

УДК 342.951:004.8:656.61:347.77/.78

DOI <https://doi.org/10.32782/2311-8040/2026-2-1>**Барабаш Ольга Олегівна,**

доктор юридичних наук, професор,

заступник директора Навчально-наукового інституту права, психології та безпекознавства;

голова Ради молодих вчених,

Львівський державний університет внутрішніх справ,

вулиця Городоцька, 26, Львів, 79000, Україна

ORCID: <https://orcid.org/0000-0003-2666-9696>

КОНЦЕПТУАЛЬНІ ЗАСАДИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ТАЄМНИЦІ ПРИ ВИКОРИСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС КВАЛІФІКАЦІЙНИХ ІСПИТІВ ЧЛЕНІВ ЕКІПАЖІВ: СТАНДАРТИ НАТО ТА ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ

Анотація. Статтю присвячено дослідженню концептуальних засад правового забезпечення професійної таємниці під час адміністративно-правового регулювання використання систем контролю на основі штучного інтелекту при проведенні кваліфікаційних іспитів членів екіпажів. Актуальність обраної тематики обумовлена цифровою трансформацією адміністративних процедур у сфері підтвердження професійної компетентності моряків, поширенням технологій «AI-proctoring», необхідністю забезпечення належного рівня захисту професійної таємниці, персональних даних та інформаційної безпеки, а також виконанням Україною міжнародних зобов'язань у процесі європейської та євроатлантичної інтеграції.

На основі аналізу законодавства України, міжнародно-правових актів, документів Європейського Союзу, НАТО, Міжнародної морської організації, практики держав – членів НАТО та сучасних доктринальних джерел здійснено критичний перегляд чинної моделі адміністративно-правового регулювання використання систем штучного інтелекту під час кваліфікаційного оцінювання членів екіпажів.

Авторкою обґрунтовано, що усталене в доктрині розуміння поняття професійної таємниці як різновиду інформації з обмеженим доступом наразі не забезпечує належного рівня правового захисту в умовах алгоритмічної обробки інформації. Доведено, що використання систем штучного інтелекту у процедурах кваліфікаційного оцінювання змінює зміст професійної таємниці, поширюючи її на алгоритмічно сформовані результати, журнали функціонування інформаційних систем, поведінкові та біометричні характеристики кандидатів, цифрові докази й інші відомості, які безпосередньо впливають на прийняття адміністративних рішень. Запропоновано авторське визначення професійної таємниці в умовах використання систем штучного інтелекту та сформульовано концепцію алгоритмічно сформованої службово-професійної інформації як самостійного об'єкта адміністративно-правової охорони.

На підставі порівняльно-правового аналізу встановлено, що нормативні моделі держав – членів НАТО ґрунтуються на принципах людиноцентричності, людського контролю, прозорості, пояснюваності алгоритмів, підзвітності, кіберстійкості та юридичної відповідальності людини за остаточне адміністративне рішення. Аргументовано доцільність імплементації зазначених стандартів у національне законодавство з урахуванням особливостей адміністративної процедури проведення кваліфікаційних іспитів членів екіпажів.

Крім того, запропоновано напрями вдосконалення адміністративно-правового регулювання, які передбачають нормативне закріплення обов'язкової алгоритмічної оцінки ризиків, незалежного аудиту систем штучного інтелекту, спеціального правового режиму алгоритмічно сформованої службово-професійної інформації, права кандидата на отримання мотивованого пояснення результатів автоматизованого оцінювання та гарантій ефективного адміністративного і судового оскарження.

Наприкінці зроблено висновок, що адаптація українського законодавства до європейських і євроатлантичних стандартів використання високоризикових систем штучного інтелекту є необхідною передумовою забезпечення законності адміністративних процедур, належного захисту професійної таємниці, зміцнення довіри до процедур підтвердження кваліфікації членів екіпажів і підвищення міжнародного авторитету української системи підготовки та сертифікації моряків.

Ключові слова: професійна таємниця, адміністративно-правове регулювання, штучний інтелект, кваліфікаційний іспит, член екіпажу, моряк, алгоритмічне прийняття рішень, персональні дані, інформаційна

безпека, кібербезпека, пояснюваність алгоритмів, людський контроль, алгоритмічний аудит, стандарти НАТО, морський транспорт.

Barabash Olha. CONCEPTUAL FOUNDATIONS OF THE LEGAL PROTECTION OF PROFESSIONAL SECRECY IN THE USE OF ARTIFICIAL INTELLIGENCE DURING CREW MEMBERS' QUALIFICATION EXAMINATIONS: NATO STANDARDS AND PROSPECTS FOR IMPLEMENTATION IN UKRAINE

Abstract. *This article examines the conceptual foundations of the legal protection of professional secrecy in the context of administrative regulation governing the use of artificial intelligence-based monitoring systems during qualification examinations for crew members. The relevance of this topic stems from the digital transformation of administrative procedures in the field of certifying seafarers' professional competence, the widespread adoption of "AI-proctoring" technologies, the need to ensure an adequate level of protection for professional secrecy, personal data, and information security, as well as Ukraine's fulfillment of its international obligations in the process of European and Euro-Atlantic integration.*

Based on an analysis of Ukrainian legislation, international legal instruments, documents of the European Union, NATO, and the International Maritime Organization, the practices of NATO member states, and contemporary doctrinal sources, a critical review of the current model of administrative and legal regulation governing the use of artificial intelligence systems during the qualification assessment of crew members has been conducted.

