеціалісти з обробки даних, інженери зі штучного інтелекту та фахівці з кібербезпеки мають справу з мовами програмування, яким також властиві наведені ознаки. В обох випадках необхідно розуміти, як правильно конструювати або опанувати відповідну архітектуру тверджень та вміти інтерпретувати їх значення. В юриспруденції *input* (“введення, початок логічної операції у програмуванні”) тексту “таємне викрадення чужого майна” або “одна сторона передає або зобов’язується передати майно у власність іншій стороні, яка приймає або зобов’язується прийняти таке майно і сплатити за нього певну грошову суму” на виході (*output* – у програмуванні) видає результат “крадіжка” або “договір купівлі-продажу” відповідно, що вказує на спорідненість у підходах до формулювання архітектури логіки і мови, які використовують структурно пов’язані словесні та(або) математичні формули та образи. Той фахівець, який оперує більшою кількістю згаданих символів, формальних мов та образів, є більш ефективним у кожній з розглядуваних сфер діяльності. Правник, який з задоволенням занурюється у деталі контракту або норми права у пошуках змісту, зв’язків та інсайтів (від *insight* – “осягнення” або “осяяння” – миттєве усвідомлення істотних властивостей певного предмета чи явища), так само відшукає натхнення у творчій акуратності програмування. Світи образів, мов та символів юриспруденції та ІТ побудовані на однакових принципах і демонструють схильність до взаємопроникнення, що може стати однією з перспективних практик.

*Пошук та виправлення помилок.* Правники шукають прогалини в аргументації, перевіряють відповідність тверджень або запитів вимогам законодавства так само, як програмісти (тут і далі цей термін буде використовуватися у широкому розумінні всіх ІТ-професій) опікуються налагодженням коду, виявляють та виправляють баги (помилки, недоліки). В обох випадках зазначена діяльність потребує аналітичних навичок, критичного мислення та уважності до деталей.

*Робота з прецедентами.* Правники опановують судову практику, в тому числі, ЄСПЛ, Конституційного Суду України, Верховного Суду, судів першої та апеляційної інстанцій, для того, щоб розуміти, яким чином певний нормативний акт був застосований в конкретній ситуації, та передбачити юридично значущі наслідки його впливу на майбутнє. Програмісти також вивчають паттерни проектування та колективний досвід, ефективні рішення типових задач тощо.

*Важливість і значущість документації* також є визначальною та спорідненою рисою, яка поширюється на сферу права та ІТ для опису коду, запиту, API тощо.

*Постійне оновлення знань, відкритість до інновацій.* Оскільки законодавство та технології постійно змінюються, представники обох галузей повинні регулярно оновлювати свої знання, вивчати нові інструменти та підходи, сповідувати концепцію Life-Long Learning (безперервного навчання впродовж всього життя), розвивати навички самоосвіти, гнучкості та адаптивності. Моделі поведінки, які раніше зарекомендували

себе в якості ефективних, можуть виявитися недосконалими у найближчому майбутньому. Так, свого часу окремі користувачі парових машин не усвідомили важливості появи феномену електричної енергії і зрештою програли у конкурентній боротьбі. На початку ХХ століття перші автомобілі у порівнянні з традиційним гужовим транспортом сприймалися ще більш небезпечними, ворожими та ненадійними, ніж сьогодні це має місце по відношенню до безпілотних транспортних засобів. Наступними показовими прикладами є відмова Kodak від розвитку свого власного винаходу у вигляді першої цифрової камери, поразка Nokia через нерозуміння перспективності сенсорних екранів та застарілого характеру своєї операційної системи Symbian, перемога молодого Netflix над гігантом індустрії Blockbuster завдяки акценту на інноваційній моделі стрімінгу, онлайн-сервісах та цифрових технологіях тощо.

*Алгоритмічний підхід* (if – else = “закон – виняток”). За своєю структурою норма права має визначену побудову у вигляді набору компонентів (диспозиція, санкція, гіпотеза), які системно пов’язані між собою. Способи викладення норми права в статтях певного нормативно-правового акта можуть бути різними і відрізнятися залежно від галузі, що не виключає загальну логічну конструкцію “якщо, то” (напр., якщо наявні обтяжуючі або кваліфікуючі обставини, то слід розраховувати на більш суворе покарання). У програмуванні код також будується на умовах (приклад для мови Python):

```
if age < 18:  
    print (“Доступ заборонено”)  
else:  
    print (“Вхід дозволено”),
```

що може бути інтерпретоване наступним чином: “якщо вік менше 18 років, то буде надруковано “Доступ заборонено”, в іншому випадку буде надруковано “Вхід дозволено”.

*Формулювання та додержання певних принципів.* Для сфери права одним з ключових виступає принцип правової визначеності, який означає, що закон має бути доступним та передбачуваним відносно своїх наслідків, тобто сформульованим із достатньою точністю, щоб дати змогу особі в разі необхідності регулювати його положеннями свою поведінку (рішення ЄСПЛ у справах Стіл та інші проти Сполученого Королівства (рішення Steel and Others v. the United Kingdom, 1998, Metropolitan Church of Bessarabia v. Moldova, 2001, рішення Конституційного Суду України у справах № 5-рп/2005 від 22.09.2005 р. та № 17-рп/2010 від 29.06.2010 р. тощо). Його дзеркальним відображенням у сфері програмування є принцип технічної визначеності, відповідно до якого код, системи та алгоритми мають бути так само чітко визначеними, передбачуваними та стабільними, щоб їх поведінка не залежала від випадкових факторів або неоднозначних інтерпретацій. Додержання принципу технічної визначеності досягається до допомогою сукупності вимог, зокрема, щодо формальної специфікації (своєрідна Конституція для коду, напр., IEEE 754 для операцій з числами з плаваючою комою), стандартів кодування (Google Style Guide, PEP 8 для Python тощо, які можливо вважати аналогами кодексів та законів в сфері права), тестування та верифікації (як судова практика за вертикаллю інстанційності) для перевірки, чи працює програма відповідно до певної специфікації, прозорості алгоритмів тощо. Порушення принципів в сфері права негативно відбиваються у юридично значущих наслідках, аналогічні порушення в сфері інформаційних технологій здатні призвести до катастрофи (так, через помилкову конвертацію 64-бітного числа у 16-бітне, “помилку Ariane-5” [7], перший політ ракети-носія Ariane-5 закінчився невдачею 4 червня 1996 р. після 40

секунд початку польоту, коли на висоті приблизно 3700 м ракета-носій відхилилася від траєкторії, розпалася і вибухнула).

