6. Огляд судової практики Верховного Суду у справах щодо державної служби (проходження державної служби): рішення, внесені до ЄДРСР за період з 2019 року по березень 2026 року / упоряд. Управління аналітичної та правової роботи Касаційного адміністративного суду Департаменту аналітичної та правової роботи Апарату Верховного Суду. Київ, 2026. 34 с. URL: https://strapi.supreme.court.gov.ua/uploads/Oglyad_Prohod_derzh_slyzhbu_2019_03_2026_10b5cf1ef1.pdf (дата звернення: 17.09.2026).

DOI https://doi.org/10.36059/978-966-397-670-9-25

ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ КОРУПЦІЙНИХ ТРАНСФОРМАЦІЙ ВОЄННОГО ЧАСУ: КРИМІНАЛЬНО-ПРАВОВІ ВИКЛИКИ ТА НАПРЯМИ ПРОТИДІЇ[1]

Клочко Альона Миколаївна
доктор юридичних наук, професор,
провідний науковий співробітник,
Сумський національний аграрний університет
м. Суми, Україна

Значення цифрових технологій, що містять елементи штучного інтелекту (далі – ШІ), динамічно зростає в умовах комплексного розвитку суспільних відносин, поглиблення процесів цифровізації та появи нових викликів і загроз, зумовлених трансформаційним характером сучасної злочинності. Особливої актуальності зазначена проблематика набуває в умовах дії проаового режиму воєнного стану, коли масштабні зміни у функціонуванні державних інституцій, перерозподіл бюджетних ресурсів, збільшення обсягів оборонних і публічних закупівель, спрощення окремих адміністративних процедур та прискорена цифровізація публічного управління спричиняють не лише модернізацію механізмів державного управління, а й трансформацію корупційних ризиків. Воєнний стан формує специфічне середовище, у якому традиційні корупційні практики можуть поєднуватися з новітніми цифровими технологіями. Використання ШІ здатне змінювати способи підготовки, вчинення та приховування

[1] Публікація підготовлена в рамках проекту «Трансформація корупційних ризиків в умовах воєнного стану: цифровізація, кримінально-правові механізми та євроінтеграційні перспективи » № 0126U004105 від 10.06.2026р.

корупційних кримінальних правопорушень, ускладнювати встановлення причетних осіб, походження цифрових даних і причинно-наслідкових зв'язків між поведінкою конкретного суб'єкта та суспільно небезпечними наслідками [1, с. 4]. Водночас технології ШІ можуть використовуватися для аналізу значних масивів інформації, виявлення аномальних фінансових операцій, конфліктів інтересів, ризикових закупівель та інших індикаторів можливої корупційної поведінки. Тож в умовах воєнного стану ШІ набуває подвійного кримінологічного значення: з одного боку, він може виступати технологічним інструментом трансформації та ускладнення корупційних практик, а з іншого – засобом їх виявлення, прогнозування та запобігання.

Істотного значення набувають корупційні ризики у сферах, безпосередньо пов'язаних із забезпеченням обороноздатності держави, використанням бюджетних і міжнародних фінансових ресурсів, оборонними та іншими публічними закупівлями, відновленням пошкодженої інфраструктури, розподілом гуманітарної допомоги та управлінням державними ресурсами. Значні обсяги фінансування, необхідність оперативного прийняття управлінських рішень та об'єктивне обмеження відкритості окремих даних з міркувань національної безпеки можуть створювати додаткові можливості для корупційних зловживань. За таких умов цифрові технології та системи ШІ потенційно можуть використовуватися для автоматизації шахрайських і корупційних схем, маніпулювання цифровими даними, створення фальсифікованих документів і цифрового контенту, приховування фінансових операцій, імітації комунікації посадових осіб або інших форм введення в оману.

Трансформація корупційних ризиків під впливом ШІ не означає автоматичної необхідності криміналізації кожної нової форми технологічно опосередкованої поведінки. Принципово важливим є встановлення того, чи охоплюються відповідні діяння чинними складами кримінальних правопорушень, а також чи існують достатні соціальні, кримінологічні та правові підстави для встановлення нових кримінально-правових заборон. У цьому аспекті розвиток ШІ формує підґрунтя для дослідження питання про межі криміналізації, юридичну визначеність кримінально-правових норм та недопустимість надмірного застосування кримінальної репресії до технологічно нових, але вже охоплених чинним кримінальним законодавством форм протиправної поведінки.

Доцільність установлення кримінальної відповідальності може бути обґрунтована за сукупності таких обставин: 1) недотримання встановлених регуляторних приписів заподіює істотну шкоду суспільним відносинам або формує реальний ризик її заподіяння;

2) наявні правові механізми не забезпечують достатнього запобіжного впливу, унаслідок чого певні суспільно небезпечні діяння залишаються поза межами ефективного правового реагування; 3) цивільно-правові та адміністративно-правові заходи є недостатніми для належного припинення й попередження протиправної поведінки, пов'язаної із застосуванням цифрових технологій, зокрема систем із компонентами штучного інтелекту.

Окремим викликом є встановлення суб'єкта кримінального правопорушення у випадках, коли ШІ використовується не лише як технічний інструмент, а як система, здатна генерувати результати з обмеженою передбачуваністю для її розробника, оператора чи користувача [2, с. 1684]. У корупційному контексті це питання безпосередньо пов'язане з необхідністю встановлення умислу, мети, фактичного контролю над функціонуванням системи та причинного зв'язку між поведінкою людини і заподіяною шкодою. Саме тому автономність алгоритмічної системи не повинна сама по собі перетворюватися на механізм уникнення кримінальної відповідальності фізичними особами, які свідомо використовують її функціональні можливості для реалізації корупційних схем або приховування їх результатів.