The author argues that the established doctrinal understanding of the concept of professional secrecy as a type of restricted-access information currently does not provide an adequate level of legal protection in the context of algorithmic information processing. It is demonstrated that the use of artificial intelligence systems in qualification assessment procedures alters the meaning of professional secrecy, extending it to algorithmically generated results, logs of information system operations, behavioral and biometric characteristics of candidates, digital evidence, and other information that directly influences administrative decision-making. The author proposes a definition of professional secrecy in the context of artificial intelligence systems and formulates the concept of algorithmically generated official and professional information as an independent object of administrative and legal protection.

Based on a comparative legal analysis, it has been established that the regulatory models of NATO member states are grounded in the principles of human-centeredness, human oversight, transparency, algorithmic explainability, accountability, cyber resilience, and human legal responsibility for the final administrative decision. The author argues for the advisability of implementing these standards into national legislation, taking into account the specific features of the administrative procedure for conducting qualification exams for crew members.

In addition, the author proposes directions for improving administrative and legal regulation, which include the normative establishment of mandatory algorithmic risk assessment, an independent audit of artificial intelligence systems, a special legal regime for algorithmically generated official and professional information, a candidate's right to receive a reasoned explanation of the results of automated assessment, and guarantees for effective administrative and judicial appeals.

The paper concludes that adapting Ukrainian legislation to European and Euro-Atlantic standards for the use of high-risk artificial intelligence systems is a necessary prerequisite for ensuring the legality of administrative procedures, adequate protection of professional secrecy, strengthening confidence in procedures for verifying the qualifications of crew members, and enhancing the international standing of the Ukrainian system for training and certifying seafarers.

Key words: *professional secrecy, administrative and legal regulation, artificial intelligence, qualification exam, crew member, seafarer, algorithmic decision-making, personal data, information security, cybersecurity, algorithmic explainability, human oversight, algorithmic audit, NATO standards, maritime transport.*

Вступ. Достатньо стрімка цифровізація публічного управління істотно змінила адміністративно-правові процедури, безпосередньо пов'язані із здійсненням державного контролю, наданням адміністративних послуг та реалізацією дозвільних функцій. Зазначені процеси привертають особливу увагу тоді, коли прийняття адміністративних рішень впливає на безпеку особи, функціонування критичної інфраструктури та виконання міжнародних

зобов'язань держави. До таких сфер, беззаперечно, належить система підтвердження професійної компетентності членів екіпажів морських суден та суден внутрішнього водного транспорту, оскільки результат кваліфікаційного оцінювання визначає можливість набуття чи підтвердження права на здійснення професійної діяльності, яка характеризується підвищеним рівнем відповідальності та міжнародної мобільності.

Останніми роками адміністративна практика багатьох держав свідчить про впровадження автоматизованих систем контролю із застосуванням технологій штучного інтелекту (далі – ШІ) під час проведення теоретичних і практичних іспитів. Власне кажучи, застосування «AI-proctoring» сьогодні перестало бути винятком для освітньої сфери та професійної сертифікації, перетворившись на один із механізмів мінімізації корупційних ризиків, протидії шахрайству, дистанційної ідентифікації кандидатів, верифікації їхньої поведінки та автоматизованої фіксації можливих порушень процедури оцінювання [1]. Одночасно із цим виникає абсолютно новий масив інформації, що формується алгоритмами машинного навчання: біометричні характеристики, поведінкові профілі, аудіовізуальні записи, результати автоматичного аналізу міміки, напрямку погляду, особливостей голосу, швидкості реакції, цифрових слідів користувача та інших параметрів, які раніше взагалі не розглядалися законодавцем як самостійний об'єкт правового регулювання.

З огляду на вищевказане, окрему увагу варто приділити питанню визначення правового режиму інформації, сформованої такими системами. У вітчизняному законодавстві України відсутня цілісна концепція, яка дозволяла б встановити співвідношення між професійною таємницею, конфіденційною інформацією, персональними даними, службовою інформацією та цифровими результатами функціонування алгоритмів ШІ. Як наслідок виникає низка адміністративно-правових ризиків, пов'язаних із доступом до відповідної інформації, порядком її зберігання, міжнародною передачею, використанням під час адміністративного чи судового оскарження результатів іспиту, а також відповідальністю суб'єктів владних повноважень за порушення режиму її охорони.

Проблематика значно ускладнюється міжнародним характером морського судноплавства. Кваліфікаційні документи українських моряків визнаються відповідно до вимог Міжнародної конвенції про підготовку і дипломування моряків та несення вахти 1978 р. [2],

тоді як цифрові технології контролю все частіше розробляються приватними транснаціональними компаніями, програмне забезпечення яких функціонує із використанням хмарних сервісів, розташованих у різних юрисдикціях. Відповідно інформація, що виникає під час кваліфікаційного оцінювання, виходить за межі виключно національного правового простору, стаючи об'єктом міжнародного інформаційного обігу.