Обидві галузі вимагають ефективної взаємодії з колегами та третіми особами, тобто *командної роботи та комунікації*, зокрема навичок пояснювати складні концепції простою мовою, узгоджувати рішення з іншими учасниками процесу тощо.

*Творчий підхід у рамках існуючих обмежень*. Правники шукають і знаходять креативні рішення в межах більш-менш окресленого правового поля, в той час як програмісти створюють інноваційні рішення в умовах технічних обмежень, тож в обох випадках виникає потреба балансувати між творчістю та дотриманням формальних правил.

Таким чином, наведений короткий і далеко не повний аналіз співвідношення певною мірою підтверджує не тільки спорідненість розглядуваних сфер діяльності, але також і можливість їх взаємопроникнення, в тому числі, через використання міждисциплінарних прийомів, методів і засобів, однакового програмного та апаратного забезпечення тощо. Людина, що отримує задоволення від скрупульозності, певного рівня перфекціонізму, уваги до дрібних деталей, логічної послідовності та точності в юриспруденції, може відшукати подібне задоволення і в програмуванні, де кожен символ і структура мають значення. Крім того, на власному прикладі автора вбачаються підстави для доведення органічності поєднання багаторічної практики в науково-педагогічній сфері в галузі кримінального права та здійснення адвокатської діяльності, з одного боку, з опануванням основ мови структурованих запитів SQL (Structured Query Language) та базових концепцій аналітики даних (Data Analytics) з використанням мови програмування Python, з іншого боку.

Хибність розподілу за критерієм інтелектуальних здібностей (схильностей) на “технарів” (фізиків, математиків, програмістів, раціоналістів, представників точних наук) та “гуманітаріїв” (ліриків, романтиків, амбасадорів соціогуманітарних напрямків) обумовлена штучним характером такої бінарної класифікації. Натомість, розум людини є набагато різноманітнішим, ніж це передбачають умовні конструкти, здібності мають багатовимірну природу, вони розвиваються та змінюються, інтелект є гнучкою та адаптивною системою, різні типи мислення не є взаємовиключними, мозок здатен до постійного навчання та перебудови. Сучасний світ демонструє дедалі більше прикладів того, що математичне мислення є також необхідним в гуманітарних науках і навпаки, вищезгадані навички важливі у всіх сферах діяльності, найбільш значущі наукові прориви відбуваються на межі різних дисциплін та у міжгалузевому просторі. Система освіти, що підтримує хибний стереотип розподілу, безпідставно розділяє навчальні траєкторії, створює психологічні бар’єри, заважає комплексному розвитку особистості, штучно зменшує потенціал здобувачів освіти, перешкоджає міждисциплінарній взаємодії тощо.

**Результати аналізу наукових публікацій.** Належну увагу питанням охорони прав, законних інтересів та охоронюваних свобод суб’єктів інформаційної діяльності приділено в роботах О.А. Баранова, В.С. Батиргарєєвої, Ю.В. Бауліна, К.І. Белякова, В.М. Брижко, В.О. Глушкова, М.В. Карчевського, О.М. Литвинова, В.О. Навроцького, М.І. Панова, В.Г. Пилипчука, Н.А. Савінової, В.Я. Тація, В.О. Тулякова, П.Л. Фрися, О.І. Харитонові та Є.О. Харитонова, а також багатьох інших. Втім, з плином часу ступінь та обсяг розробки будь-якої теми перманентно зменшується, натомість невизначеність щодо неї збільшується, в тому числі завдяки появі нових факторів та обставин, які вимагають свого врахування та нового осмислення.

**Метою статті** є виявлення та аргументування можливості та необхідності єднання правничих та ІТ-професій на прикладах використання у кримінально-правовому циклі однорідних практик сучасних інформаційних технологій.

**Виклад основного матеріалу.** Поява нового інструментарію на підґрунті використання штучного інтелекту [24, с. 123-136; 25, с. 13-29], машинного навчання та Великих Даних [27, с. 88-105] сформувала стійкий запит на формування і розвиток таких професій, як системний аналітик (System Analyst), інженер даних (Data Engineer), аналітик даних (Data Analyst), науковець з даних (Data Scientist), інженер з машинного навчання (Artificial Intelligence Engineer), інженер з машинного навчання (Machine Learning Engineer), спеціаліст з оброблення природної мови (NLP Specialist), бізнес-аналітик (Business Analyst) тощо.

В своїй діяльності системний аналітик опікується стратегічним плануванням, аналізом бізнес-моделі, проектуванням процесів і системним аналізом [4], використовуючи інструмент MATLAB для математичного моделювання, оброблення даних і виконання складних аналітичних задач, Simul8 – для моделювання процесів з метою оптимізації систем [32, с. 85-97], Microsoft Power BI та Tableau – для аналізу та візуалізації даних через інтеграцію з штучним інтелектом з метою автоматизації звітності [22] тощо. Бібліотека Scikit-learn для Python надає прості у використанні інструменти для машинного навчання, які можуть бути використані також з метою прогнозування та класифікації, фреймворки TensorFlow та PyTorch можуть бути використані для створення та навчання глибоких нейронних мереж в складних аналітичних завданнях [15]. Для виявлення трендів і патернів на великих обсягах даних (Big Data) в нагоді стають платформа IBM Watson Analytics та сервіс Microsoft Azure Machine Learning [1]. Зі свого боку, аналітик даних зосереджений на роботі з інформацією для виявлення інсайтів і підтримки прийняття рішень, для чого використовує інструмент Tableau для візуалізації даних, Power BI для прогнозування та виявлення аномалій у даних, платформи Google Cloud AutoML та Amazon SageMaker для створення моделей машинного навчання без глибоких знань програмування тощо [32, с. 85-97]. Інструменти IBM Watson та Google Natural Language API використовуються для очищення та структурування неконтрольованих текстових даних [20], платформа DataRobot автоматизує побудову моделей машинного навчання та генерує звіти, Alteryx допомагає у підготовці даних та аналітиці засобами штучного інтелекту для автоматизації рутинних завдань [17], для створення систем рекомендацій на підґрунті вивчення певної поведінки можуть бути використані Collaborative Filtering Tools [3] тощо.

Наведений далеко не повний перелік інструментів і засобів, платформ та програмного забезпечення може бути корисний також і правникам, які повною мірою здатні не тільки оволодіти базовими знаннями в сфері ІТ, але й продемонструвати в ній значні успіхи та досягнення за умови подолання психологічного бар'єру удаваної несумісності двох розглядуваних сфер професійної діяльності та уникнення поділу індивідуумів за критерієм математичного та іншого (так званого, гуманітарного) складу розуму.

