УДК 330.111.62; 004.056.5:61

https://doi.org/10.52058/2786-6025-2024-5(33)-87-97

Діордіца Ігор Володимирович доктор юридичних наук, професор, професор кафедри приватного та публічного права, Київський національний університет технологій та дизайну, вул. Мала Шияновська (Немировича-Данченка), 2, м. Київ, 01011, тел.: (044) 256-29-98, https://orcid.org/0000-0001-7765-6591

Коваль Ольга Миколаївна кандидат юридичних наук, доцент, доцент кафедри приватного та публічного права, Київський національний університет технологій та дизайну, вул. Мала Шияновська (Немировича-Данченка), 2, м. Київ, 01011, тел.: (044) 256-29-98, https://orcid.org/0000-0003-1509-7258

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

Анотація. Інтеграція штучного інтелекту (ШІ) у системи захисту даних у сфері охорони здоров'я має значний потенціал для підвищення рівня безпеки та конфіденційності медичної інформації. У статті розглядаються основні технології ШІ, які можуть бути застосовані для виявлення аномалій, управління доступом та аналізу поведінкових патернів. Технології штучного інтелекту, такі як машинне навчання та глибинне навчання, уже використовуються для виявлення аномалій у поведінці користувачів, аналізу великих обсягів даних та прогнозування потенційних ризиків. Зокрема, застосування алгоритмів машинного навчання допомагає у виявленні несанкціонованого доступу до медичних даних, а також робить можливим відстеження у реальному часі підозрілої активності. Використання технології розпізнавання природної мови (NLP) в автоматизованих розмовних агентах (чат-ботах) для спостереження за пацієнтами після фізичного втручання, а також для автоматизованої ідентифікації та класифікації втручання у сфері соціальної роботи (СР), продемонструвала гарні результати на практиці. ШІ майбутній надійний помічник людства в різних сферах життя. Система захисту даних у сфері охорони здоров’я не є виключенням. Попри нинішню ситуацію та явну недовіру до нововведень в суспільстві, штучний інтелект вже сьогодні ефективно виконує прості завдання. Наприклад, він може виявити присутність сторонніх тіл або патологій на основі рентгенівських знімків, а також визначити наявність ракових клітин у тілі людини. Для цієї статті авторами проаналізовано сучасні дослідження сфері інтеграції ШІ, виявлено основні законодавчі проблеми та перспективи використання ШІ для захисту

персональних даних. Метою дослідження статті є оцінка ефективності наявних законодавчих механізмів інтеграції ШІ у системи захисту даних та обґрунтування їх використання для підвищення рівня безпеки медичної інформації. Результати показують, що застосування технологій ШІ може значно знизити ризики кіберзагроз та забезпечити більш надійне управління доступом до конфіденційних даних. Подальші дослідження у цьому напрямі мають зосередитися на розробці конкретних методів та підходів для інтеграції ШІ у різні аспекти захисту даних, з урахуванням законодавчих вимог.

Ключові слова: штучний інтелект, захист даних, охорона здоров'я, кібербезпека, машинне навчання, управління доступом, поведінкові патерни.

Diorditsa Ihor Volodymyrovych Doctor of Law, Professor, Professor of the Department of Private and Public Law, Kyiv National University of Technology and Design, St. Mala Shyianovska (Nemyrovych-Danchenko), 2, Kyiv, 01011, tel.: (044) 256-29-98, https://orcid.org/0000-0001-7765-6591

Koval Olga Mykolaivna PhD, Associate Professor, Associate Professor of the Department of Private and Public Law, Kyiv National University of Technologies and Design, St. Mala Shyianovska (Nemyrovycha-Danchenka), 2, Kyiv, 01011, tel.: (044) 256-29-98, https://orcid.org/0000-0003-1509-7258