Щоправда, наукова література переважно зосереджена на питаннях цифровізації адміністративних процедур [3], правового регулювання ШІ [4], захисту персональних даних [5] чи кібербезпеки [6]. В той же час, професійна таємниця у процедурі автоматизованого контролю під час проведення кваліфікаційних іспитів членів екіпажів практично не досліджувалася як самостійний адміністративно-правовий інститут. Не отримали належного доктринального осмислення критерії віднесення результатів алгоритмічного аналізу до професійної таємниці, адміністративно-правовий статус суб'єктів, які здійснюють обробку відповідної інформації, правова природа автоматично сформованих висновків систем ШІ, а також їх співвідношення із принципами законності, пропорційності, належного врядування, інформаційної безпеки та права на справедливу адміністративну процедуру.

Доволі прикметно, що після набуття Україною статусу держави-кандидата на вступ до ЄС та поглиблення співробітництва з НАТО питання нормативного забезпечення використання систем ШІ вже не може оцінюватися виключно крізь призму внутрішнього законодавства. Регламент (ЄС) 2024/1689 про ШІ («AI Act» [7]), Загальний регламент про захист даних [8], Конвенція Ради Європи №108+ [9], Директива (ЄС) 2022/2555 (NIS2) [10] та низка стандартів Альянсу у сфері інформаційної безпеки формують нову нормативну парадигму, у межах якої будь-які системи автоматизованого контролю мають відповідати вимогам пояснюваності алгоритмів, підзвітності, людського контролю, кіберстійкості та захисту фундаментальних прав людини. Отож імплементація зазначених стандартів повинна супроводжува-

тися критичним переосмисленням вже існуючих адміністративно-правових конструкцій.

Науковий інтерес до окресленої проблематики визначається також відсутністю у вітчизняній юридичній доктрині єдиного розуміння професійної таємниці в умовах функціонування алгоритмічних систем прийняття рішень. На переконання автора, професійна таємниця під час проведення кваліфікаційних іспитів із використанням систем ІІІ має розглядатися не як сукупність окремих відомостей, доступ до яких обмежується законом, а як самостійний адміністративно-правовий режим інформації, що виникає у процесі автоматизованої реалізації владних повноважень, містить результати інтелектуального аналізу поведінки кандидата та потребує спеціального порядку збирання, використання, передачі, зберігання, аудиту і судового контролю. Власне перевірка даної наукової гіпотези визначає загальну концепцію пропонованого дослідження.

Метою статті є формування концептуальних засад адміністративно-правового забезпечення професійної таємниці під час використання систем контролю на основі ІІІ при проведенні кваліфікаційних іспитів членів екіпажів шляхом переосмислення існуючих доктринальних конструкцій, дослідження національного та міжнародного нормативного регулювання, правових стандартів ЄС і НАТО, визначення юридичної природи інформації, що формується алгоритмами ІІІ, обґрунтування її самостійного адміністративно-правового режиму, а також розроблення пропозицій щодо вдосконалення законодавства України.

Матеріали та методи. При цьому науковий пошук не обмежується аналізом чинних нормативних приписів, а спрямовується на виявлення закономірностей зміни адміністративно-правових відносин під впливом алгоритмічних технологій, оцінку достатності існуючих юридичних гарантій охорони професійної таємниці та вироблення критеріїв, за якими результати функціонування систем ІІІ можуть бути віднесені до інформації з обмеженим доступом. Окрему увагу приділено встановленню меж дискреційних повноважень суб'єктів владних повноважень при використанні авто-

матизованих систем контролю, визначенню співвідношення людського контролю та алгоритмічного оцінювання, а також формуванню пропозицій щодо нормативного закріплення процедур алгоритмічного аудиту, пояснюваності рішень ІІІ та адміністративно-правових гарантій судового захисту осіб, стосовно яких такі системи застосовуються.

Однак досягнення окресленої мети неможливе без з'ясування ступеня наукового опрацювання відповідної проблематики, оскільки адміністративно-правове регулювання використання систем ІІІ у процедурах кваліфікаційного оцінювання членів екіпажів перебуває на перетині кількох самостійних напрямів юридичної науки: доктрини професійної таємниці, адміністративного права, інформаційного права, права ЄС, міжнародного морського права, правового регулювання ІІІ та кібербезпеки. Беручи до уваги зазначене, слід звернутися до аналізу останніх досліджень і публікацій, у яких започатковано вирішення окремих аспектів порушеної проблеми, визначити напрями наукової дискусії, оцінити ступінь їх теоретичної розробленості та окреслити ті питання, що залишаються недостатньо дослідженими й потребують подальшого доктринального вивчення.

Результати. Окремі аспекти цифровізації публічного адміністрування та її впливу на реалізацію адміністративних процедур досліджували А. Краковська та М. Баби́к, які акцентували увагу на трансформації механізмів надання адміністративних послуг, в той же час залишивши поза науковою увагою питання використання систем ІІІ під час кваліфікаційного оцінювання осіб. Значний внесок у розвиток доктрини правового регулювання ІІІ зробила О. Кожухар, яка обґрунтувала визначальне значення принципу прозорості алгоритмічних систем для забезпечення законності адміністративної діяльності, проте специфіка захисту професійної таємниці у процедурах автоматизованого контролю предметом її дослідження не була.