Вбачається обґрунтованим припущення, що згадані професії системного аналітика та аналітика даних серед інших є найбільш наближеними до діяльності в сфері права. Тому використання вищезгаданих інструментів, а також багатьох інших, про які мова буде йти далі, може стати суттєвим фактором зростання ефективності в юриспруденції, в тому числі, в галузі кримінального, кримінально-процесуального права, кримінології та криміналістики, а так само в суддівській практиці та правоохоронній діяльності.

Так, з метою виконання завдань, сформульованих в ст. 1 КК України, ст. 2 КПК України, вбачаються підстави використовувати інструменти системної аналітики, інженерії даних та машинного навчання, аналітики даних, оброблення природної мови та бізнес-аналітики у наступних сферах та напрямках.

Розслідування кримінальних правопорушень та аналіз правової ситуації можуть стати більш ефективними за рахунок таких прийомів, як 1) побудова зв'язків між об'єктами, явищами та особами (в тому числі, схеми відмивання грошей, вчинення кіберзлочинів, незаконного обігу зброї або наркотичних препаратів, взаємодії підозрюваних, свідків, жертв, злочинних угруповань тощо), 2) таймлайни подій (графіки послідовності подій та процесів), 3) аналіз структурованих та неструктурованих даних про злочинність, робота з базами даних, в тому числі пошук закономірностей, з великими базами даних щодо підозрюваних та інцидентів (MySQL, PostgreSQL, Microsoft SQL Server, DBeaver для обробки баз даних, Python (Pandas, NumPy, SQLAlchemy) для аналізу масивів даних про злочини, поведінковий аналіз підозрюваних тощо, 4) геопросторовий аналіз суспільно небезпечної поведінки, в тому числі, виявлення “гарячих точок”, прогнозування небезпечних районів (ArcGIS, QGIS для побудови карт злочинності та виявлення аномалій, Power BI або Tableau – інтерактивні дашборди для кримінальної аналітики), 5) моніторинг та аналіз підозрілої активності (Predictive Policing), в тому числі, прогнозування ймовірності вчинення кримінальних правопорушень, поведінковий аналіз осіб під підозрою (Postman/Swagger для тестування API інтеграцій для аналізу поточкових даних (камери спостереження, дзвінки, соцмережі), Machine Learning (Scikit-learn, TensorFlow, IBM Watson) для аналізу патернів кримінальних правопорушень, прогнозування ризиків вчинення повторних правопорушень тощо.

Так, створення графічних карт (мережевих діаграм, схем зв'язків) дозволяє здійснити візуалізацію злочинних угруповань, аналіз їх структури та виявити ключових осіб. Така графічна карта може включати блоки, які стосуються керівників угруповання та ієрархії злочинного об'єднання, посередників, виконавців, фінансових зв'язків (напр., щодо відмивання грошей, джерел фінансування), регіональної або міжнародної взаємодії тощо. Інформаційним фундаментом побудови такої графічної карти можуть бути слідчі дії щодо прослуховування телефонних розмов, вивчення соцмереж та відкритих даних, фінансових операцій (банківських виписок, криптовалютних переказів), даних допитів, доказів тощо. Наприклад, Національною поліцією України було викрито організовану транснаціональну злочинну групу, яка налагодила наркотрафік до Київського слідчого ізолятора [23]. Організаторами були двоє братів, які діяли за підтримки “вора в законі”, вони залучили до своєї діяльності “смотрящих” в установі та мешканців столиці. За повідомленнями ЗМІ, під час розслідування правоохоронці використовували графічні карти для відображення зв'язків між учасниками угруповання, що сприяло успішному викриттю та затриманню злочинців.

Сучасні методи і засоби також дозволяють аналізувати величезні обсяги даних, використовуючи Machine Learning для передбачення потенційних кримінальних правопорушень, Natural Language Processing (NLP) для аналізу повідомлень та документів, Big Data Analytics для виявлення прихованих зв'язків та кореляцій тощо. Так, за допомогою Scikit-learn або TensorFlow стає можливим здійснити ефективний аналіз фінансових потоків та виявити аномальні транзакції, що дозволяє виявити прихованих співучасників тощо.

У свою чергу, платформи SAS Risk Management [18] та RapidMiner [14] можуть бути використані в якості аналітичних моделей для виявлення аномалій, оцінки та

прогнозування ризиків, їх інструменти є добре адаптованими для аналізу великих обсягів даних з метою виявлення підозрілих патернів або форм поведінки, в тому числі, для виявлення шахрайства через аналіз транзакцій та поведінкових даних для ідентифікації підозрілих дій, для прогнозування потенційної іншої неправомірної діяльності шляхом використання історичних даних для передбачення можливих злочинів та місця їх вчинення тощо.

У матеріальному кримінальному праві згадані інструменти утворюють можливості для побудови графічних карт взаємозв'язків між елементами складу кримінального правопорушення, відслідковування взаємного впливу ознак об'єктивної сторони (зокрема, діяння, місця, обстановки, способу, знарядь, особливостей розвитку причинного зв'язку тощо) та суб'єктивної сторони (вини, мотиву, мети) одна на одну.

*Судова практика та судочинство* так само можуть бути вдосконалені за рахунок використання схем судового процесу (для візуалізації стадій розгляду справи, стратегії та тактики учасників тощо), або діаграм логіки прийняття рішень (щодо варіативності застосування закону в конкретних ситуаціях). Так, наприклад, суддя може використовувати блок-схему для пояснення логіки винесення рішення. Хоча суд не повинен надавати відповіді на кожне питання, проте з рішення має бути зрозуміло, що головні проблеми, порушені в певній справі, були вивчені і була надана конкретна чітка відповідь на всі аргументи, які є вирішальними для справи (рішення ЄСПЛ у справах “Ван дер Колк проти Нідерландів” (2019 р.), “Болдеа проти Румунії” (2007 р.), “Морейра Феррейра проти Португалії” (2017 р.) тощо).

