УДК: 342.9:004.8:343.352
DOI https://doi.org/10.24144/2788-6018.2025.06.3.85

АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМАХ АВТОМАТИЗОВАНОГО ПРИЙНЯТТЯ РІШЕНЬ (АПР) ЯК ПРЕВЕНЦІЯ КОРУПЦІЙНИХ РИЗИКІВ

Головацький Н.Т.,
старший викладач кафедри адміністративного,
фінансового та інформаційного права
юридичного факультету
ДВНЗ «Ужгородський національний університет»
ORCID: 0000-0003-3593-6143

Головацький Н.Т. Адміністративно-правові механізми захисту персональних даних у системах автоматизованого прийняття рішень (апр) як превенція корупційних ризиків.

Вказується, Україна обрала стратегічний курс на цифрову трансформацію державного управління та сфери адміністративних послуг, що зумовлює дедалі ширше впровадження систем автоматизованого прийняття рішень (АПР). Така модернізація є вкрай необхідною для оптимізації діяльності адміністративних органів, скорочення бюрократичних процедур, а також протидії побутовій корупції, джерелом якої нерідко стає дискреційний характер повноважень чиновників.

В умовах стратегічного курсу України на цифровізацію публічного управління та надання адміністративних послуг, все частіше використовуються системи автоматизованого прийняття рішень (АПР), що є необхідним для підвищення ефективності та усунення побутової корупції. Проте, технологічна трансформація спричинила виникнення нового, складного адміністративно-правового конфлікту, який проявляється через недосконалість чинного національного законодавства. Дослідження акцентує увагу на кризі адміністративної відповідальності: відсутність прозорості в роботі алгоритмів та неможливість ефективно застосувати адміністративну відповідальність до суб'єкта владних повноважень через приховану обґрунтованість рішення «чорним ящиком». Цей фактор створює підґрунтя для виникнення явища «Алгоритмічної корупції», яка є системною та не піддається контролю через традиційні механізми. Метою статті є комплексне адміністративно-правове обґрунтування необхідності впровадження механізмів алгоритмічної підзвітності в публічне управління та проведення порівняльно-правового дослідження міжнародних стандартів, зокрема Регламенту ЄС № 2016/679 (GDPR), для виявлення найбільш ефективних практик захисту персональних даних у контексті АПР. Проведене дослідження встановило, що адміністративно-правова природа рішення АПР знаходиться у протиріччі з традиційним поняттям суб'єкта владних повноважень (СВП), оскільки відсутність людини як суб'єкта відповідальності створює зону адміністративної безкарності. Порівняльний аналіз чинного GDPR засвідчив, що українське законодавство лише декларативно закріплює право на людську інтервенцію, але не містить ефективної адміністративно-процедурної інфраструктури для його реалізації. Наукова новизна та практична значущість роботи полягає у формулюванні конкретних пропозицій щодо гармонізації національного законодавства, зокрема Закону України «Про адміністративну процедуру».

Ключові слова: автоматизоване прийняття рішень (АПР), адміністративна процедура, алгоритмічна підзвітність, корупційні ризики, захист персональних даних, право на пояснення, алгоритмічна корупція, оцінка впливу алгоритму (ОАВА), Регламент ЄС (GDPR).

Holvatskyi N.T. Administrative and legal mechanisms for protecting personal data in automated decision-making systems (ADR) as a prevention of corruption risks.

It is indicated that Ukraine has chosen a strategic course for the digital transformation of public administration and the sphere of administrative services, which leads to the increasingly widespread implementation of automated decision-making systems (ADR). Such modernization is extremely necessary for optimizing the activities of administrative bodies, reducing bureaucratic procedures, and combating domestic corruption, the source of which is often the discretionary nature of the powers of officials.

Under Ukraine's strategic course toward the digitalization of public administration and the provision of administrative services, Automated Decision-Making (ADM) systems are increasingly utilized. This process is essential for enhancing the efficiency of administrative bodies, eliminating bureaucracy,

