УДК 342
DOI https://doi.org/10.32782/2524-0374/2021-11/135

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В СМАРТ СІТІ

LEGAL REGULATION OF USING ARTIFICIAL INTELLIGENCE SYSTEMS IN A SMART CITY

Тимошенко Є.А., асистентка кафедри права
Вінницький національний аграрний університет

Долян І.В., студент ІІ курсу юридичного факультету
Вінницький національний аграрний університет

У статті досліджено практичний та теоретичний досвід правового регулювання систем штучного інтелекту в «смарт сіті». Дослідження проведено загальнонауковими методами, такими як аналіз, синтез та спостереження, а також аналогія. Розкрито питання легальності втручання в особисте життя громадян за допомогою вуличних камер відеоспостереження, переваги та недоліки цих систем. Розмежовано поняття біометричних та персональних даних на прикладі законодавства України та ЄС.

Розглянуто роботу Ситуаційного центру в м. Вінниця, а також роботу закордонної системи виявлення вогнепального пострілу задля захисту громадян. Технології розпізнавання обличчя, пошук особи в натовпі є надзвичайно цінними для правоохоронних органів та суспільства загалом. Зосереджено увагу на тому, яку інформацію потрібно збирати в потрібному місці та в потрібний час, хто повинен мати повноваження на доступ до неї. Після отримання доступу також важливо правильно обробляти й використовувати ці дані в подальшому. Для цього повинно бути законодавче обґрунтування та регулювання використання штучного інтелекту в системах безпечного міста.

Багато законодавчих актів ще не можуть регулювати дії ШІ, оскільки вважаються застарілими. Для того щоб ці програми працювали на повністю законних підставах, їм потрібно пройти багато тестів щодо перевірки точності роботи.

Метою статті є аналіз теоретичних досліджень та наявного практичного досвіду правового регулювання систем штучного інтелекту в розумному місті в контексті розвитку та формування інформаційного суспільства.

Проаналізовано нормативну базу ЄС та України щодо використання штучного інтелекту для збирання та ідентифікації персональних даних. Знайдено правові колізії в українському законодавстві щодо персональних та біометричних даних. Досліджено нові умови безпечного та етичного використання ШІ від 21 квітня 2021 року, які прийняла Єврокомісія. В них запропоновано критерії оцінювання ризиків використання технологій ШІ, які поділяються на високий, низький, обмежений та мінімальний ризики.

Ключові слова: інформаційне суспільство, біометричні дані, персональні дані, відеоспостереження, інформація, захист.

The scientific article examines the practical and theoretical experience of legal regulation of artificial intelligence systems in “Smart City”. The research was conducted by general scientific methods, such as analysis, synthesis and observation, as well as analogy. The issue of legality in the use of citizens’ private lives with the help of street video surveillance cameras, the advantages and disadvantages of these systems are revealed. The article distinguishes between the concepts of biometric and personal data from the examples of Ukrainian and EU legislation.

The work of the Situation Center in Vinnytsia, as well as the work of a foreign fire detection system to protect citizens. Face recognition technology, finding a person in the crowd are extremely valuable for law enforcement agencies and for society as a whole. The focus is on what information needs to be selected in the right place and at the right time, and who should have the authority to access it. Once you have access, it is also important to properly handle and use these sites in the future. To do this, there must be a legal justification and regulation of the use of artificial intelligence in safe city systems.

Many pieces of legislation that do not yet regulate AI actions are becoming obsolete. In order for the programs to work on a completely legal basis, it needs to pass many more tests to verify the correct operation.

The purpose of the article is to analyze theoretical research and existing practical experience of legal regulation of artificial intelligence systems in a smart city in the context of development and formation of the information society.

The regulatory framework of the EU and Ukraine on the use of artificial intelligence for the collection and identification of personal data is analyzed. Legal conflicts were found in the Ukrainian legislation on personal and biometric data. The new conditions for safe and ethical use of AI from April 21, 2021, which were adopted by the European Commission, have been studied. They propose criteria for assessing the risks of using AI technologies, which are divided into high, low, limited and minimal risks.

Key words: information society, biometric data, personal data, video surveillance, information, protection.