*Внутрішнє управління та адміністративна діяльність* стають більш ефективними за рахунок: 1) розподілу обов'язків в організаційних структурах поліції, прокуратурі, в суді тощо; 2) використання схем розвитку процесів (візуалізація руху кримінального провадження за допомогою Draw.io), управління документообігом (Jira або Confluence); 3) оперативної комунікації та координації, своєчасного реагування, командної роботи, стабільного оперативного зв'язку (Microsoft Teams або Slack) між структурними підрозділами та окремими фахівцями, планування розслідувань, обговорення питань стратегії і тактики (Miro або Mural); 4) автоматизації та аналітиці, зокрема, з приводу ефективності патрулювання, виявлення проблем у роботі підрозділів (Excel або Google Sheets як базова аналітика ефективності, Power BI або Tableau для візуалізації статистики злочинності та ефективності реагування поліції); 5) використання інтерактивних карт злочинності (аналітика по регіонах або інших локаціях) тощо.

*Криміналістична експертиза та докази* можуть спиратися на побудову схеми місця вчинення кримінального правопорушення (розташування доказів, траєкторії руху), реконструкцію подій (відновлення хронології на основі даних з різних джерел), аналіз цифрових доказів (відслідковування потоків фінансів, лог-файлів кіберзлочинів) тощо.

Таким чином, вбачається можливим адаптувати використання згаданих та інших інструментів для здійснення діяльності в сфері кримінального права, кримінального процесу, кримінології, криміналістики та правозастосування за наступними напрямками: 1) аналітичні платформи – для візуалізації та аналізу патернів кримінальних правопорушень за часом і місцем, створення інтерактивних карт злочинності, відстеження ефективності превентивних заходів тощо; 2) мови програмування, зокрема, Python або R – для побудови предикативних моделей злочинності, аналізу соціальних мереж та зв'язків між злочинними групами, автоматизації обробки великих масивів даних, машинного навчання з метою виявлення аномалій та підозрілої поведінки; 3) системи управління даними, зокрема, Microsoft Excel – для ведення статистики правопорушень та звітності, аналізу



патрульних маршрутів, розрахунку ресурсів та планування тощо; 4) бази даних, напр., SQL – для зберігання та обробки даних про кримінальні правопорушення, інтеграції різних джерел інформації, швидкого пошуку та аналізу історичних даних тощо; 5) інструменти візуалізації, зокрема, Draw.io, Tableau, Lucidchart – для мапування, візуалізації, створення оперативних планів, моделювання сценаріїв реагування; 6) системи співпраці, зокрема, Microsoft Teams або Slack – для координації діяльності, швидкого обміну інформацією, проведення брифінгів, спільної роботи над розслідуваннями тощо; 7) інструменти для документування, зокрема, Confluence або SharePoint – для створення баз знань та даних, документування процедур, зберігання шаблонів звітів, управління внутрішніми регламентами тощо; 8) системи управління завданнями, напр., Jira або Trello – для відстеження прогресу розслідувань, розподілу завдань між підрозділами, планування превентивних заходів, контролю строків виконання завдань тощо; 9) спеціалізовані рішення, такі як ГІС системи<sup>2</sup> – для просторового аналізу протиправної діяльності, планування патрулювання та інших заходів попередження, оптимізації маршрутів реагування, візуалізації криміногенної обстановки; 10) інструменти прототипування, зокрема, Figma або Axure – для розробки інтерфейсів аналітичних систем, створення мобільних додатків, проектування дашбордів, візуалізації звітності тощо.

При цьому ключовими аспектами впровадження зазначеного інструментарію мають бути: 1) безпека даних, в тому числі, шифрування чутливої інформації, контроль доступу, аудит дій користувачів, резервне копіювання тощо; 2) інтеграція, в тому числі, об'єднання різних джерел даних, автоматизація обміну інформацією, стандартизація форматів, забезпечення сумісності систем тощо; 3) навчання персоналу, в тому числі, регулярні тренінги, створення інструкцій, технічна підтримка, обмін досвідом тощо.

Показовими прикладами успішного комплексного застосування вказаних та інших передових технологій є наступні, але не виключно, хоча вони з часом вже встигли продемонструвати свої недоліки, що являє собою тему окремого дослідження.

*Predictive Policing (Прогнозування кримінальних правопорушень).* Для передбачення ймовірності вчинення певного кримінального правопорушення або їх сукупності використовуються такі системи штучного інтелекту, як Geolítica (попередня назва PredPol, США) – система аналізу історичних даних про злочини та розподілу патрулів поліції, завдяки якій в Лос-Анджелесі вдалося досягти зниження рівню злочинності на 20% [13], HART (Harm Assessment Risk Tool, Велика Британія) – система аналізу ризиків для прогнозування ймовірності вчинення повторного правопорушення раніше затриманими особами, яка використовує алгоритми машинного навчання для оцінки ризику на основі історичних даних про правопорушення [10].

*Розпізнавання облич, аудіо- та відео-аналітика.* Камери спостереження з використанням штучного інтелекту вже сьогодні дозволяють ідентифікувати підозрюваних осіб та розпізнавати небезпечну поведінку: Face Recognition в Китаї є складовою тотального державного контролю, зокрема, моніторингу та профілювання меншин уйгурів у Сіньцзяні [9], London Met Police (Metropolitan Police Service, MPS) являє собою одну з найбільш технологічно розвинених служб поліції у світі, яка використовує AI-систему Live Facial Recognition (CCTV, Face Recognition) для

---

<sup>2</sup> Геоінформаційна система (ГІС) – сучасна комп'ютерна технологія, яка дозволяє поєднати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо).

виявлення шляхом розпізнавання обличчя правопорушників, розшуку зниклих людей, включаючи дітей та жертв торгівлі людьми, захисту потерпілих від насильства, підтримки жертв домашнього насильства тощо [8], система ShotSpotter (США) використовує мережу акустичних сенсорів для ідентифікації та локалізації звуків пострілів у режимі реального часу, що допомагає правоохоронним органам швидко реагувати на інциденти із застосуванням вогнепальної зброї та підвищувати ефективність розслідувань [19] тощо.

*Аналіз соціальних мереж та відкритих даних.* За допомогою програм з використанням штучного інтелекту здійснюється відстеження підозрілої активності у соціальних мережах, форумах та мережі Darknet<sup>3</sup>. Так, відповідна система штучного інтелекту у Франції аналізує повідомлення у соцмережах для виявлення терористичних загроз [12].

