УДК 343.9:316.6:004.8
DOI https://doi.org/10.32782/apdp.v107.2025.3

Т. С. Батраченко, І. Г. Батраченко, І. В. Єфімова

ЕВОЛЮЦІЯ «СПЕКТРУ» ЗЛОЧИННОСТІ В ЕПОХИ ПРИРОДНОГО ТА ШТУЧНОГО ІНТЕЛЕКТУ

Вступ. В умовах втрати монополії природного інтелекту як чинника регуляції правочинної і злочинної діяльності викає критична необхідність у науковій рефлексії основних трендів еволюції (а можливо й революції) злочинності в сучасну епоху. Споконвіку у правовій сфері йшло епічне змагання природних інтелектуальних потенціалів тих хто порушував закон і тих хто його захищав. Однак на сьогодні таке змагання почало опосередковуватися все більш складними технічними засобами, інформаційно-комунікативними технологіями, серед яких нині виокремлюють феномен штучного інтелекту. Останній, фактично, перестав бути метафорою, бо вочевидь знаменитий тест Тьюрінга ці технології вже успішно пройшли. Відтак це повинно стати предметом численних досліджень в юридичній психології.

Постановка проблеми. Швидка інституціоналізація систем штучного інтелекту (ШІ) у сферах комунікації, економіки, безпеки та правосуддя призводить до якісної трансформації криміногенних процесів. «Спектр» злочинності, який традиційно описувався біполярністю «людина-правопорушник ↔ людина-правоохоронець», доповнюється трьома принципово новими вимірами: (1) алгоритмізована злочинність (автоматизоване вчинення правопорушень з використанням ШІ-моделей), (2) гібридна суб'єктність (співучасть людини та автономних/напівавтономних систем), (3) машинно-опосередкована віктимізація (масштабовані, персоналізовані впливи на жертв через генеративні технології та поведінкові платформи). Унаслідок цього класичні психологічні моделі детермінації злочину (мотиваційні, когнітивні, афективні й ситуативні) перестають бути достатніми без урахування алгоритмічних посередників, як і без аналізу «людина-в-контурі» (human-in-the-loop) та «людина-над-контуром» (human-over-the-loop) у прийнятті рішень. Постає проблема: як описати, виміряти та прогнозувати еволюцію «спектру» злочинності в умовах співіснування природного та штучного інтелектів, зберігаючи валідність психологічних пояснень і забезпечуючи операціоналізацію для правозастосування.

Аналіз останніх досліджень і публікацій. Останнє десятиріччя позначене міждисциплінарним зближенням кримінології, юридичної психології, кібербезпеки та етики ШІ. Накопичені результати можна згорнути у чотири кластери. Перший можна окреслити як кіберзлочинність і психологія правопорушника (О. В. Барановський [2], І. В. Владленова, Е. А. Кальницький [8], М. В. Гуцалюк [11; 12], О. Самойленко, Д. Цехан [21]). У цих дослідженнях описано мотиваційні профілі (інструментальна вигода, ігрова/змагальна мотивація, ідеологічна раціоналізація), когнітивні стилі (холодна раціональність, «технічна всемогутність»), соціально-інженерні патерни впливу (фішинг, маніпуляції довірою, експлуатація когнітивних упереджень). Показано роль онлайн-спільнот у нормалізації девіації.

Другий кластер торкається автоматизації правопорушень і використання генеративних технологій в злочинній діяльності (М.М. Великанова [7], В.А. Миколаєць [17], О.Е. Радутний [20]). Доведено, що генеративні моделі підсилюють масштабованість атак (масова персоналізація, швидке прототипування шкідливих артефактів, удосконалення deepfake-контенту). Висвітлено феномени «crime-as-a-service», «model-steering» та ескалацію «чорно-сірих» практик (prompt-інжиніринг для обходу бар'єрів).