Теоретичні засади права на приватність ґрунтовно висвітлено у працях О. Панкевича, який розглядає приватність як самостійну

сферу автономії особи, що потребує належних юридичних гарантій у процесі обробки інформації. Своєю чергою, М. Менджул та О. Мулеса дослідили окремі питання забезпечення кібербезпеки під час цифрової взаємодії суб'єктів публічного управління, звернувши увагу на нові виклики інформаційної безпеки в умовах воєнного стану.

Міжнародно-правові аспекти доступу систем ІІІ до професійної таємниці проаналізовано у праці Т. Пашука, де обґрунтовано потребу встановлення спеціальних правових обмежень щодо використання алгоритмів під час обробки конфіденційної професійної інформації. Водночас Д. Кертін та Т. Фіа, досліджуючи проблему алгоритмічної закритості діяльності публічної адміністрації Європейського Союзу, звернули увагу на ризики надмірної секретності функціонування систем ІІІ, яка істотно ускладнює реалізацію принципів прозорості, підзвітності та ефективного контролю за адміністративними рішеннями.

Беручи до уваги вищенаведені наукові напрацювання, слідє констатувати, що питання адміністративно-правового забезпечення професійної таємниці під час використання систем контролю на основі ІІІ при проведенні кваліфікаційних іспитів членів екіпажів, з урахуванням стандартів НАТО, міжнародних вимог до підготовки моряків та особливостей адміністративної процедури підтвердження кваліфікації, дотепер не отримало самостійного концептуального дослідження. Зокрема, поза належною увагою залишаються правова природа алгоритмічно сформованої інформації, межі поширення режиму професійної таємниці на результати функціонування систем ІІІ, а також засади імплементації міжнародних стандартів у національне адміністративне законодавство, що й зумовлює актуальність та наукову новизну цієї статті.

Правове регулювання професійної таємниці традиційно розвивалося як інститут, покликаний забезпечити баланс між публічним інтересом держави у належному функціонуванні окремих сфер професійної діяльності та приватним інтересом особи щодо нерозголошення відомостей, доступ до яких обумовлений ви-

конанням професійних обов'язків. Історично відповідна категорія формувалася крізь призму медичної, адвокатської, нотаріальної, банківської, аудиторської та інших різновидів професійної таємниці, для яких характерною була наявність спеціального суб'єкта, нормативно визначеного предмета охорони та юридичного обов'язку щодо нерозголошення отриманої інформації. Проте цифровізація адміністративних процедур та активне використання систем ІІІ засвідчили, що усталене в доктрині розуміння професійної таємниці більше не відображає реального змісту інформаційних відносин, які виникають між суб'єктами владних повноважень, розробниками програмного забезпечення, адміністраторами інформаційно-комунікаційних систем та особами, щодо яких здійснюються автоматизовані контрольні процедури.

З огляду на вищенаведене, привертає увагу одна обставина, яка тривалий час залишалася поза межами наукової дискусії. Зокрема, переважна більшість законодавчих конструкцій виходить із презумпції, що *інформація створюється людиною, накопичується людиною та використовується людиною*. Проте сучасні системи контролю із застосуванням ІІІ генерують якісно новий різновид інформації, який виникає без безпосереднього волевиявлення посадової особи. Алгоритми машинного навчання здійснюють оцінювання поведінкових характеристик кандидата, аналізують рухи очей, тембр голосу, тривалість концентрації уваги, зміну освітлення приміщення, цифрову активність користувача, швидкість виконання тестових завдань та десятки інших параметрів, результатом чого стає формування висновку про наявність чи відсутність ознак порушення процедури складання кваліфікаційного іспиту. Дана інформація має істотне юридичне значення, оскільки безпосередньо впливає на прийняття адміністративного рішення про видачу, відмову у видачі або підтвердження кваліфікаційного документа.

У зазначеному аспекті виникає питання, яке, гадаємо, ще не отримало належного доктринального опрацювання: чи можна результати алгоритмічного аналізу вважати різно-

видом професійної таємниці, якщо вони не були сформовані людиною, проте використовуються суб'єктом владних повноважень під час реалізації адміністративної компетенції? Власне кажучи, традиційні критерії професійної таємниці, що ґрунтуються виключно на професійному статусі носія інформації, вже не дозволяють надати переконливу відповідь. Натомість цифрове середовище демонструє іншу модель інформаційного обігу, в якій суб'єкт владних повноважень виконує функцію адміністратора інформації, а її первинним «автором» стає програмний алгоритм.

Конституція України від 28.06.1996 р. №254к/96-ВР, закріплюючи у ст. 32 гарантії невтручання в особисте і сімейне життя та заборону збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди [11], фактично встановлює імперативну конституційну вимогу захисту інформаційної приватності. Проте наведена норма була прийнята тоді, коли цифрові технології ще не здійснювали самостійного аналізу поведінки людини. Вочевидь тому буквально тлумачення конституційних приписів сьогодні не забезпечує належного правового регулювання випадків, за яких автоматизовані системи формують нові інформаційні масиви, які раніше взагалі не існували як об'єкт юридичної охорони.