Розумне місто – яке воно? Місто, в якому гармонійно поєднано інтереси громадян, бізнесу та влади завдяки використанню сучасних новітніх технологій та різноманітних розумних рішень задля вирішення нагальних проблем [6]. Це місто, у якого в пріоритеті громадська безпека його мешканців. Все повинно починатися зі встановлення безпечних меж, і ці межі може сьогодні встановити штучний інтелект. ШІ – це єдиний інструмент у XXI столітті, який може створити безпечний щит для кожного. Він здатний забезпечити захист за всіма критеріями, які не під силу контролювати звичайній людині, та виконувати ті речі, в яких вона помилятиметься або які не зможе встигати контролювати. В розумному місті штучний інтелект – це синонім до слів «безпека» та «захист». ШІ можна використовувати як інструмент безпеки, який дає змогу містам вдосконалювати свої послуги та розширювати інфраструктуру, використовуючи інтелектуальні технології.

Інтелектуальні системи збирають та аналізують інформацію про громадську безпеку та блискавично й ефективно реагують на події в режимі реального часу. Саме ШІ може передбачати підозрілі та зловмисні дії, що можуть статися в межах його доступу, та запобігати ним. Завдяки надточному механізму розпізнавання обличь, навіть замаскованих, автомобільних номерів, траєкторії руху автомобіля можна передбачити злочин та запобігти йому. Нині ця технологія могла б вирішити багато питань порушення правил безпеки. Наприклад, якщо автомобіль рухається з перевищенням швидкості, то ШІ зможе не просто зафіксувати швидкість авто, але й швидко вивести всю інформацію на екран щодо поточного об’єкта. Таке, здавалось би, може зробити уповноважена на це особа, проте уявіть, скільки часу знадобиться людині, щоб виписати штраф порушникові і відправити його їй. З цією справою ШІ може впоратися в рази швидше, а також паралельно зафіксовувати швидкість інших автомобілів на дорозі. Щодо цього можна сказати, що така система не лише здатна фіксувати порушення учасників дорожнього руху, але й визначати і відправляти штрафи водіям, які здійснили якесь

правопорушення. На цьому одному з небагатьох випадків можна побачити, що завдяки такій системі ШІ робота звичайних людей стане однозначно легшою, хоча збій у програмі також допустимий, тому людська праця завжди буде актуальною, все одно хтось повинен слідкувати за чіткою роботою ШІ, а разі некоректної роботи – виправити інформацію або виконати певні дії щодо конкретної ситуації. Це лише один з небагатьох прикладів, який можна привести щодо позитивних аспектів ШІ.

При цьому важливо зосередитись на тому, яку інформацію потрібно збирати в потрібному місці та в потрібний час, хто повинен мати повноваження на доступ до неї. Після отримання доступу також важливо правильно обробляти і використовувати ці дані в подальшому. Для цього повинно бути законодавче обґрунтування та регулювання використання штучного інтелекту в системах безпечного міста.

Штучний інтелект та машинне навчання вже досягли того рівня, щоб використовуватись у сфері національної безпеки та розвідувальної діяльності. Першими в цьому напрямі почали працювати США та Китай, які інтегрували велику кількість розробок на базу штучного інтелекту в державні апарати та побут своїх громадян. ІТ-компанії цих країн пропонують свої розробки іншим країнам задля забезпечення порядку та безпеки населення. Наприклад, "Huawei" пропонує свої технології «Безпечне місто» третині населення по всьому світі, але штучний інтелект можна створити поза великими компаніями, і він матиме не меншу ефективність.

Дуже відомий та ефективний стартап для розумних міст "Shotspotter" використовує складну технологію штучного інтелекту, що складається з датчиків для виявлення насильства з використанням зброї. Це попереджує відділ поліції та інші органи влади протягом 60 секунд після пострілу. Застосована технологія штучного інтелекту та машинного навчання дає змогу з'ясувати точне місце пострілу та викликати поліцію на місце інциденту. За даними Міністерства внутрішньої безпеки США, середня тривалість стрільби у школах та університетах складає 12,5 хвилин, а відповідь правоохоронних органів – 18 хвилин, тобто нескладно помітити, що реагування поліції повільне і недостатньо ефективне. Разом з технологією "Shotspotter" не потрібно телефонувати в поліцію, говорити адресу, пояснювати ситуацію, яка склалась, адже ШІ сам визначить, де є постріли, і прийде патруль. Це значно скорочує час, надає швидкості реагуванню та забирає людський фактор із цього ланцюга. Цю систему вже успішно застосовують в 90 містах світу, відзначаючи значне скорочення злочинів через посилений нагляд за пострілами з боку поліції.