INTEGRATION OF ARTIFICIAL INTELLIGENCE INTO PERSONAL DATA PROTECTION SYSTEMS IN THE HEALTHCARE SECTOR

Abstract. The integration of artificial intelligence (AI) into healthcare data protection systems has significant potential to improve the security and confidentiality of medical information. This article discusses the main AI technologies that can be used for anomaly detection, access control, and behavioral pattern analysis. Artificial intelligence technologies, such as machine learning and deep learning, have great potential for detecting anomalies in user behavior, analyzing large amounts of data, and predicting potential threats. In particular, the use of machine learning algorithms can help detect unauthorized access to medical data and monitor suspicious activity in real time. The use of natural language recognition (NLP) technology in automated conversational agents (chatbots) to monitor patients after physical interventions, as well as for automated identification and classification of social work (SW) interventions documented in electronic medical records, has demonstrated good results. AI is a future assistant to humanity in various spheres of life. The healthcare data protection system is no exception. Despite the current situation in society, artificial intelligence is already effectively performing simple tasks. Artificial intelligence is being actively integrated into

various spheres of life, including healthcare. For example, it can detect the presence of foreign bodies or pathologies based on X-rays, as well as determine the presence of cancer cells in the human body. The article analyzes current research in this area, identifies the main legislative issues and prospects for using AI for data protection. The purpose of the study is to assess the effectiveness of legislative mechanisms for integrating AI into data protection systems and to justify their use to improve the security of medical information. The results show that the use of AI technologies can significantly reduce the risks of cyber threats and provide more reliable management of access to confidential data. Further research in this area should focus on the development of specific methods and approaches for integrating AI into various aspects of data protection, taking into account legal requirements.

Keywords: artificial intelligence, data protection, healthcare, cybersecurity, machine learning, access control, behavioral patterns.

Постановка проблеми. Захист персональних даних у сфері охорони здоров'я має виняткове значення. Останнім часом проблема захисту даних набула особливої актуальності через збільшення кількості кіберзагроз, що впливають на безпеку пацієнтів та медичних установ. Інтеграція штучного інтелекту (ШІ) у системи захисту персональних даних дозволить підвищити безпеку медичної інформації. Застосування технологій ШІ може допомогти у вирішенні багатьох викликів у цій сфері, включаючи виявлення загроз, управління доступом та аналіз поведінкових патернів.

У 2019 році значна частка світових інвестицій була спрямована на компанії, що розробляють ШІ для охорони здоров’я. За оцінками експертів, розмір цих інвестицій становив приблизно $4 млрд., що свідчить про великий інтерес інвестиційних компаній і великих корпорацій до подальшого впровадження ШІ в медичну галузь [1].

Штучний інтелект активно інтегрується в різні сфери життя, включаючи охорону здоров'я. Хоча на даний момент, ще не напрацьовано достатньої нормативно-правової бази регулювання функціонування ШІ, особливо щодо захисту персональних даних, цивільно-правової та кримінальної відповідальності за викриття чи неправомірне використання таких даних. Робота у цьому напрямку ведеться.

23 вересня 2020 року комітет Ради Європи з питань штучного інтелекту представив проміжний звіт, в якому були визначені конкретні кроки для створення правового інструменту Ради Європи з питань ШІ, заснованого на правах людини, верховенстві закону і демократії [1].

Аналіз останніх досліджень і публікацій. Дослідження, присвячені різним аспектам застосування ШІ в медичній сфері, зокрема для діагностики, прогнозування хвороби і оптимізації медичних процесів стають все більш популярними. Здебільшого це праці іноземних науковців (С. Рой, Ц. Ван,

Ц. Чжан, Н. Лассі, С. Чжан, Дж. Морлі та багато інших). Однак, питання інтеграції ШІ у системи захисту персональних даних в охороні здоров'я залишаються недостатньо дослідженими. Існує багато ризиків, пов’язаних з інтеграцією ШІ в локальні системи лікарень, із навчанням ШІ з відкриттям баз даних. Звісно, технології ШІ можуть суттєво підвищити ефективність захисту персональних даних, але конкретні методи і підходи ще потребують подальшого законодавчого врегулювання.

Мета статті – дослідження деяких механізмів інтеграції штучного інтелекту у системи захисту персональних даних в охороні здоров'я, а також аналіз ефективності окремих існуючих механізмів для підвищення рівня безпеки медичних даних.

Виклад основного матеріалу. Штучний інтелект (ШІ) стрімко набуває статусу ключової технології сучасності, здатної трансформувати різноманітні галузі нашого світу, включаючи медицину. ШІ займається створенням моделей, спроможних виконувати завдання, що традиційно вимагають людського ресурсу: навчання, розуміння мови, розпізнавання образів, вирішення проблем та адаптацію до нових умов.