Аналогічні висновки впливають із положень Закону України «Про інформацію» від 02.10.1992 р. №2657-ХІІ [12]. Законодавець класифікує інформацію залежно від режиму доступу, визначаючи відкриту інформацію та інформацію з обмеженим доступом, до якої належать конфіденційна, таємна і службова інформація. Разом із тим Закон не містить критеріїв віднесення до конфіденційної інформації результатів автоматизованого поведінкового аналізу особи, здійсненого системами ШІ. Втім, відсутність відповідної регламентації не можна розглядати як випадкову законодавчу прогалину, оскільки на момент прийняття зазначеного нормативного акта технології «AI-proctoring» фактично не використовувалися в адміністративній діяльності. А отже, сформовані законодавцем класифікаційні критерії вже

не відповідають сучасному стану цифрових правовідносин.

Не менш показовим є зміст Закону України «Про захист персональних даних» від 01.06.2010 р. №2297-VI [13]. Закон визначає персональні дані як «...відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» (абз. 8 ст. 2 Закону). Водночас алгоритмічний аналіз поведінки кандидата під час складання кваліфікаційного іспиту очевидно виходить за межі усталеного розуміння персональних даних. Система ШІ не обмежується встановленням особи кандидата, а здійснює оцінювання його поведінкових патернів, прогнозує можливі ризики недоброчесної поведінки, визначає статистичні відхилення від типової моделі проходження тестування та формує інтегральний цифровий профіль.

Для дослідження заявленої проблематики варто звернутися до права ЄС. Вищезгаданий Загальний регламент про захист даних, запровадивши категорію профайлінгу та автоматизованого прийняття рішень, фактично визнав, що алгоритмічно сформована інформація може суттєво впливати на права людини. Важливе значення має ст. 22 GDPR, яка гарантує особі право не бути об'єктом рішення, що ґрунтується винятково на автоматизованій обробці, якщо таке рішення породжує юридичні наслідки або іншим чином істотно впливає на її права чи законні інтереси [8]. Вважаємо, саме ця конструкція має стати відправною точкою для формування української моделі адміністративно-правового забезпечення професійної таємниці у процедурах кваліфікаційного оцінювання членів екіпажів.

Ще більшої актуальності зазначене питання набуло після набрання чинності Регламентом (ЄС) 2024/1689 про ШІ [7]. Законодавець ЄС вперше запропонував ризик-орієнтовану модель правового регулювання систем ШІ, віднісши окремі системи оцінювання осіб до категорії високого ризику. Прикметно, що правове значення у даному випадку має вже не характер інформації як такої, а можливість алгоритму впливати на реалізацію прав людини, доступ до професії та здійснення еконо-

мічної діяльності. Отож професійна таємниця у сфері AI-контролю повинна оцінюватися крізь призму потенційних юридичних наслідків використання алгоритмічно сформованої інформації, а не виключно через критерій її конфіденційності.

Припустимо, що під час дистанційного складання кваліфікаційного іспиту моряком система «AI-proctoring» зафіксувала багаторазове відведення погляду від монітора, після чого автоматично сформувала повідомлення про високий рівень ймовірності використання сторонньої допомоги. На підставі такого повідомлення екзаменаційна комісія ухвалює рішення про припинення іспиту та відмову у видачі кваліфікаційного документа. Під час судового оскарження кандидат вимагає надати технічні параметри функціонування алгоритму, дані машинного навчання, критерії оцінювання ризику та математичну модель, відповідно до якої система сформувала негативний висновок. Адміністратор інформаційної системи відмовляє, посилаючись на комерційну таємницю розробника програмного забезпечення. Відповідно виникає конфлікт між правом особи на ефективний судовий захист, необхідністю забезпечення прозорості адміністративної процедури, охороною інтелектуальної власності розробника та обов'язком держави гарантувати конфіденційність інформації, отриманої під час кваліфікаційного оцінювання.

Саме з огляду на зазначене є підстави підтримати наукову позицію, відповідно до якої професійна таємниця в умовах використання систем ШІ має розглядатися значно ширше, ніж традиційний інститут інформації з обмеженим доступом [див. 14; 15]. На нашу думку, **професійною таємницею** у сфері проведення кваліфікаційних іспитів членів екіпажів слід розуміти встановлений адміністративним законодавством правовий режим інформації, яка формується, накопичується, аналізується або використовується суб'єктами владних повноважень та автоматизованими системами контролю під час реалізації адміністративної процедури підтвердження професійної компетентності, розголошення чи неправомірне

використання якої здатне вплинути на права особи, безпеку судноплавства, довіру до результатів кваліфікаційного оцінювання чи виконання міжнародних зобов'язань України.

Не менш важливо, що додаткові гарантії встановлює модернізована Конвенція Ради Європи №108+, яка вперше закріпила принципи *пропорційності*, мінімізації обсягу оброблюваних даних, прозорості алгоритмічної обробки та відповідальності контролера даних. В порівнянні з окремими національними моделями, Конвенція поширює відповідні вимоги незалежно від місця фізичного розташування серверів чи інформаційної системи [9]. Вбачається, окреслений підхід має вагоме значення і для України, адже більшість комерційних платформ «AI-proctoring» використовує хмарні дата-центри, розміщені за межами держави.