*Аналіз великих даних та автоматизація процесів розслідування.* Машинне навчання використовується для аналізу великих обсягів даних (Великі Дані [27, с. 88-105]) для вдосконалення розслідувань: система кримінальної аналітики CompStat (США) задіює штучний інтелект для оцінки ефективності роботи поліції та розробки стратегій боротьби зі злочинністю [2]; аналітична платформа Palantir (США, Європа) [11] працює за принципом інтеграції та аналізу розрізнених даних, створює єдину картину для слідчих та аналітиків на підставі сукупності таких джерел, як відеоспостереження та камери (аналіз відео з міських камер спостереження та камер спеціального призначення, автоматичне розпізнавання обличчя та транспортних засобів, перехресне зіставлення відео з іншими джерелами, напр., списками розшуку), банківські операції та фінансові транзакції (виявлення підозрілих транзакцій та фінансових схем, аналіз руху коштів між особами, компаніями та кримінальними угрупованнями, автоматична перевірка банківських операцій з іншими базами даних), телефонні дзвінки, мобільні дані та соцмережі (аналіз метаданих дзвінків та повідомлень, зокрема, їх час, місце, частота спілкування), виявлення зв'язків між особами через телефонні контакти, моніторинг соціальних мереж для пошуку загроз (напр., терористичних змов), дані про переміщення та геолокацію (відстеження пересування підозрюваних за допомогою мобільних веж, GPS та камер, побудова маршрутів переміщень і можливих зон діяльності злочинних груп, використання даних авіакомпаній, залізниць та автомобільного транспорту) тощо.

*Біометрична ідентифікація та детектори брехні.* Штучний інтелект аналізує голос, мікроекспресії обличчя, зміни в поведінці для виявлення неправдивих повідомлень та небезпечних намірів: Silent Talker (Велика Британія) являє собою AI-детектор брехні для аналізу мікроекспресій підозрюваних [16], iBorderCtrl (ЄС) є системою для сканування міміки осіб на кордонах та визначення ризику незаконного перетину [6] тощо.

*Криміналістична аналітика та цифрова експертиза.* Аналіз повідомлень, зображень, фінансових транзакцій здійснюється за допомогою штучного інтелекту, зокрема, платформою DataWalk (ЄС, США) [5], яка дозволяє об'єднувати дані з різних джерел (банківські виписки, мобільні дані та інформація з соціальних мереж) для

---

<sup>3</sup> Даркнет (від dark net – “темна мережа”) – анонімна оверлейна мережа, що являє собою систему не пов'язаних між собою віртуальних тунелів і дозволяє передавати дані в зашифрованому вигляді. Доступ можливий лише через певне програмне забезпечення, налаштування чи авторизацію, часто з використанням нестандартних комунікаційних протоколів та портів. Типовими є friend-to-friend мережі, які зазвичай використовуються для спільного користування файлами та peer-to-peer з'єднання, а також приватні мережі на кшталт Tor (більш докладніше див.: <https://www.dw.com/uk/даркнет/t-45087705>).

ефективної боротьби з фінансовими злочинами, спираючись на інтеграцію даних (об'єднання розрізаних джерел інформації в єдину систему для створення повної картини подій та взаємозв'язків), аналіз та візуалізацію (використання графічних технологій для виявлення прихованих патернів, зв'язків та аномалій у великих обсягах даних), виявлення шахрайства (автоматичне ідентифікування потенційних злочинних груп та підозрілої поведінки), відповідність нормативним вимогам (забезпечення дотримання стандартів та регуляторних практик у сфері фінансового моніторингу та боротьби з відмиванням грошей) тощо. Інструмент MATLAB використовується для створення складних математичних моделей аналізу доказів та реконструкції подій (напр., моделювання траєкторії руху куль, аналізу аудіозаписів на предмет автентичності або реконструювання автомобільної аварії), моделювання поведінки злочинців, аналізу злочинних схем, обробки відео з камер спостереження (розпізнавання номерних знаків) тощо; Simul8 – для оптимізації робочих процесів шляхом симуляції різних сценаріїв (моделювання реагування на надзвичайні ситуації, оптимізація ресурсів, розподіл патрульних, планування заходів з евакуації під час масових заходів, аналізування навантаження на суддів тощо); Microsoft Power BI та(або) Tableau трансформують великі масиви даних у зрозумілі візуалізації, дозволяють створювати інтерактивні карти злочинності, відстежувати тренди правопорушень та генерувати звіти для зацікавлених осіб та громадськості, які можуть бути особливо ефективними для виявлення “гарячих точок” злочинності та планування превентивних заходів; бібліотека Scikit-learn (Python) є потужним інструментом для створення предиктивних моделей, що дозволяє розробляти алгоритми для прогнозування ймовірності повторних правопорушень, оцінки ризиків втечі підозрюваних осіб або аналізу патернів злочинної діяльності; фреймворки TensorFlow та PyTorch використовуються для складних задач машинного навчання, обробки відео з камер спостереження для розпізнавання облич, аналізу відбитків пальців або ідентифікації підроблених документів, а також для аналізу великих обсягів текстової інформації у справах; платформи IBM Watson Analytics та Microsoft Azure Machine Learning пропонують готові рішення для аналітики, допомагають автоматизувати аналіз доказів, обробляти неструктуровані дані та створювати системи раннього попередження про потенційні загрози; платформа SAS Risk Management допомагає оцінювати різноманітні ризики у правоохоронній діяльності, в тому числі, під час проведення операцій, оцінювати ймовірність рецидиву або допомагати у прийнятті рішень щодо запобіжних заходів; RapidMiner спрощує створення аналітичних workflow (потоків робіт) без глибоких знань програмування, що є корисним для користувачів з мінімальним обсягом знань та навичок (створення моделей для виявлення шахрайських схем або аналізу соціальних мереж злочинних угруповань); бібліотеки spaCy та NLTK (Natural Language Toolkit) є незамінними для обробки природної мови, допомагають аналізувати свідчення, виявляти ключові факти у документах, порівнювати різні версії показань або шукати невідповідності у матеріалах справ; платформи UiPath та Blue Prism автоматизують рутинні процеси, зокрема, заповнення стандартних бланків і документів, перевірку даних у різних базах або генерацію поточних звітів, що звільняє час для більш важливих завдань тощо.

Таким чином, додатковими до наведених вище аргументами щодо корисності опанування правниками сучасних технологічних інструментів та(або) розуміння принципів їх роботи можуть бути наступні.

По-перше, відбувається стрімка цифрова трансформація самої правової сфери. Мова йде не тільки про автоматизацію рутинних процесів, але й втручання в тканину матеріального права (так, під тиском кореляцій на підставі Великих Даних може зазнати

впливу феномен необхідного причинного зв'язку як обов'язкової ознаки об'єктивної сторони кримінальних правопорушень з матеріальним складом [28, с. 94-113]). Крім того, дедалі більше доказів, документів та інших об'єктів починають існувати одночасно або переважно у цифровому форматі, від електронного листування до даних з соціальних мереж та геолокації. Правник, який розуміє як взаємодіяти з такими даними з використанням сучасних технологій, може більш ефективно збирати та аналізувати інформацію, виявляти важливі зв'язки, кореляції та закономірності. Наприклад, навички програмування дозволяють автоматизувати пошук ключової інформації у великих масивах документів або створювати візуалізації для кращого представлення складних справ у суді.