У сфері охорони здоров'я, ШІ революціонізує підходи до діагностики, лікування та управління особистими даними пацієнтів, надаючи нові інструменти для покращення точності та ефективності медичних послуг. Завдяки обробці великих обсягів медичних даних, ШІ допомагає лікарям виявляти захворювання на ранніх стадіях, оптимізувати лікувальні протоколи та персоналізувати медичне обслуговування [2]. Наприклад, алгоритми машинного навчання аналізують інформацію з медичних записів, рентгенівських знімків, результатів аналізів та інших джерел для допомоги у визначенні оптимальних методів лікування.

У 2018 році було розроблено алгоритм для прогнозування аномального падіння тиску під час хірургічних операцій. Для його створення використали технологію машинного навчання: штучний інтелект проаналізував дані 1334 пацієнтів, у яких реєструвався артеріальний тиск під час операцій [1].

Крім того, використання ШІ в системах моніторингу пацієнтів і управління персональними даними покращує якість надання медичних послуг і забезпечує більшу доступність медицини, особливо у віддалених регіонах. Це стало можливим завдяки інноваціям, таким як телемедицина та мобільні медичні додатки, які використовують ШІ для надання консультацій та моніторингу стану здоров'я на відстані [3].

Приклади використання ШІ в медицині є численними і демонструють майбутні покращення діагностики, лікування та ефективності медичних послуг. Зокрема, IBM Watson Health використовує ШІ для аналізу великої кількості медичних даних у лікуванні онкологічних захворювань. Google DeepMind Health розробляє системи ШІ, які використовують машинне

навчання для вдосконалення розуміння медичних зображень і більш точної діагностики. Ці технології створюють нові можливості для медичної сфери, але також вимагають відповідального підходу до захисту даних і етичного використання штучного інтелекту [4].

Інтеграція ШІ у системи захисту даних у сфері охорони здоров'я також гостро ставить питання конфіденційності, безпеки персональних даних та етики перед фахівцями. Важливо виробити стратегії, які забезпечать захист медичних даних пацієнтів, забезпечить їхнє нерозголошення та, водночас, розкриє потенціал ШІ для підвищення ефективності медичних послуг [2].

Технологія ШІ потребує перш за все нормативно-правового регулювання. Що допоможе частково вирішити проблему упередженості суспільства до використання штучного інтелекту, яка шириться світом. Вирішення цієї проблеми сприятиме поширенню ШІ в галузі охорони здоров’я та подальшому використанню отриманих результатів у медичній практиці, оскільки зменшить опір громадськості.

На сьогодні маємо схвалену розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р «Концепцію розвитку штучного інтелекту в Україні». Пріоритетними напрямами реалізації Концепції визначено впровадження технологій штучного інтелекту у сфері освіти, економіки, публічного управління, кібербезпеки, оборони та інших сферах для забезпечення довгострокової конкурентоспроможності України на міжнародному ринку.

17 січня 2020 року в Україні був створений комітет з питань штучного інтелекту, який спочатку зосередив свою увагу на кібербезпеці. Однак наразі виникає потреба в законодавчому регулюванні ШІ в сфері охорони здоров'я, адже він матиме значний вплив на цю галузь у найближчому майбутньому [1].

Захист даних у медичній сфері є критично важливим аспектом, який забезпечує не тільки конфіденційність та безпеку інформації пацієнта, але й підтримує довіру між пацієнтами та медичними установами. Медичні дані включають в себе особисту інформацію про здоров'я, історію хвороб, результати лабораторних тестів, діагнози, інформацію про лікування та інші чутливі дані, які потребують високого рівня захисту. Величезні обсяги даних обробляються та зберігаються в електронному вигляді, а отже потенційно вони завжди знаходяться під загрозою викрадення. Захист медичних даних гарантує, що особиста інформація пацієнтів не буде використана або розголошена без згоди.