Кожне розумне місто вимагає посилення використання ШІ для безпеки своїх людей та місць, але це повинно відбуватися в поєднанні з жорстокими правилами безпеки проти майбутньої нестабільності штучного інтелекту.

16 лютого 2017 року Європейський Парламент прийняв резолюцію законодавчої ініціативи, в якій рекомендував Європейській Комісії низку законодавчих та незаконодавчих ініціатив у галузі робототехніки та ШІ. Окрім іншого, він закликав Європейську Комісію прийняти пропозицію щодо відповідальності роботів та ШІ, встановити критерії класифікації роботів, які потрібно реєструвати, та створити спеціальне Агентство ЄС із робототехніки та штучного інтелекту й запропонувати хартію, що складається з Кодексу поведінки інженерів-робототехніків, Кодексу комісій з етики досліджень під час перегляду робототехніки, протоколів та типових ліцензій для дизайнерів.

У Вінниці працює Ситуаційний центр при Головному управлінні Національної поліції у Вінницькій області в рамках програми «Безпечне місто». Він дає можливість працівникам поліції ефективно реагувати та впливати на зміни оперативної обстановки, резонансні, надзвичайні події тощо. Він працює на унікальній комплексній системі відеоспостереження "Vezha", що створена на основі штучного інтелекту. Вона розпізнає обличчя, номерні знаки, різні складні ситуації, відслідковує людей за різними параметрами. Лише штучний інтелект здатний розпізнати особу з натовпу в режимі реального часу, навіть якщо її зовнішність була навмисно змінена. З 1 червня 2021 року в Україні почали встановлювати камери заміру швидкості, що працюють у режимі реального часу завдяки певному алгоритму штучного інтелекту, що надає контроль за швидкісним режимом у місті. З кожним днем їх стає все більше й більше, оскільки технології не стоять на місці, необхідний захист громадян, а також слід перевіряти або використовувати відео як доказ щодо порушення закону. Однак окрема увага приділяється управлінню транспортними потоками, завдяки чому збільшується пропускна спроможність наявних доріг та здійснюється керування дорожнім рухом. Їх використання зменшує кількість заторів, покращує екологічну ситуацію та має економічний ефект. Головна спеціалізація таких інформаційних систем полягає в аналізі оперативних сигналів щодо неправильно припаркованих транспортних засобів, вчинення порушень правил дорожнього руху, перевищення швидкості та недотримання технічних параметрів транспортних засобів, нестандартних ситуацій [1].

Однак виникає питання про законність повноважень і правове підґрунтя використання системи збору персональних даних. В українському законодавстві відсутні прямі норми, які б регулювали цю сферу. Отже, поки що держава керується іншими дотичними законами.

Наприклад, нормативною базою використання штучного інтелекту для збору та ідентифікації персональних даних є Конвенція Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», Закон України «Про захист персональних даних», Закон України «Про основи національної безпеки України», Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про інформацію».

Єврокомісія запропонувала нові умови використання штучного інтелекту з 21 квітня 2021 року. Штучний інтелект, з одного боку, може покращити наше життя, зокрема він здатний тестувати ліки, діагностувати хвороби, стояти на заваді шахрайству у фінансовій сфері чи розрізняти фейки, з іншого боку, створює певні ризики, зокрема непрозоре прийняття рішень, дискримінацію, порушення приватності або використання технології в злочинних цілях (для створення фейків, наприклад). Для того щоб уникнути таких загроз та створити умови для безпечного та етичного використання ШІ, Єврокомісія опублікувала пропозиції щодо регулювання ШІ. Зокрема, запропоновані критерії для оцінювання ризиків користування технологій ШІ.