По-друге, штучний інтелект та машинне навчання дедалі активніше використовуються у правовій практиці і допомагають передбачати ймовірність настання певних подій, зокрема, змісту судового рішення або рецидиву з боку злочинця, оцінювати ризики при обранні запобіжних заходів, виявляти потенційні правопорушення тощо. Правник, який розуміє принципи роботи таких систем, може краще оцінювати надійність або хибність їх висновків та виявляти можливі упередження в алгоритмах, що є критично важливим для забезпечення справедливого правосуддя.

По-третє, поступово з'являються нові види кримінальних правопорушень, які безпосередньо пов'язані з розвитком технологій та нових віртуальних просторів [29, с. 40-68], зокрема, нові різновиди кіберзлочинів, шахрайство з криптовалютами або NFT, суспільно небезпечне використання штучного інтелекту тощо. Для ефективного розслідування таких справ необхідне глибоке розуміння їх технічних аспектів.

По-четверте, технологічні навички стають конкурентною перевагою на ринку праці, тому юридичні фірми, суди та правоохоронні органи дедалі частіше шукають фахівців, які поєднують правові знання з розумінням сучасних технологій. Такі спеціалісти можуть працювати на перетині права та технологій, розробляти нові інструменти для правової практики, консультувати з питань регулювання та правозастосування.

По-п'яте, розуміння технологій необхідне для забезпечення прав людини у цифрову епоху [26, с. 19-41]. Правники повинні розуміти з самого початку, як технології можуть впливати на безпеку, приватність, свободу слова, свободу від самовикриття, право на забуття у справедливому балансі з інтересами суспільства, правову визначеність як складову верховенства права, право на справедливий суд та інші гарантії демократичного устрою.

Скоріш за все, до трьох основних навичок сучасної культурної людини, серед яких одними з принципів донедавна визначали вміння читати (так, щоб зрозуміти особисто і вміти пояснити іншим), писати (так, щоб лаконічно та переконливо викладати свої думки), а також рахувати, невдовзі обов'язково будуть додані обізнаність в сучасних технологіях та оволодіння однією з базових ІТ компетентностей. І хоча наразі не йдеться про те, щоб юристи стали програмістами, але у найближчому майбутньому не буде достатнім мати лише поверхове уявлення про поточні технології.

Такий підхід повною мірою збігається з Європейськими еталонними рамками (European Reference Framework) [31], які визначають наступні основні компетентності: 1) спілкування рідною мовою (Communicating in a mother tongue); 2) спілкування іноземними мовами (Communicating in a foreign language); 3) знання математики та загальні знання у сфері науки і техніки (Mathematical, scientific and technological competence); 4) навички роботи з цифровими носіями (Digital competence); 5) навчання заради здобуття знань (Learning to learn); 6) соціальні та громадянські навички (Social

and civic competences); 7) ініціативність та практичність (Sense of initiative and entrepreneurship); 8) обізнаність та самовираження у сфері культури (Cultural awareness and expression).

Процеси навчання юриспруденції та програмуванню мають багато спільного, тому навчальні програми повинні формуватися у тісному міждисциплінарному зв'язку між ними.

### **Висновки та пропозиції.**

Професії в сфері права та інформаційних технологій мають численні спільні риси, зокрема, структурована логіка мислення, робота з формальними мовами, образами та символами, пошук та виправлення помилок, робота з прецедентами, постійне оновлення знань, відкритість до інновацій, алгоритмічний підхід, формулювання та додержання певних принципів, важливість командної роботи та комунікації, творчий підхід у рамках існуючих обмежень тощо. Така спорідненість вказує на можливість їх взаємопроникнення, в тому числі, через використання міждисциплінарних прийомів, методів і засобів, однакового програмного та апаратного забезпечення тощо. Людина, що отримує задоволення від скрупульозності, певного рівня перфекціонізму, уваги до дрібних деталей, логічної послідовності та точності в юриспруденції, може відшукати подібне задоволення і в програмуванні, де кожен символ і структура мають значення.

Хибність розподілу за критерієм інтелектуальних здібностей (схильностей) на “технарів” (фізиків, математиків, програмістів, раціоналістів, представників точних наук) та “гуманітаріїв” (ліриків, романтиків, амбасадорів соціогуманітарних напрямків) обумовлена штучним характером такої бінарної класифікації. Натомість, розум людини є набагато різноманітнішим, ніж це передбачають умовні конструкти, здібності мають багатовимірну природу, вони розвиваються та змінюються, інтелект є гнучкою та адаптивною системою, різні типи мислення не є взаємовиключними, мозок здатен до постійного навчання та перебудови. Сучасний світ демонструє дедалі більше прикладів того, що математичне мислення є також необхідним в гуманітарних науках і навпаки, вищезгадані навички важливі у всіх сферах діяльності, найбільш значущі наукові прориви відбуваються на межі різних дисциплін та у міжгалузевому просторі. Система освіти, що підтримує хибний стереотип розподілу, безпідставно розділяє навчальні траєкторії, створює психологічні бар'єри, заважає комплексному розвитку особистості, штучно зменшує потенціал здобувачів освіти, перешкоджає міждисциплінарній взаємодії тощо.

З метою виконання сформульованих в ст. 1 КК України та ст. 2 КПК України завдань вбачаються підстави використовувати наступні інструменти системної аналітики, інженерії даних та машинного навчання, аналітики даних, оброблення природної мови та бізнес-аналітики у наступних сферах та напрямках: розслідування кримінальних правопорушень та аналіз правової ситуації – MySQL, PostgreSQL, Microsoft SQL Server, DBeaver для обробки баз даних, Python (Pandas, NumPy), SQLAlchemy, ArcGIS, QGIS для побудови карт злочинності та виявлення аномалій, Power BI або Tableau як інтерактивні дашборди для кримінальної аналітики, Postman або Swagger для тестування API інтеграцій для аналізу потокових даних, Machine Learning (Scikit-learn, TensorFlow, IBM Watson) для аналізу патернів кримінальних правопорушень, прогнозування ризиків вчинення повторних правопорушень, платформи SAS Risk Management та RapidMiner – в якості аналітичних моделей для виявлення аномалій, оцінки та прогнозування ризиків тощо; внутрішнє управління та адміністративна діяльність – розподіл обов'язків в організаційній структурі поліції, прокуратури, в суді, використання схем розвитку процесів, візуалізація руху