А от критичні прорахунки застосування ШІ, виявляються у витіканні персональних даних. На сьогодні відомі випадки витоку персональних даних, пов’язані з використанням штучного інтелекту, але немає конкретного інциденту, який став би широко відомим або привернув значну увагу громадськості. У 2018 Cambridge Analytica, яка спеціалізувалася на аналізі

даних для політичних кампаній, отримала доступ до персональних даних без належного дозволу користувачів, порушуючи принципи конфіденційності та приватності даних. Проект Google Health, спрямований на аналіз медичних даних пацієнтів, зіткнувся з проблемами щодо конфіденційності та захисту даних. У 2016 році з'ясувалося, що Google отримав доступ до особистої медичної інформації понад 1,6 мільйона пацієнтів без їхньої згоди. Це викликало значну критику з боку громадськості та регуляторних органів.

Закони, такі як Загальний регламент про захист даних (GDPR) в ЄС та Закон про відповідальність у страхуванні здоров'я (HIPAA) в США, спрямовані на мінімізацію подібних витоків і встановлюють чіткі правила щодо збереження та обробки медичних даних [3].

Медичні установи стають все більш привабливими цілями для кібератак через велику кількість зберігаємої інформації. Несанкціонований доступ або злом систем може призвести до великого витоку, що надалі матиме серйозні наслідки для приватного життя пацієнтів. Помилки в обробці або навмисні маніпуляції з даними це шлях до неправильного лікування пацієнта. А порушення в обробці даних гарантований шлях до юридичних позовів, великих штрафів, а також репутаційних втрат для медичної установи.

Попри можливі ризики, і як не парадоксально, інтеграція ШІ цілком здатна значно підвищити захист даних у медичній сфері за рахунок автоматизації процесів моніторингу та виявлення несанкціонованого доступу, а також покращення методів шифрування та аутентифікації. Також, ШІ може аналізувати поведінкові патерни для виявлення підозрілих активностей, що є ключовим фактором в активній обороні медичних інформаційних систем [4].

Найбільша загроза пов'язана з великими обсягами медичної інформації, яка стає доступною через цифрові системи. ШІ вимагає доступу до великих даних для навчання і аналізу, що підвищує ризики несанкціонованого доступу та витоків даних.

Визначення меж використання ШІ у медицині наразі справжній етичний парадокс. Виникають питання: хто несе відповідальність за медичні помилки ШІ, та як забезпечити, що ШІ не виявляє упереджень проти певних груп пацієнтів. Часто існуючі медичні системи не є повністю сумісними з новітніми ШІ, що може призвести до технічних труднощів, зайвих витрат на модернізацію і потенційні проблеми з безперервністю лікування. Залежність від автоматизованих систем може призвести до помилок у діагностиці чи лікуванні, особливо якщо ШІ система отримує недостатньо даних або даних поганої якості [3].

Інтеграція ШІ може зменшити безпосереднє спілкування між лікарями і пацієнтами, що може вплинути на якість догляду та задоволеність пацієнтів. З ростом цифровізації медичних даних зростає і ризик кібератак, які можуть призвести не тільки до витоку даних, але й до зупинки важливих медичних служб.

Для мінімізації цих ризиків важливо:

- Розробка та дотримання строгих протоколів безпеки даних.
- Впровадження багаторівневих систем аутентифікації та шифрування.
- Ретельне тестування та моніторинг ШІ систем перед їх впровадженням у клінічну практику.
- Навчання медичного персоналу основам кібербезпеки та етичним аспектам використання ШІ.

Законодавче регулювання використання штучного інтелекту в охороні здоров'я відіграє ключову роль у забезпеченні безпеки, конфіденційності та етичності в обробці медичних даних [4]. Різні країни розробляють і впроваджують нормативні акти, що регулюють як використання ШІ в медицині, так і захист даних. Найвідомішими прикладами такого регулювання є Загальний регламент захисту даних (GDPR) у Європейському Союзі та Закон про переносимість та відповідальність у страхуванні здоров'я (HIPAA) у США.

GDPR встановлює суворі вимоги до обробки особистих даних громадян ЄС, включаючи медичні дані. Регламент вимагає:

- Чіткої згоди на обробку особистих даних.
- Обмеження збору даних лише тими, що необхідні для визначених цілей.
- Право на доступ, виправлення та видалення своїх даних.
- Оцінка впливу на захист даних (DPIA) обов'язкова для процесів, які несуть високі ризики для прав і свобод осіб.

Закон про відповідальність у страхуванні здоров'я (HIPAA) регулює обробку медичних даних, забезпечуючи конфіденційність та безпеку пацієнтської інформації, а також управління цими даними.