Третій, особливо, масштабний кластер пов'язаний з застосуванням ШІ у правоохоронній діяльності та судочинстві (М. В. Бєлова, Д. М. Бєлов, І. В. Рущак [3], Бєлова М. В., Бєлов Д. М. [4], О.І. Бугера [5], І. Варава [6], О. Гетманцев, А. Алєксєєва [9], В.І. Гришко, С.С. Вознюк [10], О.О. Кармаза [13], Ю.В. Кривицький [16], Ю. Муравська, І. Метельський, Р. Романів. [18], І.С. Похиленко [19], В.М. Стратонов, В.М. Дзюрбель [22], В.Ю. Цьомра, С.Т. Корильчук, Д.О. Оленюк [23]). Описані переваги (високошвидкісна аналітика, інтеграція мультиджерельних слідів, аномалієвий моніторинг) і ризики (упередженість даних, помилки класифікації, непрозорість рішень). Підкреслено потребу у верифікації, аудиті алгоритмів і збереженні ролі людини як остаточного суб'єкта оцінювання доказів. Четвертий кластер пов'язаний з нормативно-етичні рамки і психологічні наслідки (Асірян С. Р. [1], Т.Г. Каткова [14], Aliane N. [24], Cybercrime and Artificial Intelligence [25], Mohamed E., Ahmed S., Zhang Y. [26], Schmitt C., Flechais I. [27]). Регуляторні підходи (GDPR, AI-регламенти ЄС, етичні кодекси) намагаються синхронізувати інновації з правами людини. Психологічні дослідження фіксують зростання дигітальної тривожності, ерозію довіри до інформаційного середовища та адаптивні розриви між темпами освоєння ШІ злочинцями та правоохоронцями.

Попри прогрес, існують лакуни: (а) відсутність уніфікованої таксономії «спектру» злочинності в координатах «ступінь автономності системи – ступінь людської участі – рівень психологічної маніпуляції»; (б) недостатня психометрична операціоналізація нових феноменів (наприклад, алгоритмічна віктимність, «довіра-до-ШІ» як модератор правової поведінки); (в) брак проспективних моделей ко-еволюції злочину і правопорядку за наявності генеративних технологій.

Мета даної роботи полягає к тому щоб розробити психологічно та юридично релевантну рамку опису й вимірювання еволюції «спектру» злочинності в епоху ко-екзистенції природного та штучного інтелектів, придатну для наукового аналізу й практики протидії. Передбачається сконструювати концептуальну модель «спектру» з тривимірним простором: автономність ШІ-компоненти; інтенсивність людської участі (ініціація, нагляд, делегування); рівень психологічного впливу на жертву/свідка/правоохоронця. Побудувати гіпотетичні сценарії ко-еволюції (інерційний, акселераційний, регуляторно-консервативний) і визначити їхні психологічні маркери (динаміка довіри, толерантність до ризику, адаптаційні стратегії). Сформулювати рекомендації для правозастосування і підготовки кадрів (правників, психологів, фахівців з безпеки) з урахуванням когнітивно-афективних наслідків взаємодії з системами ШІ.

Виклад основного матеріалу. Ще кілька десятиліть тому кримінальний ландшафт складався переважно з форм, які сьогодні доцільно узагальнити як класична

(офлайн-) злочинність. Йдеться про діяння, що вчиняються переважно у фізичному просторі: крадіжки, грабежі й розбої, шахрайства «віч-на-віч», насильницькі злочини, корупційні практики, контрабанда, «класичні» економічні злочини тощо. Частина історично поширених явищ, як-от конокрадство, фактично зникла або перетворилася на рідкісний анахронізм разом зі зникненням об'єкта посягання й зміною господарського укладу. Інші, навпаки, виникли як технологічні аналоги старих форм – приміром, крадіжка автомобілів (по суті, модернізована крадіжка засобів пересування з новими способами проникнення, відмикання, перепрошивки електроніки тощо). Проте попри трансформації об'єктів і засобів, сутнісна логіка класичної злочинності збереглася: безпосередня взаємодія сторін у фізичному світі, матеріальні сліди, локальна юрисдикція, «людський фактор» як домінанта в ухваленні рішень злочинцем і правоохоронцем. Інакше кажучи, історичний пласт «класики» не зникає, а співіснує з новими шарами злочинності, що з'явилися з розвитком техносфери.

Однак порівняно недавно відбулося виникнення кіберзлочинності без використання ШІ у якій поєднується нове середовище та стара суб'єктність. Поширення інформаційно-комунікаційних технологій створило цифровий простір як місце, інструмент і ціль посягання. Звідси – фішинг, злам акаунтів, шкідливе ПЗ, крадіжка даних, шахрайства з платіжними інструментами, онлайн-спуфінг, незаконні маркетплейси тощо. На цьому етапі злочинець переважно спирається на власний, «природний» інтелект, а технології виконують роль інструментів доступу, маскування й масштабування. При цьому й зявляються відмінності від «класики», які стають принциповими: транскордонність, анонімізація, інша логіка слідів (логи, трафік, метадані), інша динаміка часу (миттєве розповсюдження атаки), інший характер доказування.