У сфері кібербезпеки визначальне місце посідає Директива (ЄС) 2022/2555 (NIS2), яка значно посилила вимоги до управління кіберризиками, реагування на інциденти та захисту цифрової інфраструктури [10]. Так, хоча вона безпосередньо не регулює проведення кваліфікаційних іспитів, її положення формують єдиний стандарт захисту інформаційних систем, що використовуються суб'єктами публічної влади. Для України, своєю чергою, імплементація підходів NIS2 – це беззаперечна потреба законодавчого закріплення обов'язкового аудиту інформаційної безпеки платформ «AI-proctoring», періодичного тестування їхньої стійкості до кібератак та визначення адміністративної відповідальності операторів за неналежний рівень кіберзахисту.

Вагомий науковий інтерес становить нормативна політика НАТО щодо використання ШІ. Зокрема, у NATO Artificial Intelligence Strategy 2021 р. Альянс визначив, що застосування ШІ повинно відповідати принципам законності, відповідальності, пояснюваності, надійності, можливості відстеження функціонування алгоритмів та керованості людиною [16]. Подальший розвиток ці положення отримали у документі NATO Responsible Use of Artificial Intelligence, схваленому у 2024 році, де державам рекомендовано забезпечити постійний людський контроль за функціонуванням ви-

сокоризикових AI-систем, здійснювати незалежний аудит алгоритмів, гарантувати їхню кіберстійкість та запобігати алгоритмічній дискримінації [17]. При цьому, незважаючи на військову спрямованість зазначених документів, сформульовані принципи мають універсальний характер і можуть бути застосовані до адміністративних процедур професійної сертифікації. Передусім це стосується обов'язку пояснюваності алгоритмів, адже кандидат повинен мати можливість зрозуміти, з яких причин система сформувала негативний висновок.

З точки зору практики, варто звернути увагу на положення NATO Digital Transformation Implementation Strategy, відповідно до якої цифрові системи, що використовуються органами державної влади, повинні відповідати принципам «...interoperability, cyber resilience, secure-by-design, data governance...» [18]. У контексті проведення кваліфікаційних іспитів членів екіпажів зазначені положення означають потребу нормативного закріплення вимог до захищеного обміну інформацією між Морською адміністрацією, державними реєстрами, інформаційними системами підготовки моряків та міжнародними базами даних. До слова, українське законодавство наразі не встановлює спеціальних критеріїв сертифікації програмного забезпечення, що використовується під час автоматизованого оцінювання кандидатів, тоді як підходи НАТО виходять із необхідності попередньої перевірки цифрових платформ на відповідність визначеним вимогам безпеки.

Досвід держав – членів НАТО підтверджує, що нормативне регулювання «AI-proctoring» формується за єдиною концепцією, хоча способи її реалізації різняться. Так, у Великій Британії Office of Qualifications and Examinations Regulation після пандемії COVID-19 сформував окремий напрям правового регулювання дистанційного контролю за перебігом кваліфікаційних іспитів, а згодом оприлюднив політику щодо використання ШІ у сфері кваліфікацій. Регулятор виходить із необхідності забезпечення справедливості оцінювання, пропорційного використання ШІ, обов'язкового людського контролю за висо-

коризиковими процедурами та недопустимості використання ШІ як єдиного механізму ухвалення рішень щодо результатів кандидатів [19; 20]. Очевидно, дана модель заслуговує на підтримку, оскільки мінімізує ризик помилкових рішень, спричинених технічними помилками чи недосконалістю алгоритмів.

У Нідерландах питання використання систем автоматизованого прокторингу (автоматизованого спостереження та контролю за дотриманням встановленої процедури під час дистанційного складання іспитів) стало актуальним після судових спорів, пов'язаних із використанням програмного забезпечення «Proctorio» у закладах вищої освіти. Національний орган із захисту персональних даних (Autoriteit Persoonsgegevens), а також нідерландська судова практика акцентували увагу на потребі дотримання принципу пропорційності під час втручання у приватне життя, проведення попередньої оцінки впливу на захист персональних даних відповідно до ст. 35 GDPR [8] та належного обґрунтування неможливості застосування менш інтенсивних засобів контролю. За відсутності такого обґрунтування використання автоматизованих систем прокторингу може розглядатися як *непропорційне обмеження права на повагу до приватного життя* [21]. Думається, саме критерій **пропорційності** повинен стати обов'язковою складовою адміністративної процедури запровадження AI-контролю в Україні.

Норвегія та Данія, які активно цифровізують публічне управління, використовують дещо іншу модель [22, 23]. Замість максимальної автоматизації вони зберігають вирішальну роль екзаменатора, тоді як ШІ виконує допоміжну функцію з аналізу потенційних ризиків. Вочевидь, практика названих країн відповідає принципам НАТО щодо «human oversight» і видається більш прийнятною для адміністративно-правової системи України, ніж моделі повністю автоматизованого прийняття рішень.

Свою чергою, у Сполучених Штатах Америки нормативне регулювання здійснюється переважно на рівні окремих штатів, федеральних рекомендацій та технічних стандартів, що

обумовлює певну децентралізацію відповідної правової політики. Водночас NIST AI Risk Management Framework сформував універсальну модель управління ризиками, засновану на принципах пояснюваності, достовірності, безпечності та підзвітності алгоритмів [24; 25]. Втім, незважаючи на відсутність спеціального федерального закону про ШІ, американська модель привертає увагу насамперед розвитком процедур незалежного аудиту алгоритмів, що доцільно використати під час вдосконалення положень українського законодавства.