Основні положення HIPAA включають:

- Захист конфіденційності у вигляді покладання обов’язку на медичні установи вживати заходів для захисту приватності пацієнтів.
- Впровадження фізичних, адміністративних та технічних заходів безпеки для захисту медичної інформації.
- Строгі правила щодо розкриття та обміну медичною інформацією.

Окрім GDPR та HIPAA, багато країн розробляють власні закони, які регулюють використання ШІ та захист даних у медичній сфері. Це включає все: від обмежень на використання ШІ у діагностиці до вимог щодо локального зберігання даних. Міжнародні організації, такі як Всесвітня організація охорони здоров'я (ВООЗ), також розробляють рекомендації та стандарти, що спрямовані на гармонізацію підходів до захисту даних та використання ШІ в охороні здоров'я на глобальному рівні [5].

Законодавче регулювання є фундаментом, що забезпечує впевненість в тому, що медичні інновації впроваджуються з дотриманням прав пацієнтів та високих стандартів етики. Тому законодавство, як GDPR і HIPAA, має значний вплив на розробку та впровадження штучного інтелекту в медичній сфері. Наприклад, GDPR вимагає від розробників ШІ виконувати оцінку впливу на захист даних (DPIA), що спонукає до розробки більш безпечних систем [6].

Правове регулювання ШІ спонукає до впровадження етичних принципів у дизайн ШІ систем, що підвищує довіру до технологій штучного інтелекту серед медичних фахівців та пацієнтів. Правове регулювання як HIPAA, вимагають від медичних установ та розробників ШІ вживати заходів для забезпечення конфіденційності та безпеки персональних даних. Тобто розробити захист від несанкціонованого доступу, шифрування даних та використання безпечних протоколів передачі даних. Наявність чітких вимог безпеки на рівні законодавства знижує ризики, пов'язані з кіберзагрозами та помилками у системах ШІ, забезпечуючи більшу відповідальність за дотримання стандартів безпеки.

Розглянемо кілька прикладів захисту персональних даних. У Франції захист персональних даних регулюється Загальним регламентом про захист даних (GDPR), що набув чинності 25 травня 2018 року. Франція також має національний орган із захисту даних – Комісію з інформатики та свобод (CNIL), яка забезпечує дотримання GDPR на території країни. Основні положення GDPR, які впливають на використання ШІ у медичній сфері, включають необхідність отримання згоди на обробку даних, право на доступ до даних, право на виправлення та видалення даних, а також обов’язкову оцінку впливу на захист даних (DPIA) для процесів, що несуть високі ризики[7,8].

Після виходу з Європейського Союзу, Велика Британія зберегла більшість положень GDPR, прийнявши їх у вигляді Закону про захист даних 2018 року (Data Protection Act 2018). Цей закон включає положення GDPR з деякими змінами. Медичні установи у Великій Британії зобов’язуються забезпечувати захист персональних даних пацієнтів, включаючи застосування ШІ для обробки даних. Британський комісар з інформації (ICO) забезпечує нагляд за дотриманням законодавства про захист даних.

У Японії захист персональних даних регулюється Законом про захист персональної інформації (APPI), який набув чинності у 2005 році та був оновлений у 2017 році. APPI встановлює вимоги щодо обробки персональних даних, включаючи медичні дані, та містить положення щодо обмеження збору, використання та розкриття персональної інформації. Японська комісія із захисту персональної інформації (PPC) відповідає за нагляд за дотриманням APPI. Порівнюючи законодавчі підходи цих країн, можна виділити кілька ключових моментів. По-перше, GDPR у Франції та Великій Британії, а також

APPI в Японії встановлюють високі стандарти захисту даних, що сприяє безпечному використанню ШІ у медичній сфері. Вимоги щодо оцінки впливу на захист даних (DPIA) є важливим інструментом для виявлення та мінімізації ризиків, пов'язаних з використанням ШІ. По-друге, національні органи із захисту даних у цих країнах відіграють важливу роль у забезпеченні дотримання законодавства та наданні рекомендацій для медичних установ.