кримінального провадження за допомогою Draw.io, управління документообігом (Jira або Confluence), оперативна комунікація та координація, своєчасне реагування, командна робота, стабільний оперативний зв'язок (Microsoft Teams або Slack) між структурними підрозділами та окремими фахівцями, планування розслідувань, обговорення питань стратегії і тактики (Miro або Mural), автоматизація та аналітика (Excel або Google Sheets як базова аналітика ефективності, Power BI або Tableau для візуалізації статистики злочинності та ефективності реагування поліції); Confluence або SharePoint – для створення баз знань та даних, документування процедур, зберігання шаблонів звітів, управління внутрішніми регламентами тощо; Jira або Trello – для відстеження прогресу розслідувань, розподілу завдань між підрозділами, планування превентивних заходів, контролю строків виконання завдань тощо; інструменти прототипування Figma або Axure – для розробки інтерфейсів аналітичних систем, створення мобільних додатків, проектування дашбордів, візуалізації звітності тощо.

При цьому ключовими аспектами впровадження зазначеного інструментарію мають бути: 1) безпека даних, в тому числі шифрування чутливої інформації, контроль доступу, аудит дій користувачів, резервне копіювання тощо; 2) інтеграція, в тому числі об'єднання різних джерел даних, автоматизація обміну інформацією, стандартизація форматів, забезпечення сумісності систем тощо; 3) навчання персоналу, в тому числі регулярні тренінги, створення інструкцій, технічна підтримка, обмін досвідом тощо.

Практичними сферами застосування інформаційних технологій в сфері права є: Predictive Policing (прогнозування кримінальних правопорушень) – Geolitics (система аналізу історичних даних про злочини та розподілу патрулів поліції); HART (Harm Assessment Risk Tool – система аналізу ризиків для прогнозування ймовірності вчинення повторного правопорушення раніше затриманими особами); розпізнавання облич, аудіо- та відео-аналітика – Face Recognition, Live Facial Recognition (CCTV, Face Recognition), ShotSpotter тощо; аналіз великих даних та автоматизація процесів розслідування – CompStat, Palantir; біометрична ідентифікація та детектори брехні – Silent Talker, iBorderCtrl; криміналістична аналітика та цифрова експертиза – DataWalk тощо.

Ефективно можуть бути використані такі інструменти, фреймворки, платформи та бібліотеки, як MATLAB, Simul8, Microsoft Power BI, Tableau, Scikit-learn (Python), spaCy та NLTK (Natural Language Toolkit), TensorFlow, PyTorch, IBM Watson Analytics, Microsoft Azure Machine Learning, SAS Risk Management, RapidMiner, UiPath, Blue Prism тощо.

Додатковими аргументами щодо корисності опанування правниками сучасних технологічних інструментів та(або) розуміння принципів їх роботи можуть бути: 1) стрімка цифрова трансформація самої правової сфери; 2) штучний інтелект та машинне навчання все більш активно використовуються у правовій практиці і допомагають передбачати ймовірність настання певних подій; 3) з'являються нові види кримінальних правопорушень, які безпосередньо пов'язані з розвитком технологій та нових віртуальних просторів; 4) технологічні навички стають конкурентною перевагою на ринку праці; 5) розуміння технологій необхідне для забезпечення прав людини у цифрову епоху.

До трьох основних навичок сучасної культурної людини вміння читати (так, щоб зрозуміти особисто і вміти пояснити іншим), писати (так, щоб лаконічно та переконливо викладати свої думки), а також рахувати, невдовзі будуть додані обізнаність в сучасних технологіях та оволодіння однією з базових ІТ компетентностей.

Процеси навчання юриспруденції та програмуванню мають багато спільного, тому навчальні програми повинні формуватися у тісному міждисциплінарному зв'язку між ними.

**Перспективи подальших наукових досліджень.** Порушені питання та надана їм авторська оцінка, щодо перспектив єднання правничих та ІТ-професій, є дискусійними та відкритими для конструктивної критики і широкого обговорення з огляду на їх актуальність та важливість для забезпечення подальшого розвитку інформаційного суспільства.

### Використана література

1. Andersen G. (2024) Systems Analysis in Artificial Intelligence: Leveraging AI Technologies for Success / MoldStud, Feb 14, 2024. URL: <https://moldstud.com/articles/p-systems-analysis-in-artificial-intelligence-leveraging-ai-technologies-for-success> (дата звернення: 24.03.2025).
2. CompStat / New York City Police Department. URL: <https://www.nyc.gov/site/nypd/stats/crime-statistics/compstat.page> (дата звернення: 24.03.2025).
3. Crabtree M., Nehme A. (2024) What is Data Analysis? An Expert Guide With Examples / DataCamp, Nov 10, 2024. URL: <https://www.datacamp.com/blog/what-is-data-analysis-expert-guide> (дата звернення: 24.03.2025).
4. Dahmann Ju., DeLaurenits D. (2023) Unique Challenges in System of Systems Analysis, Architecting, and Engineering / Systems Engineering for the Digital Age. 2023. P. 581-600. URL: <https://doi.org/10.1002/9781394203314.ch28> (дата звернення: 24.03.2025).
5. DataWalk. URL: <https://datawalk.com/> (дата звернення: 24.03.2025).
6. iBorderCtrl. URL: <https://www.iborderctrl.eu> (дата звернення: 24.03.2025).
7. Lions, J. L. (1996) Ariane 5 Flight 501 Failure Report / European Space Agency, 23 July 1996. URL: [https://www.esa.int/Newsroom/Press\\_Releases/Ariane\\_501\\_-\\_Presentation\\_of\\_Inquiry\\_Board\\_report?utm\\_source=chatgpt.com](https://www.esa.int/Newsroom/Press_Releases/Ariane_501_-_Presentation_of_Inquiry_Board_report?utm_source=chatgpt.com) (дата звернення: 24.03.2025).
8. Metropolitan Police Service. (n.d.). URL: <https://www.met.police.uk> (дата звернення: 24.03.2025).
9. Mozur, P. (2019) One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. The New York Times, 2019, April 14. URL: <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> (дата звернення: 24.03.2025).
10. Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and “Experimental” proportionality / *Information & Communications Technology Law*, 27(2), 223-250. URL: [https://www.researchgate.net/publication/324202083\\_Algorithmic\\_risk\\_assessment\\_policing\\_models\\_lessons\\_from\\_the\\_Durham\\_HART\\_model\\_and\\_'Experimental'\\_proportionality](https://www.researchgate.net/publication/324202083_Algorithmic_risk_assessment_policing_models_lessons_from_the_Durham_HART_model_and_'Experimental'_proportionality) (дата звернення: 24.03.2025).
11. Palantir Technologies. (n.d.). URL: <https://www.palantir.com> (дата звернення: 24.03.2025).
12. Pieper, Diana. (2024). Stärkstes Schwert im Kampf gegen Terror – So radikal geht Frankreich gegen Islamisten vor / WELT, 02.09.2024. URL: [https://www.welt.de/politik/ausland/plus253254288/Islamismus-So-radikal-geht-Frankreich-gegen-Islamisten-vor.html?utm\\_source=chatgpt.com](https://www.welt.de/politik/ausland/plus253254288/Islamismus-So-radikal-geht-Frankreich-gegen-Islamisten-vor.html?utm_source=chatgpt.com) (дата звернення: 24.03.2025).
13. PredPol. URL: <https://teamupturn.gitbooks.io/predictive-policing/content/systems/predpol.html> (дата звернення: 24.03.2025).
14. RapidMiner. (n.d.). URL: <https://docs.rapidminer.com/9.9/studio/installation> (дата звернення: 24.03.2025).
15. Role of Artificial Intelligence (AI) in System Design. URL: <https://www.geeksforgeeks.org/role-of-artificial-intelligenceai-in-system-design> (дата звернення: 24.03.2025).
16. Rothwell, J., Bandar, Z., O’Shea, J. and McLean, D. (2006). Silent talker: a new computer-based system for the analysis of facial cues to deception. *Appl. Cognit. Psychol.*, 20: 757-777. URL: <https://doi.org/10.1002/acp.1204> (дата звернення: 24.03.2025).