Але на разі вже зявилася й кіберзлочинність із використанням ШІ, яка ма якісне прискорення й, навіть, часткову автоматизацію. Останніми роками відбувся перехід від «цифрових інструментів без ШІ» до інструментів і схем, у яких ШІ відіграє активну роль. Це не просто новий набір засобів – це якісна зміна темпу, масштабу й адаптивності злочинних операцій. Умовно можна виділити три режими:

1. Підсилення (enablement): ШІ спрощує й пришвидшує вже відомі техніки – генерація правдоподібних листів/діалогів, переклад і локалізація фішингових кампаній, підбір соціотехнічних тригерів для конкретних профілів жертв.

2. Автоматизація (automation): чат- та мультиагенти виконують послідовні кроки атаки (збір OSINT, написання коду, тестування вразливостей, ведення багатоканальної комунікації з жертвою), зменшуючи потребу у безперервній участі людини.

3. Адаптивність/квазі-автономність (adaptivity/agentic): системи динамічно змінюють стратегію під впливом відповіді захисника, обходять фільтри, створюють синтетичний контент (deepfake-відео/аудіо/зображення), масштабують імперсонізацію з високою точністю наслідування.

У підсумку правоохоронець дедалі частіше протистоїть не лише людині-злочинцю, а й алгоритмічному «множнику», що робить атаки масовішими, дешевшими та психологічно правдоподібнішими для жертви. Тому трирівнева рамка

аналізу стає методично доцільною. Тобто коли ми говоримо про психологічні засади використання ШІ правоохоронцями, важливо розрізняти три контексти, оскільки вони задають різні профілі компетентностей, ризиків і тактичних помилок:

1. Класична злочинність, коли має місце фізична присутність злочинця на місці злочину, лишаються матеріальні сліди, а, нерідко, є контакт із людською агресією та травмою. Психологічні вимоги до правоохоронців зазвичай включають стресостійкість, комунікативну майстерність, етична чутливість у зборі доказів, уміння інтегрувати цифрові підказки (відеоаналітика, розпізнавання) з людською інтуїцією та досвідом.

2. Кіберзлочинність без ШІ, коли має місце «невидимий» супротивник, транскордонність, перевага інформаційних і процесуальних навичок. Психологічні вимоги до правоохоронців зазвичай включають: когнітивна гнучкість, толерантність до невизначеності, робота з інформаційним перевантаженням, міжвідомча координація, цифрова грамотність (без надмірної віри в «чарівність» інструментів).

3. Кіберзлочинність, що активно використовує ШІ, коли має місце симетрія «ШІ проти ШІ», швидка еволюція тактик, синтетичний контент високої правдоподібності, часткова автоматизація атаки. Психологічні вимоги до правоохоронців зазвичай включають: критична довіра до ШІ (уникнення як сліпої автоматизації, так і алгоритмічної відрази), стратегічне мислення, здатність працювати з мінливою картиною ризиків, профілактика «цифрової параної», уміння приймати остаточні рішення та документувати сумніви.

Інакше кажучи, «класика», «кібер без ШІ» і «кібер із ШІ» – це не взаємовиключні, а нашаровані реальності, кожна з яких висуває свій набір психологічних вимог до правоохоронця. У всіх згаданих різновидах злочинності є доречним застосування ШІ. Однак у випадку класичної злочинності роль ШІ полягає у допоміжній криміналістиці (відеоаналітика, розпізнавання об'єктів/облич, предиктивний аналіз «гарячих точок»), інтерпретації цифрових підказок у поєднанні з польовими спостереженнями, управління вторинною травматизацією, командна координація між «аналоговими» і «цифровими» ролями тощо. У контексті протидії класичній злочинності ШІ виступає як потужний інструмент для аналізу великих обсягів даних про минулі злочини (місце, час, тип злочину) для ідентифікації закономірностей та прогнозування потенційних «гарячих точок». Це дозволяє правоохоронним органам ефективніше розподіляти ресурси та запобігати злочинам. ШІ може допомогти в аналізі відеозаписів з камер спостереження, ідентифікації підозрюваних за допомогою розпізнавання обличчя, а також у швидкій обробці інформації з різних джерел (показання свідків, фінансові транзакції тощо), що значно прискорює процес розслідування.