Розробка та введення міжнародних стандартів сприятимуть уніфікації підходів до використання ШІ в охороні здоров'я на глобальному рівні, що полегшує міжнародну співпрацю та впровадження транскордонних медичних послуг [6]. Водночас, відмінності в законодавстві між країнами створюватимуть перешкоди для компаній, що розробляють ШІ, оскільки їм потрібно адаптуватися до різних правових систем.

Прикладом введення ШІ для захисту персональних даних є університетський госпіталь Гамбурга-Еппендорфа, що успішно впровадив систему ШІ для захисту медичних даних пацієнтів. Вони використали алгоритми машинного навчання для виявлення аномалій у поведінці користувачів, що дозволило швидко ідентифікувати потенційні загрози та несанкціонований доступ до медичних записів. Система аналізує поведінкові патерни та повідомляє про будь-які підозрілі дії в режимі реального часу. Це значно знизило кількість випадків несанкціонованого доступу та підвищило загальний рівень безпеки медичних даних.

IBM Watson Health використовує ШІ для аналізу великих обсягів медичних даних з метою підтримки рішень у лікуванні онкологічних захворювань. Система ШІ здатна швидко аналізувати медичні записи, рентгенівські знімки та інші джерела даних, щоб виявити потенційні загрози та забезпечити високий рівень захисту конфіденційної інформації пацієнтів.

Висновки. На даний момент комплексного регулювання ШІ в Україні немає. Закон України "Про захист персональних даних" частково охоплює питання автоматизованої обробки даних, а Законі України "Про авторське право і суміжні права" ШІ згадується як система, здатна створювати неоригінальні об'єкти за допомогою комп'ютерної програми. Тому наше законодавство потребує змін та введення законопроектів по прикладу GDPR і HIPAA.

Інтеграція штучного інтелекту в системи захисту даних у сфері охорони здоров'я має значний потенціал для підвищення рівня безпеки та захисту конфіденційної інформації. Впровадження технологій ШІ може значно знизити ризики кіберзагроз, забезпечити більш надійне управління доступом та виявлення аномалій у поведінці користувачів. Подальші дослідження у цьому напрямі мають зосередитися на розробці конкретних методів та підходів для інтеграції ШІ для захисту даних.

Література:

1. Міца О. Дослідження перспектив використання засобівштучного інтелекту в галузі охорони здоров'я [Електронний ресурс] / О. Міца, О. Рябощук // Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/37126/1/%D0%A2%D0%B5%D0%B7%D0%B8_2021_%D0%A0%D1%8F%D0%B1%D0%BE%D1%89%D1%83%D0%BA_%D0%9C%D1%96%D1%86%D0%B0.pdf

2. Roy S. Privacy Prevention of Health Care Data Using AI [Електронний ресурс] // Journal of Data Acquisition and Processing. 2022. Режим доступу: https://www.researchgate.net/profile/Soumit-Roy-3/publication/375957548_PRIVACY_PREVENTION_OF_HEALTH_ CARE_DATA_USING_AI/links/6564e0b8ce88b87031197ecc/PRIVACY-PREVENTION-OF-HEALTH-CARE-DATA-USING-AI.pdf.

3. Wang C., Zhang J., Lassi N., Zhang X. Privacy protection in using artificial intelligence for healthcare: Chinese regulation in comparative perspective [Електронний ресурс] // Healthcare. 2022. № 10. С. 1878. Режим доступу: https://www.mdpi.com/2227-9032/10/10/1878.

4. Morley J., Murphy L., Mishra A., Joshi I. Governing data and artificial intelligence for health care: developing an international understanding [Електронний ресурс] // JMIR Formative Research. 2022. Режим доступу: https://formative.jmir.org/2022/1/e31623.

5. Liaw S. T., Liyanage H., Kuziemsky C. Ethical use of electronic health record data and artificial intelligence: recommendations of the primary care informatics working group [Електронний ресурс] // Yearbook of Medical Informatics. 2020. Режим доступу: https://www.thieme-connect.com/products/ejournals/html/10.1055/s-0040-1701980.

6. Pablo R. G. J., Roberto D. P., Victor S. U. Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology [Електронний ресурс] // Journal of Integrative Bioinformatics. 2022. Режим доступу: https://www.degruyter.com/document/doi/10.1515/jib-2020-0035/html.

7. Aldoseri A., Al-Khalifa K. N., Hamouda A. M. Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges [Електронний ресурс] // Applied Sciences. 2023. № 13. С. 7082. Режим доступу: https://www.mdpi.com/2076-3417/13/12/7082.