17. Saharawat V. (2023) 15 Different Types of Data Scientists In 2024 / PWSkills, Oct 29, 2023. URL: <https://pwskills.com/blog/15-different-types-of-data-scientists-in-2024> (дата звернення: 24.03.2025).
18. SAS Risk Management Solutions. (n.d.). SAS. URL: [https://www.sas.com/en\\_us/solutions/risk-management.html](https://www.sas.com/en_us/solutions/risk-management.html) (дата звернення: 24.03.2025).
19. SoundThinking Inc. (n.d.). Gunshot Detection – SoundThinking. URL: <https://www.soundthinking.com/law-enforcement/leading-gunshot-detection-system> (дата звернення: 24.03.2025).
20. Srijani S. (2024) Top 13 Data Analyst Career Paths You Should Know About / Advisor Uncle, Nov 2, 2024. URL: <https://advisoruncle.com/data-analyst-career> (дата звернення: 24.03.2025).
21. Stanley Jay. (2021) Four Problems with the ShotSpotter Gunshot Detection System - A new investigation points to yet another problematic outcome of the technology's use and the company's lack of transparency / ACLU, August 24, 2021. URL: <https://www.aclu.org/news/privacy-technology/four-problems-with-the-shotspotter-gunshot-detection-system> (дата звернення: 24.03.2025).
22. Wang Ch., Lee B., Drucker S., Marshall D., Gao J. (2024) Data Formulator 2: Iteratively Creating Rich Visualizations with AI / Cornell University, arXiv., Aug 28, 2024. Vol. 2408.16119. URL: <https://doi.org/10.48550/arXiv.2408.16119> (дата звернення: 24.03.2025).
23. Міллер І. Викрито злочинне угруповання, яке налагодило наркотрафік до Київського СІЗО. *Главком*, 28 січня 2025 р. URL: <https://glavcom.ua/kyiv/news/vikrito-zlochinne-uhrupovan-nja-jake-nalahodilo-narkotrafik-do-kijivskooho-sizo-foto-1042471.html> (дата звернення: 24.03.2025).
24. Радутний О. Суб'єктність штучного інтелекту у кримінальному праві. *Право України*, 1/2018. С. 123-136.
25. Радутний О.Е. Право та окремі аспекти світу атомів і бітів (робототехніка, штучний інтелект, цифрова людина: зб. наук. пр. *Питання боротьби зі злочинністю* / редкол.: Б.М. Головкін та ін. Харків: Право, 2021. Вип. 41. 216 с. С. 13-29.
26. Радутний О.Е., Якулявічене Л. Права людини крізь призму штучного інтелекту, роботизації та цифрової людини / Права людини в умовах цифрової трансформації суспільства: монографія / Д.В. Лученко, О.В. Капліна, В.Я. Настюк та ін.: за ред. проф. Д.В. Лученка. Харків: НЮУ імені Ярослава Мудрого, 2022. 272 с. С. 19-41.
27. Радутний О.Е. Великі дані: поняття, ознаки та виклики (кримінально-правовий аспект). *Інформація і право*. № 1(44)/2023. 208 с. С. 88-105.
28. Радутний О.Е. Великі дані: кореляції та причинність (кримінально-правовий аспект). *Інформація і право*. № 2 (45)/2023. 226 с. С. 94-113.
29. Радутний О.Е. Метавсесвіт та загальна економіка добра і зла (кримінально-правовий вимір): зб. наук. пр. *Питання боротьби зі злочинністю* / редкол.: В.С. Батиргареева (голов. ред.) та ін. Харків: Право, 2022. Вип. 44. 152 с. С. 40-68.
30. Радутний О.Е. Віртуальні кримінальні посягання на статеву свободу або недоторканність у просторі Метавсесвіту. *Інформація і право*. № 3(50)/2024. 247 с. С. 82-99.
31. Про основні компетенції для навчання протягом усього життя: Рекомендація 2006/962/ЄС Європейського Парламенту та Ради (ЄС) від 18 грудня 2006 р. URL: [https://web.archive.org/web/20170331205544/http://zakon3.rada.gov.ua/laws/show/994\\_975](https://web.archive.org/web/20170331205544/http://zakon3.rada.gov.ua/laws/show/994_975) (дата звернення: 24.03.2025).
32. Трофименко О. Г., Лобода Ю. Г., Дика А. І., Мільченко О. О., Стрілець М. І. Штучний інтелект у системному аналізі. *Таврійський науковий вісник. Серія: Технічні науки*. 2024. № 5. с. 85 - 97. URL: <https://doi.org/10.32782/tnv-tech.2024.5.9> (дата звернення: 24.03.2025).

~~~~~ \* \* \* ~~~~~