1) Небажана гра з вогнем, адже всі системи ШІ, які відверто загрожують безпеці, засобам добуття чи правам людей (наприклад, технології, які дають змогу чинити маніпуляції поведінкою людей чи дають можливість органам влади робити «соціальну оцінку»), забороняються [7].

2) Високий ризик. Йдеться про технології ШІ, які застосовуються у таких сферах:

− громадський транспорт та інші об'єкти критичної інфраструктури, які можуть загрожувати життю та здоров'ю громадян;

− освіта та професійна підготовка, коли ШІ визначає підхід до освіти чи професійного курсу (наприклад, оцінка іспитів);

− працевлаштування (зокрема, технології для відбору резюме);

– основні приватні та державні послуги (кредитний ступінь популярності та автоматична відмова в отриманні кредиту тощо);

– забезпечення правопорядку (зокрема, оцінювання достовірності доказів);

– міграція, прихисток та прикордонний контроль (наприклад, контроль справжності документів);

– правосуддя та решта демократичних процесів.

Іншими словами, ця категорія охоплює всі сфери, які зачіпають безпеку особи чи права людини, в тому числі право на освіту, працю чи отримання соціальних послуг. Використання систем ШІ з високим ризиком можливе тільки за дотримання жорстких вимог. Крім того, ризиковими є системи розпізнавання особи, які передбачають біометричну ідентифікацію. Їх вжиток у публічних місцях, у тому числі в інтересах правоохоронних органів, заборонено, за винятком деяких випадків (наприклад, для пошуку загублених дітей, запобігання терористичній діяльності або пошуку перш за все небезпечних злочинців). Кожний з цих винятків потребує дозволу від суду чи іншого уповноваженого органу.

3) Обмежений ризик. Йдеться про системи на основі ШІ, наприклад чат-боти. Застосування таких технологій не потребує додаткового дозволу. Потрібно лише давати знати користувачу про те, що він взаємодіє з машиною, щоб він міг прийняти усвідомлене розв'язання проблеми, продовжити чи припинити таку взаємодію.

4) Мінімальний ризик. Йдеться про більшість технологій ШІ, наприклад відеоігри, фільтри комп'ютерного спаму, які не несуть загрози для безпеки або прав користувачів. Використання таких технологій не потребує додаткового дозволу.

Якщо Європарламент прийме ці пропозиції, розвиток корисного та надійного ШІ буде заохочуватися, і навпаки, буде заборонений розвиток ШІ, що загрожує безпеці та правам людини. Отже, ШІ може стати силою добра для світу.

Якщо говорити про Закон України «Про захист персональних даних», то він регулює відносини у сфері оброблення персональних даних, пов'язаних з відеоспостереженням. Згідно із законодавством, ведення відеоспостереження вимагає впровадження відповідних інструментів попередження громадян про факт ведення спостереження, правил одержання, зберігання та накопичення файлів даних для автоматизованого оброблення, певних гарантій їх захисту від незаконного втручання [3]. Кінцевий володілець цих файлів повинен пересвідчитись, чи відповідатиме ведення відеоспостереження загальним або спеціальним положенням законодавства, чи буде воно легальним. Щоб не чекати, доки права громадянина будуть порушені, задля загальної громадської безпеки, органи місцевого самоврядування або парламент можуть запровадити необхідність отримання спеціальних дозволів від державних органів на оброблення персональних даних.

Головна мета оброблення персональних даних повинна бути адекватною і пропорційною та відповідати цілям такого оброблення. Перш за все це означає, що системи відеоспостереження та аналогічні обладнання можуть бути розгорнуті тільки на так званій субсидіарній основі, тобто в цілях, які можуть насправді виправдати необхідність застосування таких систем.

Володілець бази персональних даних, який здійснює відеоспостереження, повинен повідомити потенційного суб'єкта персональних даних про факт здійснення відеоспостереження шляхом розміщення відповідного застереження. Воно має бути розташоване у видному місці і візуально добре сприйматись ще до початку ведення відеоспостереження.