Кіберзлочинність без використання ШІ різко підвищує роль ШІ для правохоронців. Йдеться про аналітичне підсилення слідчих – моніторинг мереж, кореляція журналів, графовий аналіз зв'язків, пріоритизація інцидентів. Психологічні акценти в діяльності правоохоронців стосується когнітивної гнучкості, толерантності до «невидимого супротивника», протидії інформаційному перевантаженню,

міжвідомчої взаємодії тощо. Протидія кіберзлочинності без використання ШІ може зробити ШІ корисним для виявлення та аналізу кібератак, які не ґрунтуються на ШІ. Це більш технічна боротьба, де ШІ є аналітиком і детектором. ШІ також може моніторити мережевий трафік, поведінку користувачів та системи в цілому, щоб виявити незвичні активності, які можуть свідчити про кібератаку (наприклад, фішинг, DDoS-атаки, несанкціонований доступ). ШІ здатен швидко аналізувати велику кількість зразків шкідливого програмного забезпечення, ідентифікувати його характеристики та розробляти відповідні «антидоти». Це значно швидше, ніж ручний аналіз. Аналіз цифрових слідів допомагає ШІ ідентифікувати закономірності поведінки хакерів, що дозволяє правоохоронцям краще розуміти їхні методи.

Кіберзлочинність, що використовує ШІ (AI-enabled) робить роль ШІ критично важливою, освільки стає неодхідною симетрична протидія («ШІ проти ШІ») – виявлення deepfake/voice-clone, детекція синтетики, моделювання поведінки бот-мереж, контргенерація пасток. Психологічні акценти у діяльності правоохоронців зміщуються на керування рівнем довіри до алгоритмів (уникання сліпої автоматизації та «алгоритмічної відрази»), прийняття рішень у ситуації швидкої еволюції тактик, профілактика «цифрової параної». Це найскладніший сценарій, оскільки боротьба переходить у площину «ШІ проти ШІ». Злочинці використовують ШІ для створення динамічних та швидкозмінних атак, які здатні обходити традиційні системи безпеки. Наприклад, ШІ може генерувати унікальні фішингові листи для кожного одержувача або автоматично змінювати код шкідливого ПЗ. У відповідь, правоохоронні органи повинні використовувати власні системи ШІ, які здатні навчатися та адаптуватися до нових загроз у режимі реального часу. У цьому контексті ШІ може бути використаний для імітації поведінки правоохоронних органів, щоб заплутати злочинний ШІ та виявити його слабкі місця. У цьому сценарії критично важливим є людський фактор. Правоохоронцям потрібно не лише розуміти технічні аспекти, а й психологічні особливості «людини за машиною», яка керує ворожим ШІ. Розуміння мотивації та стратегії зловмисника дозволить випередити його.

Різниця між цими трьома сценаріями полягає у ролі, яку відіграє ШІ: від аналітичного інструменту (класична злочинність) до виявника (кіберзлочинність без ШІ) і, нарешті, до адаптивної системи, що бореться з іншою адаптивною системою (кіберзлочинність, що використовує ШІ). Це вимагає від правоохоронців не лише технічних знань, а й глибокого розуміння психології взаємодії з ШІ. Узагальнено все можна представити у таблиці1.

Контекст «ШІ проти ШІ» з точки зору юридичної психології створює унікальні виклики та вимагає від правоохоронців не лише технічних, а й глибоких психологічних змін. Адже конфронтація «ШІ проти ШІ» – це не просто технологічна битва, а й психологічні перегони озброєнь. Злочинці використовують ШІ для автоматизації атак, що робить їх швидшими, складнішими для відстеження та менш залежними від людського фактора. Це створює величезний психологічний тиск на правоохоронців, оскільки їм доводиться протистояти ворогу, який не спить, не втомлюється і може адаптуватися за долі секунди.