and combating common corruption stemming from officials' discretionary powers. However, this technological transformation has led to a new and complex administrative and legal conflict, stemming from the imperfection of current national legislation. The research focuses on the crisis of administrative accountability: the lack of transparency in the operation of algorithms and the inability to effectively apply administrative liability to the Subject of Authority (SA) due to the hidden justification of the decision by a «black box.» This factor creates the basis for the emergence of «Algorithmic Corruption,» which is systemic and impervious to traditional control mechanisms. The article aims to provide a comprehensive administrative and legal justification for the necessity of implementing algorithmic accountability mechanisms in public administration and to conduct a comparative legal analysis of international standards, particularly EU Regulation No. 2016/679 (GDPR), to identify the most effective practices for personal data protection in the context of ADM. The study established that the administrative and legal nature of an ADM decision contradicts the traditional concept of the Subject of Authority, as the absence of a human subject of responsibility creates a zone of administrative impunity. A comparative analysis of the current GDPR demonstrated that Ukrainian legislation only declaratively enshrines the right to human intervention but lacks the effective administrative and procedural infrastructure for its implementation. The scientific novelty and practical significance of the work lie in formulating concrete proposals for harmonizing national legislation, specifically the Law of Ukraine «On Administrative Procedure,» to integrate procedural safeguards into the administrative process.

Key words: Automated Decision-Making (ADM); Administrative Procedure; Algorithmic Accountability; Corruption Risks; Personal Data Protection; Right to Explanation; Algorithmic Corruption; Algorithmic Impact Assessment (AIA); EU Regulation (GDPR).

Постановка проблеми. В умовах стратегічного курсу України на цифровізацію публічного управління та надання адміністративних послуг, все частіше використовуються системи автоматизованого прийняття рішень (АПР). Цей процес є життєво необхідним для підвищення ефективності адміністративних органів, усунення бюрократії та боротьби з побутовою корупцією, що виникає через дискреційні повноваження посадових осіб.

Проте, технологічна трансформація адміністративної сфери спричинила виникнення нового, більш складного адміністративно-правового конфлікту, який проявляється через недосконалість законодавчого забезпечення, оскільки чинне національне законодавство, включаючи Закон України «Про захист персональних даних», є загальним і не містить деталізованого адміністративно-правового регулювання щодо використання алгоритмів для індивідуального прийняття рішень. Це стосується, зокрема, практичної реалізації права на пояснення та права на людську інтервенцію у випадку незгоди з рішенням АПР. Також присутність виникнення явища «Алгоритмічної корупції», тобто відсутність прозорості в роботі алгоритмів створює ризик внесення свідомих упереджень (bias) у вихідні дані або критерії функціонування системи. Така маніпуляція, призводить до неправомірного надання переваг (чи відмови) окремим суб'єктам, є формою прихованої, системної корупції, яка практично не піддається контролю через традиційні механізми адміністративного оскарження. І також варто відзначити кризу адміністративної відповідальності, тобто у ситуації, коли рішення формально є законним, але його фактична обґрунтованість прихована «чорним ящиком» алгоритму, неможливо ефективно застосувати адміністративну відповідальність до суб'єкта владних повноважень. Це підриває принцип адміністративної законності та довіри громадян до електронного урядування.

Таким чином, існує гостра необхідність у розробці комплексних адміністративно-правових механізмів, які б, з одного боку, забезпечили високий рівень захисту персональних даних при використанні АПР, а з іншого – гарантували прозорість та алгоритмічну підзвітність як фундаментальні антикорупційні запобіжники. Без цього цифровізація може стати джерелом нових корупційних ризиків та викликів.

Аналіз останніх досліджень і публікацій. Питання адміністративно-правового регулювання у сфері цифровізації є предметом активних наукових дискусій в Україні. Значна частина досліджень зосереджена на загальних аспектах ефективності електронного урядування та оптимізації надання адміністративних послуг, зокрема, у працях таких вчених, як В. Авер'янов, А. Вишневський, Т. Коломоєць. Ці науковці закладають фундаментальні основи розуміння трансформації адміністративного права в умовах технологічних змін. Паралельно активно розвивається напрямок, присвячений захисту персональних даних та інформаційному праву. Праці таких дослідників, як О. Поляк, В. Гусєв та І. Ковбас, ґрунтовно вивчають правові засади обробки даних, доступу до публічної інформації та загальні гарантії права на приватність в цифровому середовищі. Окремо досліджується і сфера антикорупційного регулювання, де вчені аналізують адміністративну відповідальність та процедури прозорості (зокрема, Т. Коломоєць та І. Венедіктова).Однак, більшість

останніх публікацій вивчають ці сфери ізольовано. Зокрема, недостатньо уваги приділено саме інтегративному адміністративно-правовому аналізу, який поєднує: а) особливості АПР як джерела адміністративних рішень; б) недоліки існуючих процедур захисту персональних даних (зокрема, права на пояснення) у Законі України «Про адміністративну процедуру»; в) прямий зв'язок між цією процедурною непрозорістю та корупційними ризиками на етапі розробки та впровадження алгоритмів. Таким чином, існує наукова прогалина у розробці чітких, юридично зобов'язуючих адміністративно-правових механізмів алгоритмічної підзвітності та людської інтервенції як необхідних антикорупційних запобіжників.