Застереження має містити такі елементи:

– попередження про факт здійснення відеоспостереження;

– назва та реквізити володільця бази персональних даних, який здійснює відеоспостереження;

– мета здійснення відеоспостереження, яка сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця бази персональних даних;

– контактні дані для пред'явлення вмотивованої вимоги щодо зміни або знищення персональних даних суб'єкта персональних даних.

Такі застереження можна зробити перед входом до офісу, магазину, адміністративної будівлі. Тоді можна повішати попередження про зйомку, з яким громадяни можуть ознайомитись. Однак коли відеоспостереження ведеться на вулиці, то неможливо попередити про це всіх громадян. Абсурдно біля кожної камери ставити табличку «Ведеться відеоспостереження». Тут можна обвинуватити державу в нерівноправності між державними органами та приватними особами. Чому перед входом до магазину застереження про відеонагляд за умови камер повинно бути обов'язковим, а на вулиці, де спостереження здійснюється від органів місцевого самоврядування, таких застережень не вимагають?

Під час дослідження основних термінів законодавства одразу виникає правова колізія щодо визначення персональних даних та їх оброблення. Українське законодавство, хоча й повинно відповідати європейському, поки не повністю підлаштовано під сучасні вимоги.

Персональні дані поділяються на дві категорії, такі як загальні та особливі (чутливі).

До загальної категорії можна віднести прізвище та ім'я; дату та місце народження; громадянство; сімейний стан; псевдонім; дані, записані в посвідченні водія; економічне і фінансове становище; дані про майно; банківські дані; підпис; дані з актів цивільного стану; номер пенсійної справи; адресу місця проживання; дипломи про освіту, професійну підготовку тощо.

Особлива категорія охоплює інформацію про расове, етнічне та національне походження; політичні, релігійні та світоглядні переконання; членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи громадських організаціях світоглядної спрямованості; стан здоров'я (медичні дані); статеве життя; біометричні дані; генетичні дані; притягнення до адміністративної чи кримінальної відповідальності; застосування до особи заходів у рамках досудового розслідування; вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»; вчинення щодо особи тих чи інших видів насильства тощо.

Під час оброблення даних необхідно враховувати їх категорію та застосовувати відповідні рівні безпеки. Більш того, в разі оброблення даних, які становлять ризик для прав і свобод людини (особливої категорії даних), розпорядники персональних даних повинні повідомити Уповноваженого Верховної Ради України з прав людини про структурний підрозділ або відповідальну особу, яка організовує роботу з даними.

Персональні дані, згідно із ЗУ «Про захист персональних даних», – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Нині це визначення втрачає актуальність, тому що з'явилось більш уточнююче поняття, що підходить для використання його у законодавстві щодо використання штучного інтелекту для збирання й оброблення інформації про особу, а саме «біометричні дані». Біометричні дані – це сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані – це відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук) [2]. Оброблення цих даних, включаючи розпізнавання обличчя, повинна здійснюватися чітко відповідно до закону, про що йдеться в європейських документах. Наприклад, Загальний

регламент про захист даних (GDPR) забороняє таку обробку, а Директива про захист даних у зв'язку з правоохоронною діяльністю дає змогу обробляти такі дані лише тоді, коли це є крайньою необхідністю, на відміну від нашого законодавства, яке це дозволяє, але лише в окремих випадках та за умови встановлення відповідних гарантій безпеки.

В GDPR встановлено дві категорії біометричних даних. По-перше, інформація, що стосується тілесних характеристик (фізичні або фізіологічні особливості людини, зокрема обличчя, відбитки пальців, сканування райдужної оболонки ока). По-друге, інформація, що стосується поведінки людини (будь-які поведінкові характеристики людини, які є унікальними, завдяки чому є можливість ідентифікації людини). Такий розподіл дає змогу краще захистити дані та уникнути втручання в особисте життя особи. Проте у суспільстві не зникла проблема зчитування біометричних даних з таких приладів, як мобільні гаджети, персональні комп'ютери, ноутбуки, планшети та інші подібні пристрої. Ні для кого не секрет, що нині багато програм використовують наші камери і мікрофони. Усе це робиться для загального збору інформації, щоб у подальшому використати її проти персони, якій належать ці дані, або для розслідування якогось злочину, або з власних інтересів тієї людини, яка налаштувала штучний інтелект для досягнення своїх цілей. Також методи зчитування інформації через ці пристрої можуть допомогти врятувати комусь життя в екстреній ситуації. Наприклад, органи поліції розшукують безвісно зниклу персону, і завдяки законному або протилежному йому методу використання штучного інтелекту щодо біометричних даних можна з легкістю знайти суб'єкта. Правильне застосування цієї технології може вирішити багато питань щодо безпеки людини й громадянина. Проте є багато проблем, що тісно пов'язані зі ШІ та його роботою в просторі Інтернету, а також багатьма іншими аспектами.