Таблиця 1

Порівняльна матриця використання ШІ правоохоронцями у трьох контекстах

Критерій	**1) Класична злочинність**	**2) Кіберзлочинність без ШІ**	**3) Кіберзлочинність з використанням ШІ**
Об'єкт протидії	Людина/група; матеріальні сліди	Людина/група в мережі; цифрові сліди	Людина + адаптивні алгоритми; синтетичні сліди
Роль ШІ у правоохоронця	Допоміжна криміналістика	Аналітика/пріоритизація інцидентів	«ШІ-проти-ШІ»: контргенерація, детекція синтетики
Ключові компетентності	Аналітичне мислення, комунікація, етика доказів	Цифрова грамотність, когнітивна гнучкість	Толерантність до невизначеності, стратегічність, критична довіра до ШІ
Провідні ризики	Вигорання, вторинна травма	Інформаційне перевантаження, ізоляція	Хронічна «гонка озброєнь», фрагментація уваги
Типові помилки	Переоцінка «об'єктивності» відеоаналітики	Тунельне мислення на технічних деталях	Автоматизаційна упередженість / алгоритмічна відраза
Оцінка ефективності	Час до події/розкриття; якість доказів	MTTR інцидентів; точність атрибуції	Детекція синтетики; зменшення шкоди від шахрайств з використанням ШІ

Постійна необхідність моніторингу та реагування на динамічні загрози, які створює ворожий ШІ, може призвести до емоційного та професійного вигорання. Правоохоронець може відчувати себе відстаючим, незважаючи на всі зусилля. Окрім того важливе значення має й «Ефект невидимого ворога», бо психологічно складно боротися з ворогом, який не має фізичного втілення. Це почуття невизначеності та відсутність прямої конфронтації можуть вплинути на мотивацію та відчуття значущості.

У цьому сценарії ШІ стає для правоохоронця партнером і зброєю одночасно. Це створює психологічну дилему щодо довіри. Йдеться про те наскільки правоохоронець готовий довіряти рекомендаціям свого ШІ? Чи може він сліпо покладатися на нього в критичній ситуації? Якщо ШІ дає збій, це може підірвати довіру не лише до технології, а й до всієї системи. Правоохоронець також може стати надмірно залежним від аналізу, який надає ШІ, і втратити здатність до інтуїтивного, критичного мислення, яке є ключовим для розслідування. Юридична психологія підкреслює, що саме людська здатність до аналізу контексту та невербальних сигналів є унікальною і не може бути повністю замінена машиною. При цьому ключове психологічне завдання – не передати відповідальність ШІ, а навчитися ефективно працювати з ним. Роль правоохоронця змінюється з безпосереднього виконавця

на стратегічного супервайзера та верифікатора. Його психологічна стійкість та етична позиція стають вирішальними.

Таким чином, у сценарії «ШІ проти ШІ» юридична психологія стає не просто допоміжною, а фундаментальною наукою, яка допомагає зрозуміти та підготувати людину до нової ери правоохоронної діяльності. Це винятково важливо, оскільки використовуючи аналогію з військовою історією, можна стверджувати, що в боротьбі «ШІ проти ШІ» у кримінологічному аспекті наразі переважає сторона нападу. Це пов'язано з кількома ключовими факторами. Зокрема злочинні угруповання, що використовують ШІ, не обтяжені бюрократією та законодавчими обмеженнями. Вони можуть швидко створювати та розгортати нові адаптивні атаки, які миттєво масштабуються по всьому світу. ШІ дозволяє автоматизувати пошук вразливостей і генерувати унікальний шкідливий код, що ускладнює його виявлення традиційними засобами.

Окрім того на сьогодні має місце така асиметрична перевага, коли створення одного ефективного ШІ-інструменту для атаки вимагає менше ресурсів, ніж розробка всеохоплюючої системи оборони. Злочинцям достатньо знайти одну слабку ланку, тоді як правоохоронні органи повинні захищати всі можливі вектори атаки. Діє також і «Ефект чорного ринку коли технології ШІ, що використовуються для злочинних цілей, швидко поширюються. Це дозволяє навіть менш кваліфікованим злочинцям використовувати складні інструменти. Однак, як і у військовій історії, домінування нападу не є вічним. Існує кілька факторів, які в перспективі можуть змістити баланс на користь оборони. Правоохоронні органи, корпорації кібербезпеки та наукові спільноти можуть об'єднати зусилля, створюючи «колективний інтелект» для протидії загрозам. Обмін даними та спільна розробка захисних ШІ-систем може значно підвищити їх ефективність.

На даний момент, можна з упевненістю сказати, що хоч сторона нападу і перевершує сторону оборони, що пояснюється їхньою гнучкістю, асиметричною перевагою та відсутністю правових обмежень. Однак у довгостроковій перспективі, за умови координації зусиль, значних інвестицій та розвитку адаптивних захисних технологій, баланс може зміститися. Боротьба «ШІ проти ШІ» – це постійна еволюційна гонка, де кожна зі сторін постійно навчається та адаптується до стратегій іншої.