Мета статті полягає у комплексному адміністративно-правовому обґрунтуванні необхідності впровадження механізмів алгоритмічної підзвітності в публічне управління та проведенні порівняльно-правового аналізу міжнародних стандартів (зокрема, досвіду Європейського Союзу щодо Загального регламенту про захист даних (GDPR)) для виявлення найбільш ефективних практик захисту персональних даних у контексті автоматизованого прийняття рішень (АПР). На основі цього аналізу планується розробити та обґрунтувати теоретико-практичну модель адміністративно-правових механізмів прозорості та контролю в системах АПР, яка передбачає гарантування права суб'єкта на зрозуміле пояснення та людський перегляд автоматизованого рішення. Кінцевим результатом роботи є формулювання конкретних пропозицій щодо гармонізації національного законодавства (зокрема, Закону України «Про захист персональних даних» та Закону України «Про адміністративну процедуру») з міжнародними вимогами, з метою усунення правових прогалин, що створюють підґрунтя для прихованих корупційних ризиків, та зміцнення адміністративної законності в умовах цифровізації.

Виклад основного матеріалу. Ключове протиріччя, яке виникає в українському адміністративному праві при переході від людини-чиновника до алгоритму, полягає у конфлікті між традиційним поняттям суб'єкта владних повноважень (СВП) та технологічним засобом прийняття рішення. Традиційно, адміністративне право базується на припущенні, що рішення приймає людина, яка наділена дискреційними повноваженнями (хоча б мінімальними) та підлягає адміністративній відповідальності. Саме СВП, згідно з Законом України «Про адміністративну процедуру», забезпечує обґрунтованість, пропорційність та законність адміністративного акта [1].

У той час, як система АПР є лише інструментом або засобом обробки даних. Рішення, прийняте виключно алгоритмом, не має тих самих ознак, що й рішення людини-СВП, оскільки алгоритм не може бути суб'єктом відповідальності і не може пояснити своє рішення у юридичному сенсі, оперуючи мотивами чи доцільністю [2].

Цей конфлікт підриває легітимність та юридичну силу самого адміністративного акта, оскільки ускладнює встановлення таких питань, як: 1. Хто несе адміністративну відповідальність за неправомірне чи упереджене рішення?; 2. Чи було дотримано право суб'єкта на пояснення та перегляд, гарантоване Законом України «Про захист персональних даних» та міжнародними стандартами? [3].

Це правове нерозуміння природи рішення АПР – коли немає чіткого людського суб'єкта, який підлягає контролю та відповідальності – безпосередньо створює ґрунт для корупційного ризику.

Критичним адміністративно-правовим правом, яке є ключовим для розкриття та оскарження прихованого корупційного рішення АПР, є право суб'єкта на пояснення та право на людську інтервенцію. У сучасному українському адміністративному праві, відповідно до Закону України «Про адміністративну процедуру», будь-який адміністративний акт має бути обґрунтованим, тобто містити мотивацію (підстави), що дозволяє особі зрозуміти, чому було прийнято саме таке рішення [1].

Ця вимога є фундаментальним запобіжником проти свавілля та, як наслідок, проти корупції. Однак, коли рішення приймається виключно алгоритмом (АПР), дотримання вимоги щодо мотивації стає формальним і незрозумілим. Посадова особа, що підписує електронний акт, часто не може надати сутнісного, юридично значущого пояснення логіки автоматизованих систем.

Саме тут виникає концептуальна прогалина: Право на пояснення (у сфері захисту даних) є ключовим інструментом для забезпечення прозорості адміністративного акта. Закон України «Про захист персональних даних» надає особі право вимагати пояснення щодо обробки її персональних даних, що включає інформованість про: хто, для чого, кому, на яких підставах та як довго обробляє дані. Ця вимога ґрунтується на принципах добровільності та інформованої згоди, закріплених у статті 2 Закону, яка вимагає, щоб володілець даних чітко та доступно пояснив усі умови обробки перед її початком. Закон України «Про захист персональних даних» закріплює право суб'єкта не бути об'єктом рішення, що ґрунтується виключно на автоматизованій обробці, яка має суттєві правові наслідки. Проте цей Закон не надає конкретного адміністративно-процедурного механізму реалізації цього права (наприклад, чітких вимог до змісту та форми пояснення, чи стандартів його «зрозумілості») [3].