8. Forcier M. B., Gallois H., Mullan S. Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers? [Електронний ресурс] // Journal of Law and the Biosciences. 2019. № 1. С. 317. Режим доступу: https://academic.oup.com/jlb/article-abstract/6/1/317/5570026.

9. Kasula B. Y. Framework Development for Artificial Intelligence Integration in Healthcare: Optimizing Patient Care and Operational Efficiency [Електронний ресурс] // Transactions on Latest Trends in IoT. 2023. Режим доступу: https://www.ijsdcs.com/index.php/TLIoT/article/view/406.

10. Ellahham S., Ellahham N. Application of artificial intelligence in the health care safety context: opportunities and challenges [Електронний ресурс] // American Journal of Medical Quality. 2020. Режим доступу: https://journals.sagepub.com/doi/abs/10.1177/1062860619878515.

11. Gerke S., Minssen T., Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare [Електронний ресурс] // Artificial Intelligence in Healthcare. 2020. Режим доступу: https://www.sciencedirect.com/science/article/pii/B9780128184387000125.

References:

1. Mitsa, O. V., & Ryaboshchuk, O. M. (2021). Doslidzhennya perspektyv vykorystannya zasobiv shtuchnoho intelektu v haluzi okhorony zdorov'ya [Research on the Prospects of Using Artificial Intelligence in Healthcare]. Retrieved from https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/37126/1/%D0%A2%D0%B5%D0%B7%D0%B8_2021_%D0%A0%D1%8F%D0%B1%D0%BE%D1%89%D1%83%D0%BA_%D0%9C%D1%96%D1%86%D0%B0.pdf. [in Ukrainian]

2. Roy, S. (2022). Privacy Prevention of Health Care Data Using AI. Journal of Data Acquisition and Processing. Retrieved from: https://www.researchgate.net/profile/Soumit-Roy-3/publication/375957548_PRIVACY_PREVENTION_OF_HEALTH_CARE_DATA_USING_AI/links/6564e0b8ce88b87031197ecc/PRIVACY-PREVENTION-OF-HEALTH-CARE-DATA-USING-AI.pdf.

3. Wang, C., Zhang, J., Lassi, N., & Zhang, X. (2022). Privacy protection in using artificial intelligence for healthcare: Chinese regulation in comparative perspective. Healthcare, 10, 1878. Retrieved from https://www.mdpi.com/2227-9032/10/10/1878.

4. Morley, J., Murphy, L., Mishra, A., & Joshi, I. (2022). Governing data and artificial intelligence for health care: developing an international understanding. JMIR Formative Research. Retrieved from https://formative.jmir.org/2022/1/e31623.

5. Liaw, S. T., Liyanage, H., & Kuziemsky, C. (2020). Ethical use of electronic health record data and artificial intelligence: recommendations of the primary care informatics working group. Yearbook of Medical Informatics. Retrieved from https://www.thieme-connect.com/products/ejournals/html/10.1055/s-0040-1701980.

6. Pablo, R. G. J., Roberto, D. P., & Victor, S. U. (2022). Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology. Journal of Integrative Bioinformatics. Retrieved from https://www.degruyter.com/document/doi/10.1515/jib-2020-0035/html.

7. Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Applied Sciences, 13, 7082. Retrieved from https://www.mdpi.com/2076-3417/13/12/7082.

8. Forcier, M. B., Gallois, H., & Mullan, S. (2019). Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers? Journal of Law and the Biosciences, 1, 317. Retrieved from https://academic.oup.com/jlb/article-abstract/6/1/317/5570026.

9. Kasula, B. Y. (2023). Framework Development for Artificial Intelligence Integration in Healthcare: Optimizing Patient Care and Operational Efficiency. Transactions on Latest Trends in IoT. Retrieved from https://www.ijsdcs.com/index.php/TLIoT/article/view/406.

10. Ellahham, S., & Ellahham, N. (2020). Application of artificial intelligence in the health care safety context: opportunities and challenges. American Journal of Medical Quality. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/1062860619878515.

11. Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. Artificial Intelligence in Healthcare. Retrieved from https://www.sciencedirect.com/science/article/pii/B9780128184387000125.