Інтеграція штучного інтелекту у злочинну діяльність створює нові виклики для правової системи, психології та кібербезпеки. Якщо раніше використання технологій у кримінальній сфері обмежувалося традиційними засобами автоматизації, то нині алгоритми машинного навчання, генеративні нейронні мережі та інші інструменти ШІ відкрили можливості для нових форм злочинів, які відрізняються високою адаптивністю, анонімністю та психологічним впливом на жертв.

Висновки і перспективи подальших досліджень. Проведений аналіз дає підстави стверджувати, що сучасний «спектр» злочинності зазнає якісної трансформації внаслідок інтеграції штучного інтелекту до соціально-правових практик. Якщо класичні злочини характеризувалися безпосереднім міжособистісним контактом та матеріальними слідами, а кіберзлочини без ШІ – віртуалізацією середовища та інформаційною анонімністю, то поява ШІ-опосередкованих правопорушень формує нову реальність: гібридну суб'єктність та алгоритмізовану злочинність, що

змінюють саму природу криміногенного середовища. Відтак в юридичній психології слід враховувати тривимірність сучасного спектру злочинності – за параметрами автономності технологій, ступеня людської участі та рівня психологічного впливу, а також нові типи суб'єктності, зокрема «людина+ШІ» як кримінальний агент, що поєднує раціональність та алгоритмічну адаптивність. Це створює нові психологічні виклики для правоохоронців: необхідність критичної довіри до алгоритмів, здатність працювати в умовах високої невизначеності, ризик «цифрової параної» та професійного вигорання.

Перспективи подальших досліджень можуть полягати у розробці інтегративних моделей суб'єктності у форматі «human-in/over-the-loop», аналіз психологічних механізмів прийняття рішень у взаємодії з алгоритмами, напрями: створення та апробація психодіагностичних інструментів для вивчення алгоритмічної довіри, цифрової тривожності, схильності до маніпулятивних впливів ШІ, побудові сценарних прогнозів еволюції злочинності у координатах BANI-контексту (нестабільність, невизначеність, багатозначність, нестійкість), формуванні програм психопрофілактики кіберзлочинності, розвиток компетенцій правоохоронців і юристів у сфері роботи з ШІ, створення систем колективного штучного інтелекту для виявлення й нейтралізації загроз.

У підсумку, юридична психологія має трансформуватися від аналізу «людини-злочинця» в умовах класичної злочинності до системного дослідження ко-еволюції людини й алгоритму у сфері протиправних дій. Саме створення науково обґрунтованої концепції еволюції «спектру» злочинності може стати підґрунтям для нової генерації профілактичних, правових і психотерапевтичних стратегій у світі, де природний і штучний інтелект взаємодіють у спільному просторі.

Література

1. Асірян С. Р. Кроки країн ЄС у напряму захисту конституційних прав громадян в епоху штучного інтелекту // *Науковий* вісник Ужгородського національного університету. Серія : Право. 2023. Вип. 76(2). С. 285–290.

2. Барановський О. В. Історико-правовий аналіз діяльності міліції України у сфері протидії кіберзлочинності (1991–2015 рр.) // *Держава та регіони*. Серія : Право. 2019. № 1. С. 4–10.

3. Бєлова М. В., Бєлов Д. М., Рущак І. В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики // Аналітично-порівняльне правознавство / редкол.: Ю. М. Бисага (голов. ред.), В. В. Заборовський, Д. М. Бєлов, С. Б. Булеца та ін. – Ужгород : ДВНЗ «УжНУ», 2025. № 1. С. 818–824.

4. Бєлова М. В., Бєлов Д. М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід // Аналітично-порівняльне правознавство. 2023. № 2. С. 448–453.

5. Бугера О. І. Використання штучного інтелекту для запобігання злочинності // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : *Юридичні науки*. 2021. Т. 32(71), № 6. С. 82–86.

6. Варава І. Інновації у професійній діяльності юристів: використання потужностей штучного інтелекту // Інформація і право. 2020. № 1. С. 47–54.

7. Великанова М. М. Штучний інтелект: правові проблеми та ризики // *Вісник* Національної академії правових наук України. 2020. Т. 27, № 4. С. 220–238.