Антикорупційний вимір: Відсутність такого чіткого механізму робить неможливим встановлення факту алгоритмічної корупції або упередженості в судовому чи адміністративному порядку. Якщо особа не знає, які саме критерії та дані (окрім її власних персональних даних) призвели до негативного рішення, вона не може довести, що на рішення вплинули корупційні маніпуляції з алгоритмом чи вхідними даними. Це руйнує принцип адміністративної підзвітності.

Таким чином, у контексті українського адміністративного права, рішення АПР де-юре залишається адміністративним актом, прийнятим СВП, але де-факто цей акт втрачає свою обґрунтованість та прозорість через «чорний ящик» алгоритму. Для усунення цього корупційного ризику необхідно перейти від загальних декларацій про захист даних до розробки деталізованих адміністративно-правових норм, які чітко визначають процедуру розкриття алгоритму та обов'язкового людського факту перегляду рішення, як невід'ємних елементів законності адміністративного акта, прийнятого АПР.

Основу порівняльного аналізу становить Регламент ЄС № 2016/679 (GDPR), який є чинним та обов'язковим міжнародним стандартом і у Статті 22 закріплює право суб'єкта не бути об'єктом рішення, що ґрунтується виключно на автоматизованій обробці [5].

Це право є критичним, оскільки воно вимагає людської інтервенції та, відповідно, адміністративної підзвітності. Однак, як показує практика, сам GDPR не містить деталізованих процедурних вимог щодо того, як саме адміністративний орган має провести аудит чи пояснити логіку алгоритму. Саме ця прогалина в процедурі, а не в суб'єктивному праві, найбільше сприяє корупційним ризикам в українській адміністративній практиці. Виходячи з цього, для забезпечення ефективності права на скасування рішення АПР, яке ми визначили як ключовий антикорупційний запобіжник, українське законодавство має бути доповнене конкретними вимогами до адміністративного аудиту та документування. Саме відсутність цих вимог не дозволяє посадовій особі виявити та обґрунтувати причини для скасування рішення, яке є технічно правильним, але корупційно упередженим [6].

Для усунення цієї прогалини необхідно закріпити два ключові адміністративно-правові механізми, які є квінтесенцією міжнародних тенденцій у розвитку законодавства з питань використання штучного інтелекту, а саме:

1. Обов'язок документування алгоритмічного впливу, тобто необхідне введення вимоги щодо проведення Адміністративної оцінки впливу алгоритму (аналог Algorithmic Impact Assessment). Ця оцінка, як частина адміністративної процедури, має включати детальне документування наборів вхідних даних (з оцінкою їхньої упередженості), логіки функціонування системи та методології її навчання. Це створює доказову базу для подальшого адміністративного та судового оскарження.

2. Право на незалежний аудит - законодавче закріплення права адміністративного аудиту за уповноваженими контролюючими органами (наприклад, Омбудсменом, НАЗК). Цей аудит має перевіряти документацію АПР на предмет відповідності антикорупційним стандартам та принципам законності, пропорційності та обґрунтованості до введення системи в експлуатацію.

Впровадження цих процедурних вимог у Закон України «Про адміністративну процедуру» перетворює формальне право на пояснення на дієвий антикорупційний інструмент, роблячи АПР підзвітною і контрольованою на всіх етапах.

Для усунення корупційного ризику, що виникає через непрозорість АПР, варто внести зміни до Закону України «Про адміністративну процедуру», запровадивши обов'язкову процедурну інфраструктуру алгоритмічної підзвітності. Пропонується два ключові механізми:

1: Введення оцінки адміністративного впливу алгоритму (ОАВА), тобто необхідно доповнити Закон України «Про адміністративну процедуру» положенням про обов'язкове проведення Оцінки адміністративного впливу алгоритму (ОАВА) для будь-якої системи АПР, що використовується для високоризикових адміністративних рішень. ОАВА має бути обов'язковою попередньою адміністративною процедурою, яка вимагає від СВП (розробника або власника системи) повного документування вхідних наборів даних, логіки алгоритму та результатів перевірки на упередженість. Це створює правовий слід алгоритму, який може бути предметом подальшого аудиту [7]. Цей механізм виступає як потужний превентивний антикорупційний інструмент, оскільки унеможливлює приховане внесення маніпуляцій у дані чи логіку.