Висновки. Підсумовуючи викладене, слід констатувати, що жодна з розглянутих іноземних моделей не допускає використання систем ШІ як повністю автономного суб'єкта прийняття адміністративного рішення. У центрі європейської та євроатлантичної нормативної парадигми перебуває *людина*, тоді як алгоритм розглядається винятково як інструмент підтримки управлінської діяльності. Власне ця концепція, на нашу думку, пови-

нна бути покладена в основу майбутнього адміністративно-правового регулювання використання систем контролю на основі ШІ під час проведення кваліфікаційних іспитів членів екіпажів в Україні. Більш того, її імплементація має передбачати законодавче визначення правового статусу «AI-proctoring», обов'язковості алгоритмічного аудиту, нормативне закріплення права кандидата на отримання мотивованого пояснення результатів автоматизованого оцінювання, проведення оцінки впливу на права людини до введення відповідної системи в експлуатацію, а також спеціальний режим охорони професійної таємниці щодо інформації, сформованої алгоритмами ШІ. Вважаємо, що тільки за таких умов можливо досягти належного балансу між інтересами держави у забезпеченні об'єктивності кваліфікаційного оцінювання, міжнародними зобов'язаннями України та гарантіями захисту основоположних прав людини.

Список використаних джерел

1. Lareo X. Automated proctoring. *European Data Protection Supervisor*. URL: <https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/automated-proctoring>
2. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers of 1978. URL: <https://www.imo.org/en/ourwork/humanelement/pages/stcw-convention.aspx>
3. Краковська А., Бабик М. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського Національного Університету*. Серія: Право. 2022. Вип. 70. С. 329–334. DOI: <https://doi.org/10.24144/2307-3322.2022.70.52>
4. Кожухар О. Принцип прозорості в контексті правового регулювання систем штучного інтелекту. *Наукові записки НаУКМА*. 2025. Серія: Юридичні науки. Т. 15. С. 78–85. DOI: <https://doi.org/10.18523/2617-2607.2025.15.78-85>
5. Панкевич О.З. Право на приватність: царица незалежності особи. *Науковий вісник Львівського державного університету внутрішніх справ*. Серія юридична. 2017. Вип. 2. С. 47–56. <http://dspace.lvduvs.edu.ua/handle/1234567890/1761>
6. Менджул М., Мулеса О. Проблеми гарантування кібербезпеки у процесі транскордонного співробітництва під час воєнного стану. *Кібербезпека в транскордонному співробітництві*. Наукове видання (Збірник тез доповідей) Закарпатського угорського інституту імені Ференца Ракоці II / Редактори: Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Ганна Мелегачич та Оксана Мулеса. Берегове: ЗУІ ім. Ференца Ракоці II, 2024. (українською, англійською та угорською мовами). С. 35–37. <https://dspace.kme.org.ua/items/f7d61419-1539-45fe-a1e9-fde130074868>
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

9. Convention 108+. Convention for the protection of individuals with regard to the processing of personal data of 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
11. Конституція України від 28.06.1996 №254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
12. Про інформацію: Закон України від 02.10.1992 №2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
13. Про захист персональних даних: Закон України від 01.06.2010 №2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
14. Pashchuk T. Regulatory limits on Artificial Intelligence access to professional secrets in the digital age: an international legal perspective. *Legal, Economic Science and Praxis*. 2025. №16. P. 11-18. https://lesp.hu/wp-content/uploads/2026/02/2-Taras-Pashchuk_16_2025_p-11-18.pdf
15. Curtin D., Fia T. Cracking AI secrecy: (beyond) EU migration law and governance. *European Law Open*. 2026. P. 1-30. DOI: <https://doi.org/10.1017/elo.2025.10064>
16. Summary of the NATO Artificial Intelligence Strategy. NATO. 2021. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy>
17. Summary of NATO's revised Artificial Intelligence (AI) strategy. NATO. 2024. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
18. NATO's Digital Transformation Implementation Strategy 2.0. NATO. 2026. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy>
19. Remote invigilation in vocational and technical qualifications. 2023. URL: <https://www.gov.uk/government/publications/remote-invigilation-in-vocational-and-technical-qualifications>
20. Ofqual's approach to regulating the use of artificial intelligence in the qualifications sector. 2024. URL: <https://www.gov.uk/government/publications/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector>
21. Data protection impact assessment (DPIA). Autoriteit Persoonsgegevens. URL: <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia>
22. The National Strategy for Artificial Intelligence. 2020. URL: <https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/>
23. Danish strategies for artificial intelligence. URL: <https://en.digst.dk/digital-governance/new-technologies/danish-strategies-for-artificial-intelligence/>
24. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST. 2023. URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>
25. AI Risk Management Framework. NIST. 2026. URL: <https://www.nist.gov/itl/ai-risk-management-framework>

References:

1. Lareo X. Automated proctoring. European Data Protection Supervisor. URL: <https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/automated-proctoring> [In English].
2. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers of 1978. URL: <https://www.imo.org/en/ourwork/humanelement/pages/stcw-convention.aspx> [In English].
3. Krakovska A., Babyk M. (2022). Tsyfrovizatsiia administratyvnykh posluh v Ukraini: problemy ta perspektyvy rozvytku [Digitalization of administrative services in Ukraine: challenges and development prospects]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriya: Pravo (Scientific Bulletin of Uzhhorod National University. Series: Law)*. Vyp. 70. S. 329–334. DOI: <https://doi.org/10.24144/2307-3322.2022.70.52> [In Ukrainian].
4. Kozhukhar O. (2025). Pryntsyp prozorosti v konteksti pravovoho rehuliuвання system shtuchnoho intelektu [The Principle of Transparency in the Context of the Legal Regulation of Artificial Intelligence Sys-

tems]. Naukovi zapysky NaUKMA . Serii: Yurydychni nauky (NaUKMA Research Papers. Legal Sciences Series). T. 15. S. 78–85. DOI: <https://doi.org/10.18523/2617-2607.2025.15.78-85> [In Ukrainian].

5. Pankevych O.Z. (2017). Pravo na pryvatnist: tsaryna nezalezhnosti osoby [The Right to Privacy: The Realm of Personal Independence]. Naukovyi visnyk Lvivskoho derzhavnogo universytetu vnutrishnikh sprav. Serii: yurydychna (Scientific Bulletin of Lviv State University of Internal Affairs. Legal Series). Vyp. 2. S. 47–56. <http://dspace.lvduvs.edu.ua/handle/1234567890/1761> [In Ukrainian].

6. Mendzhul M., Mulesa O. (2024). Problemy harantuvannya kiberbezpeky u protsesi transkordonnoho spivrobitnytstva pid chas voiennoho stanu [Challenges of Ensuring Cybersecurity in Cross-Border Cooperation under Martial Law. Cybersecurity in Cross-Border Cooperation. Scientific Publication (Collection of Abstracts) Ferenc Rákóczi II Transcarpathian Hungarian Institute]. Kiberbezpeka v transkordonnomu spivrobitnytstvi. Naukove vydannia (Zbirnyk tez dopovidei)

Zakarpatskoho uhorskoho instytutu imeni Ferentsa Rakotsi II (Cybersecurity in Cross-Border Cooperation. Scientific Publication (Collection of Abstracts) Ferenc Rákóczi II Transcarpathian Hungarian Institute)/ Redaktery: Stepan Chernychko, Marianna Marusynets, Yelyzaveta Molnar D, Hanna Melehanych ta Oksana Mulesa. Berehove: ZUI im. Ferentsa Rakotsi II. (ukrainskoiiu, anhliiskoiu ta uhorskoiiu movamy). S. 35–37. <https://dspace.kme.org.ua/items/f7d61419-1539-45fe-a1e9-fde130074868> [In Ukrainian, English, Hungarian].

7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> [In English].

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> [In English].

9. Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data of 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf [In English].

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> [In English].

11. Konstytutsiia Ukrainy [Constitution of Ukraine] vid 28.06.1996 №254k/96-VR. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> [In Ukrainian].

12. Pro informatsiiu: Zakon Ukrainy [On Information: Law of Ukraine] vid 02.10.1992 №2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> [In Ukrainian].

13. Pro zakhyst personalnykh danykh: Zakon Ukrainy [On Personal Data Protection: Law of Ukraine] vid 01.06.2010 №2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [In Ukrainian].

14. Pashchuk T. Regulatory limits on Artificial Intelligence access to professional secrets in the digital age: an international legal perspective. Legal, Economic Science and Praxis. 2025. № 16. P. 11–18. https://lesp.hu/wp-content/uploads/2026/02/2-Taras-Pashchuk_16_2025_p-11-18.pdf [In English].

15. Curtin D., Fia T. (2026). Cracking AI secrecy: (beyond) EU migration law and governance. *European Law Open*. P. 1–30. DOI: <https://doi.org/10.1017/elo.2025.10064> [In English].

16. Summary of the NATO Artificial Intelligence Strategy. NATO. 2021. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy> [In English].

17. Summary of NATO's revised Artificial Intelligence (AI) strategy. NATO. 2024. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy> [In English].

18. NATO's Digital Transformation Implementation Strategy 2.0. NATO. 2026. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy> [In English].

19. Remote invigilation in vocational and technical qualifications. 2023. URL: <https://www.gov.uk/government/publications/remote-invigilation-in-vocational-and-technical-qualifications> [In English].

20. Ofqual's approach to regulating the use of artificial intelligence in the qualifications sector. 2024. URL: <https://www.gov.uk/government/publications/ofqual-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector> [In English].
21. Data protection impact assessment (DPIA). Autoriteit Persoonsgegevens. URL: <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia> [In English].
22. The National Strategy for Artificial Intelligence. 2020. URL: <https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/> [In English].
23. Danish strategies for artificial intelligence. URL: <https://en.digst.dk/digital-governance/new-technologies/danish-strategies-for-artificial-intelligence/> [In English].
24. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST. 2023. URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf> [In English].
25. AI Risk Management Framework. NIST. 2026. URL: <https://www.nist.gov/itl/ai-risk-management-framework> [In English].

Creative Commons Attribution 4.0
International (CC BY 4.0)



Дата першого надходження статті до видання: 31.07.2026
Дата прийняття статті до друку після рецензування: 03.09.2026
Дата публікації (оприлюднення) статті: 00.00.2026