8. Владленова І. В., Кальницький Е. А. Кіберзлочинність як виклик інформаційному суспільству // Гілея: науковий вісник. 2013. № 77. С. 142–146.

9. Гетманцев О., Алєксєєва А. Правові та організаційні засади використання штучного інтелекту у цивільному судочинстві // Ehrlich's journal. 2024. Т. 8. С. 32–37.

10. Гришко В. І., Вознюк С. С. Проблемні аспекти впровадження штучного інтелекту у сфері юриспруденції // Аналітично-порівняльне правознавство. 2024. № 2. С. 29–34.

11. Гуцалюк М. В. Кіберзагрози під час гібридної війни та протидія організованій кіберзлочинності // Інформація і право. 2025. № 1. С. 123–131.

12. Гуцалюк М. В. Новітні тенденції кіберзлочинності // Інформація і право. 2021. № 1. С. 79–89.

13. Кармаза О. О. Принципи штучного інтелекту в правосудді України // *Право і суспільство*. 2021. № 2. С. 18–24.

14. Каткова Т. Г. Штучний інтелект в Україні: правові аспекти // *Право і суспільство*. 2020. № 6. С. 46–55.

15. Ковальчук О. Я. Правові рамки застосування штучного інтелекту в судовій системі // Міжнародний науковий журнал «Інтернаука». Серія : *Юридичні науки*. 2024. № 5. С. 21–27.

16. Кривицький Ю. В. Штучний інтелект як інструмент правової реформи: потенціал, тенденції та перспективи // *Науковий* вісник Національної академії внутрішніх справ. 2021. № 2. С. 90–101.

17. Миколаєць В. А. Стан правової регламентації застосування технологій штучного інтелекту // Ірпінський юридичний часопис. 2022. Вип. 1. – С. 42–51.

18. Муравська Ю., Метельський І., Романів Р. Перспективи використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності // Актуальні проблеми правознавства. 2024. № 2. С. 90–97.

19. Похиленко І. С. Штучний інтелект у судовому процесі : виклики для права на справедливий суд // Права людини та публічне врядування : матеріали VIII Міжнародного правничого форуму, м. Чернівці, 30 травня 2025 р. Львів Торунь : Liha-Pres, 2025. С. 198–202.

20. Радутний О. Е. Відповідальність юридичної особи у кримінальному праві у розрізі правосуб'єктності штучного інтелекту // Інформація і право. 2024. № 2. С. 138–150.

21. Самойленко О., Цехан Д. Транснаціональні кіберзлочини : навч.-метод. посіб. для здобувачів вищої освіти [Електронне видання] / О. Самойленко, Д. Цехан ; Нац. ун-т «Одеська юридична академія». Одеса : Фенікс, 2024. 136 с.

22. Стратонов В. М., Дзюрбель А. Д. Використання штучного інтелекту та інформаційних можливостей у створенні профіля злочинця // *Науковий* вісник Херсонського державного університету. Серія : *Юридичні науки*. 2024. Вип. 5. С. 21–26.

23. Цьомра В. Ю., Корильчук С. Т., Оленюк Д. О. Розвиток штучного інтелекту в сучасній юриспруденції // Scientific notes of Lviv University of Business and Law. 2023. Вип. 38. С. 100–108.

24. Aliane N. Role of AI, e-governance and cyberbullying coping // International Journal of Cyber Criminology. 2024. Vol. 18, No. 1. P. 122–138. Режим доступу: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/download/364/115 (дата звернення: 12.09.2025).

25. Cybercrime and Artificial Intelligence [Електронний ресурс] // ResearchGate. 2025. Режим доступу: https://www.researchgate.net/publication/383532701_CYBERCRIME_AND_ARTIFICIAL_INTELLIGENCE (дата звернення: 12.09.2025).

26. Mohamed E., Ahmed S., Zhang Y. Artificial intelligence and machine learning in cybersecurity // Knowledge and Information Systems. 2025. Vol. 67, No. 2. P. 455–482. DOI: 10.1007/s10115-025-02429-y.

27. Schmitt C., Flechais I. Digital deception: generative artificial intelligence in social engineering and phishing [Електронний ресурс] // arXiv. 2023. Режим доступу: https://arxiv.org/abs/2310.13715 (дата звернення: 12.09.2025).