2: Деталізація процедури людської інтервенції та оскарження. Слід уточнити відповідні статті Закону України «Про адміністративну процедуру» (щодо оскарження та обґрунтованості адміністративного акта), зазначивши, що: а) оскарження рішення АПР автоматично вимагає змістовного, а не лише технічного чи людського фактору перевірки; б) посадовій особі, яка здійснює перевірку, надається право на скасування або зміну рішення АПР на основі аналізу документації ОАВА. Це гарантує, що право суб'єкта, закріплене у Законі України «Про захист персональних даних», реалізується через ефективну адміністративну процедуру.

Впровадження цих двох процедурних елементів усуває «чорний ящик», відновлює зв'язок із суб'єктом владних повноважень та перетворює адміністративну процедуру на головний антикорупційний механізм у цифровій сфері.

Висновки. Проведене дослідження засвідчило, що впровадження систем автоматизованого прийняття рішень (АПР) в публічне адміністрування створює фундаментальний адміністративно-правовий виклик, який прямо генерує нові корупційні ризики. Основний висновок полягає в тому, що головний ризик корупції в цифровій адміністрації усувається не технічними засобами, а виключно через обов'язковість адміністративного аудиту та права на пояснення, інтегрованих у процедурний закон.

По-перше, встановлено, що адміністративно-правова природа рішення АПР знаходиться у протиріччі з традиційним поняттям суб'єкта владних повноважень (СВП), оскільки відсутність людини як суб'єкта відповідальності створює зону адміністративної безкарності та уможливлює приховану алгоритмічну корупцію через маніпуляції з вхідними даними та логікою системи. Це порушує принцип обґрунтованості адміністративного акта.

По-друге, порівняльно-правовий аналіз чинного Регламенту ЄС № 2016/679 (GDPR) засвідчив, що українське законодавство, зокрема Закон України «Про захист персональних даних», лише декларативно закріплює право на людську інтервенцію, але не містить ефективної адміністративно-процедурної інфраструктури для його реалізації. Це підтверджує необхідність гармонізації адміністративного права України із сучасними міжнародними стандартами прозорості та підзвітності.

По-третє, для усунення виявлених правових прогалин та посилення антикорупційної стійкості запропоновано внесення конкретних змін до Закону України «Про адміністративну процедуру».

Ключовими механізмами є запровадження Оцінки адміністративного впливу алгоритму (ОАВА) як обов'язкової попередньої процедури документування та закріплення права посадової особи на субстантивний перегляд, скасування або зміну рішення АПР на основі даних ОАВА. Ці пропозиції гарантують відновлення адміністративної підзвітності та перетворюють процедурні права суб'єкта на ефективний антикорупційний запобіжник у цифровій сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про адміністративну процедуру: Закон України . *Відомості Верховної Ради України (ВВР),* 2023, № 15, ст. 50. URL: https://zakon.rada.gov.ua/laws/show/2073-20#Text.
2. Гачкевич Андрій. Поняття та правова основа автоматизованого прийняття рішень в Україні. *Український часопис конституційного права.* № 3(36). (2025). 86–97. DOI: https://doi.org/10.30970/jcl.3.2025.7.
3. Про захист персональних даних. Закон України від 01.06.2010 року № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
4. Аністратенко Ю.І., Бодунова О.М., Грицюк І.В. Адміністративно-правові засади регулювання електронного урядування: світовий досвід. *Юридичний науковий електронний журнал.* 2021. № 8. С. 400–404. URL: http://lsej.org.ua/8_2021/96.pdf.
5. Регламент Європейського парламенту і Ради (ЄС) 2016/679, від 27 квітня 2016 року. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
6. Шабатура М.М., Салашник Р.О. Аналіз методів захисту персональних даних за українським законодавством і GDPR. *Український журнал інформаційних технологій.* 2021, т. 3, № 2. С. 51–57. URL: https://doi.org/10.23939/ujit2021.02.051.
7. Бєлов Д.М., Переш І.Є., Покорба І. Цифрові права людини: доктринальні засади. *Аналітично-порівняльне правознавство.* № 2. С. 110–116. URL: https://dspace.uzhnu.edu.ua/items/14fa9a08-4d74-43c5-9339-7b281061b730.
8. Мигаль, Р.В., Фітяк, Є.М., Кузик, Д.О. Адміністративно-правове регулювання цифровізації адміністративних процедур в Україні. Академічні візії, (33). 2024. URL https://academy-vision.org/index.php/av/article/view/1633.