Однією з таких проблем може бути проблема вітчизняної нормативної бази через те, що нові технології керуються старими законами, які апріорі не можуть врахувати всі нюанси використання штучного інтелекту та захисту персональної інформації від нього. Технології розпізнавання обличчя, пошук особи в натовпі є надзвичайно цінними для правоохоронних органів та суспільства загалом [5]. Нині немає жодного законодавчого акта або законопроєкта, який би регулював установку системи відеоспостереження в громадських місцях. Окремі Органи місцевого самоврядування затвердили положення про роботу систем відеоспостереження, але всі вони містять недоліки. Потенційно це створює ризик, що за рішенням суду або іншого уповноваженого органу вже встановлені дорогі камери можуть заборонити використовувати.

Отже, з огляду на те, що в Україні регулювання сфери інформаційних правовідносин здійснюється шляхом вирішення окремих проблем нормативно-правовими актами вузької спеціалізації, усі сили законодавців повинні бути спрямовані на комплексне та кодифіковане правове регулювання інформаційних правовідносин суспільства в Україні. Зрозуміло, що лише у громадянському суспільстві можливий розвиток інформаційних правовідносин. На жаль, сучасне українське законодавство щодо розвитку інформаційного суспільства є недосконалим і не відповідає європейському правовому досвіду з цих питань. Базовим поняттям є інформаційне право, яке включає вирішення правових проблем, які стосуються використання, обміну, зберігання та поширення інформації. Позитивним є те, що в Україні прийнято низку законодавчих актів щодо регулювання інформаційних відносин, які дають змогу на якісно новому рівні розвивати інформаційне суспільство.

Багато законодавчих актів ще не можуть регулювати дії ШІ, оскільки вважаються застарілими. Для того щоб ці програми працювали на повністю законних підставах, їм потрібно пройти багато тестів щодо перевірки точності роботи. Також потрібно підготувати суспільство української держави до нововведень, оскільки не всі громадяни можуть зрозуміти, що для доведення правоти тієї чи іншої особи ШІ повинен не просто використовувати камери відеоспостереження, але й записувати усі події, тому багато суб'єктів права все одно вважатимуть ШІ непотрібною річчю. Проте прогрес не стоїть на місці, і ШІ – це один із небагатьох способів кращого майбутнього, тому його введення і використання сприятимуть підвищенню рівня життя й безпеки в країні.

ЛІТЕРАТУРА

1. Про дорожній рух : Закон України від 28 січня 1993 року № 2953-XII. URL: https://zakon.rada.gov.ua/laws/show/3353-12#Text (дата звернення: 20.11.2021).
2. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 5 липня 2012 року № 5492-VI. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення: 26.11.2021).
3. Про захист персональних даних : Закон України від 1 червня 2021 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 25.11.2021).
4. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 січня 2018 року № 67-р. URL: http://zakon5.rada.gov.ua/laws/show (дата звернення: 30.10.2021).
5. Дмитренко В.І. Механізми впровадження електронного урядування на місцевому рівні : дис. … канд. наук : спец. 25.00.02. Київ, 2018. 248 с.
6. "How Artificial Intelligence Will Reshape the Global Order The Coming Competition Between Digital Authoritarianism and Liberal Democracy" by Nicholas Wright. Foreign affairs. July 10, 2018. URL: https://www.foreignaffairs.com/article$/world/2018-07-10/how-artificial-intelliqence-will-reshape-qlobal-order (дата звернення: 20.11.2021).
7. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. European Commission – Press release. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682 (дата звернення: 20.11.2021).