Анотація

Батраченко Т. С., Батраченко І. Г., Єфімова І. В. **Еволюція «спектру» злочинності в епохи природного та штучного інтелекту.** – Стаття.

У статті розглядається феномен трансформації сучасної злочинності під впливом цифровізації та зростання ролі штучного інтелекту. Автори аналізують еволюцію поняття «спектр злочинності», акцентуючи увагу на переході від традиційних форм правопорушень до кіберзлочинів, що використовують інструменти штучного інтелекту та алгоритмічні системи. Зазначається, що цифрове середовище не лише розширює можливості правопорушників, а й радикально змінює психологічні механізми впливу на особу: від прямого фізичного тиску до маніпуляцій інформаційними потоками, алгоритмами та персональними даними. У роботі підкреслюється міжнародний характер нових викликів, що зумовлений глобалізацією інформаційного простору, швидким поширенням цифрових технологій та транснаціональною природою кіберзлочинності, яка не визнає державних кордонів, що

істотно ускладнює її виявлення, розслідування та притягнення винних до відповідальності й, у свою чергу, вимагає від держав поглибленої співпраці, координації зусиль на міждержавному рівні, розроблення спільних стандартів безпеки та ефективного функціонування міжнародних механізмів протидії. Особливу увагу приділено психологічним аспектам: формуванню довіри до цифрових технологій, ризикам розвитку цифрової тривожності, можливості втрати критичного мислення у віртуальному просторі. Автори виокремлюють низку прогалин у сучасних дослідженнях: відсутність цілісної таксономії «цифрових» і «алгоритмічних» злочинів, недопрацьовані методики психодіагностики віктимності, недостатню інтеграцію між правовою та психологічною науками. Запропоновано розвивати комплексні міждисциплінарні підходи, що поєднують правові інструменти з психологічними індикаторами у виявленні та запобіганні злочинам. Робиться висновок, що протидія новим формам злочинності потребує не лише удосконалення правового регулювання, а й інвестицій у наукові дослідження, створення адаптивних систем захисту на основі ШІ та підготовки фахівців, здатних поєднувати юридичні та психологічні знання. Представлений аналіз може бути корисним для науковців, правників, фахівців із кібербезпеки та усіх, хто цікавиться проблематикою безпеки у цифрову добу.

Ключові слова: спектр злочинності, кіберзлочинність, штучний інтелект, психологічна безпека, правове регулювання.

Summary

Batarchenko T. S., Batarchenko I. H., Yefimova I. V. **Evolution of the «spectrum of crime» in the era of natural and artificial intelligence.** – Article.

The article examines the phenomenon of the transformation of contemporary crime under the influence of digitalization and the growing role of artificial intelligence. The authors analyze the evolution of the concept of the "spectrum of crime," emphasizing the transition from traditional forms of offenses to cybercrimes that employ artificial intelligence tools and algorithmic systems. It is noted that the digital environment not only expands the capabilities of offenders but also radically alters the psychological mechanisms of influence on individuals: from direct physical pressure to manipulation through information flows, algorithms, and personal data.

The study highlights the international nature of emerging challenges, shaped by the globalization of the information space, the rapid spread of digital technologies, and the transnational character of cybercrime, which recognizes no state borders. This significantly complicates detection, investigation, and prosecution, while simultaneously demanding deeper cooperation among states, coordination of efforts at the interstate level, the development of joint security standards, and the effective functioning of international counteraction mechanisms.

Special attention is paid to psychological aspects: the formation of trust in digital technologies, the risks of developing digital anxiety, and the potential loss of critical thinking in virtual environments. The authors identify several gaps in current research: the absence of a comprehensive taxonomy of "digital" and "algorithmic" crimes, underdeveloped methods of psychodiagnostics of victimization, and insufficient integration between legal and psychological sciences.

The article proposes advancing complex interdisciplinary approaches that combine legal instruments with psychological indicators in the detection and prevention of crime. It concludes that combating new forms of criminality requires not only the improvement of legal regulation but also investment in scientific research, the creation of adaptive AI-based protection systems, and the training of specialists capable of integrating legal and psychological knowledge. The analysis presented may be of value to scholars, legal practitioners, cybersecurity experts, and all those interested in security issues in the digital age.

Key words: crime spectrum, cybercrime, artificial intelligence, psychological security, legal regulation.

Дата надходження статті: 24.09.2025
Дата прийняття статті: 22.10.2025
Дата публікації: 27.11.2025