У цьому контексті посилюється значення Акту Європейського Союзу про штучний інтелект (EU AI Act) [3], який формує ризик-орієнтовану модель правового регулювання систем ШІ та встановлює комплекс вимог до їх розроблення, впровадження і використання. Хоча EU AI Act не є актом кримінального законодавства і не встановлює самостійної системи кримінально-правової відповідальності за неправомірне використання ШІ, закріплені ним стандарти мають опосередковане значення для подальшого розвитку національного законодавства. Для України це питання набуває актуальності в контексті європейської інтеграції та необхідності наближення національного цифрового правопорядку до європейських стандартів регулювання ШІ.

З урахуванням активізації корупційних ризиків, пов'язаних із використанням ШІ у воєнний час, доцільно доповнити ЗУ «Про запобігання корупції» [4] положеннями, які зобов'язуватимуть органи державної влади проводити оцінювання корупційних ризиків перед упровадженням алгоритмічних систем у сферах оборонних закупівель, розподілу гуманітарної допомоги та бюджетних коштів. Така оцінка має охоплювати перевірку джерел даних, можливостей зовнішнього втручання, наявності конфлікту інтересів і механізмів людського контролю. Проте рішення, сформоване за допомогою інструментів ШІ, не повинно звільняти посадову особу від персональної юридичної відповідальності, а навмисне використання алгоритмічної системи для

приховування корупційного правопорушення або одержання неправомірної вигоди доцільно передбачити у КК України [5] як обставину, що обтяжує кримінальну відповідальність.

Таким чином, цифровізація та розвиток ШІ в умовах воєнного стану виступають одним із чинників трансформації сучасних корупційних ризиків, змінюючи способи вчинення, приховування, виявлення та документування відповідних правопорушень. Це зумовлює необхідність формування комплексної кримінально-правової та кримінологічної моделі реагування, яка поєднуватиме технологічні засоби запобігання корупції, належне регуляторне забезпечення використання ШІ та кримінально-правові механізми реагування на найбільш суспільно небезпечні форми зловживання цифровими технологіями. В умовах воєнного стану та подальшої повоєнної відбудови України особливого значення набуває не стільки розширення кримінально-правових заборон саме по собі, скільки забезпечення їх обґрунтованості, правової визначеності та здатності ефективно реагувати на нові форми корупційної поведінки, не створюючи водночас перешкод для правомірного технологічного розвитку.

Сучасна динаміка розвитку технологій ШІ та їх впровадження у сфери публічного управління, фінансів, правосуддя, інформаційної безпеки й обумовлює необхідність посилення кримінально-правової охорони від суспільно небезпечних форм їх використання. Виникнення якісно нових способів учинення та приховування кримінальних правопорушень із застосуванням алгоритмічних систем потребує переосмислення меж чинних кримінально-правових заборон.

Література:

1. Alaa Saud, 2024. “Criminal Liability about the Use of Artificial Intelligence: Investigating the Actus Reus Element of AI-driven Technology”, American Journal of Law, AJPO, vol. 6(1), pages 1-25.

2. Kostenko, O.M., Bieliakov, K.I., Tykhomyrov, O.O., Aristova I. V. “Legal personality” of artificial intelligence: methodological problems of scientific reasoning by Ukrainian and EU experts AI & Society 2023. Volume 39. p. 1683–1693 (2024). URL: https://doi.org/10.1007/s00146-023-01641-0. URL: https://goo.su/c60s.

3. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту (Акт про штучний інтелект) та вносить зміни до регламентів (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 і (ЄС) 2019/2144 та директив 2014/90/ЄС, (ЄС) 2016/797 і (ЄС) 2020/1828 (Акт про штучний інтелект). OJ L, 2024/1689, 12.07.2024.

4. Про запобігання корупції: Закон України від 14 жовтня 2014 р. № 1700-VII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text.

5. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

DOI https://doi.org/10.36059/978-966-397-670-9-26

РОЛЬ І МІСЦЕ КРИМІНОЛОГІЧНОЇ ІНФОРМАЦІЇ У ПРАВОВОМУ МЕХАНІЗМІ ЗАПОБІГАННЯ ЗЛОЧИНАМ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Колб Олександр Григорович
доктор юридичних наук, професор,
професор кафедри кримінального права та процесу,
Державний податковий університет,
заслужений юрист України
м. Ірпінь, Україна

Дучимінська Леся Миронівна
начальник управління контрольно-перевірочної роботи,
Головне управління Пенсійного фонду України у Волинській області
м. Луцьк, Україна

Результати вивчення законодавчих та інших нормативно-правових актів України, що стосуються сфери запобігання і протидії злочинності, свідчать про те, що останнім часом все рідше у них вживається термін «кримінологічна інформація», а це, у свою чергу, зменшує рівень запобіжної діяльності та ефективність реалізації на практиці відповідних відомостей, пов'язаних з її предметом (про злочинність; причини і умови її виникнення, розвитку та функціонування; особу кримінального правопорушника; заходи, спрямовані на недопущення суспільно небезпечних явищ і наслідків) [1, с. 15–27].

Як приклад можна назвати ті тенденції, що склалися впродовж дії прийнятого у 2012 Кримінального процесуального кодексу (КПК) України (2013–2025 рр.), а також ті суспільно небезпечні наслідки, які їх спричинили та обумовили [2]. Мова, зокрема, йде про різку невідповідність відомостей про кількість щорічно зареєстрованих та облікованих в Єдиному реєстрі досудових розслідувань (ЄРДР)