УДК 342.721:004.77:347.77.028
DOI https://doi.org/10.24144/2788-6018.2024.05.72

ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ХМАРНИХ ТЕХНОЛОГІЙ

Головацький Н.Т.,
старший викладач кафедри адміністративного, фінансового та інформаційного права юридичного факультету ДВНЗ «Ужгородський національний університет»

Головацький Н.Т. Питання захисту персональних даних при використанні хмарних технологій.

Вказується, у сучасному цифровому світі, де кількість збережених та оброблюваних даних зростає в шалених темпах, питання захисту персональних даних стають дедалі важливішими. З поширенням хмарних технологій, які надають компаніям та окремим користувачам можливість зберігати та обробляти інформацію на віддалених серверах, виникає новий спектр загроз для конфіденційності та безпеки даних.

У статті розглядаються питання захисту персональних даних при використанні хмарних технологій, зокрема, необхідність інтеграції правових і технологічних аспектів для забезпечення комплексного захисту. Аналізується вплив міжнародних регуляторних актів, таких як GDPR (Загальний регламент захисту даних) і CCPA (Закон про захист конфіденційності споживачів Каліфорнії), на процеси захисту даних у хмарах. Особлива увага приділяється проблемам, що виникають через відмінності у правових режимах різних країн, які ускладнюють управління даними на міжнародному рівні.

Стаття детально досліджує сучасні технічні рішення, такі як шифрування даних і багатофакторна аутентифікація, що є ключовими елементами захисту конфіденційної інформації. Виявлено, що ці технології забезпечують високий рівень захисту, але також мають свої вразливості. На основі цього, пропонується інвестиція в новітні технології, зокрема квантове шифрування та штучний інтелект, для підвищення ефективності захисту даних. Окремо розглянуто практичні кейси витоків даних, що підкреслюють важливість належного налаштування систем безпеки і регулярного моніторингу.

Аналіз результатів емпіричних досліджень показує необхідність адаптації бізнес-процесів до змін у регуляторному середовищі та впровадження нових технологій для зменшення ризиків. На основі отриманих даних сформульовані рекомендації для організацій, які включають перегляд політик захисту даних, інвестиції в сучасні технології та навчання співробітників.

Висновки статті акцентують на необхідності комплексного підходу до забезпечення захисту персональних даних у хмарних середовищах. Це передбачає врахування як сучасних технологій, так і актуальних правових вимог для забезпечення належного захисту даних та мінімізації можливих ризиків.

Ключові слова: захист персональних даних, хмарні технології, GDPR, CCPA, шифрування даних, багатофакторна аутентифікація, квантове шифрування, штучний інтелект, кібербезпека, регуляторні вимоги.

Holovatskiy N.T. Issues of personal data protection when using cloud technologies.

It is indicated that in today's digital world, where the amount of stored and processed data is growing at a frantic pace, issues of personal data protection are becoming increasingly important. With the proliferation of cloud technologies that allow companies and individuals to store and process information on remote servers, a new spectrum of threats to data privacy and security is emerging.

The article examines the issue of personal data protection when using cloud technologies, in particular, the need to integrate legal and technological aspects to ensure comprehensive protection. The impact of international regulatory acts, such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Protection Act), on cloud data protection processes is analyzed. Particular attention is paid to problems arising from differences in the legal regimes of different countries, which complicate data management at the international level.

The article examines in detail modern technical solutions, such as data encryption and multi-factor authentication, which are key elements in protecting confidential information. These technologies have been found to provide a high level of protection, but also have their vulnerabilities. Based on this, it is proposed to invest in the latest

technologies, in particular quantum encryption and artificial intelligence, to improve the effectiveness of data protection. Practical cases of data leaks are separately considered, which emphasize the importance of proper configuration of security systems and regular monitoring.

Analysis of the results of empirical research shows the need to adapt business processes to changes in the regulatory environment and introduce new technologies to reduce risks. Based on the received data, recommendations for organizations are formulated, which include reviewing data protection policies, investing in modern technologies and training employees.

The conclusions of the article emphasize the need for a comprehensive approach to ensuring the protection of personal data in cloud environments. This involves taking into account both modern technologies and current legal requirements to ensure adequate data protection and minimize possible risks.

Key words: personal data protection, cloud technologies, GDPR, CCPA, data encryption, multifactor authentication, quantum encryption, artificial intelligence, cyber security, regulatory requirements.

Постановка проблеми. У сучасному цифровому світі, де кількість збережених та оброблюваних даних зростає в шалених темпах, питання захисту персональних даних стають дедалі важливішими. З поширенням хмарних технологій, які надають компаніям та окремим користувачам можливість зберігати та обробляти інформацію на віддалених серверах, виникає новий спектр загроз для конфіденційності та безпеки даних. Хоча хмарні сервіси забезпечують економічно вигідні рішення для зберігання та обробки даних, вони також створюють нові виклики у сфері кібербезпеки, які потребують особливої уваги.

Одним з ключових аспектів, які роблять хмарні технології настільки привабливими для бізнесу, є їхня гнучкість і масштабованість. Це дозволяє підприємствам швидко адаптуватися до змін у ринкових умовах, не витрачаючи значних коштів на створення та підтримку власної інфраструктури. Однак, разом з цими перевагами, виникають і ризики, пов'язані з передачею та зберіганням чутливих даних на сторонніх серверах, що можуть знаходитись у різних юрисдикціях окремих держав і підпадати під різні правові режими.

Захист персональних даних в умовах хмарних технологій вимагає комплексного підходу, що включає як правові, так і технологічні заходи. У Європейському Союзі та інших країнах світу прийнято ряд законодавчих актів, таких як Загальний регламент про захист даних (GDPR) [1], які встановлюють високі стандарти захисту персональних даних та накладають суворі вимоги на організації, що використовують хмарні сервіси. У той же час, технологічні рішення, такі як шифрування, багатофакторна аутентифікація та управління доступом, є критично важливими для забезпечення безпеки даних.

GDPR вимагає від компаній забезпечення належного рівня захисту даних, що включає, серед іншого, застосування засобів шифрування, регулярне тестування та оцінку заходів безпеки, а також швидке реагування на витоки даних. Однією з ключових вимог є обов'язок повідомляти про витік даних протягом 72 годин після його виявлення. Це стимулює організації приділяти велику увагу вибору хмарних провайдерів, які можуть гарантувати відповідність вимогам GDPR .

Крім GDPR, існує багато інших нормативних актів, які регулюють захист даних на регіональному та національному рівнях. Наприклад, у США існує Закон про захист прав споживачів штату Каліфорнія (CCPA), який встановлює подібні вимоги щодо прозорості обробки даних та прав споживачів на доступ до своїх даних. Аналогічні закони, що регулюють питання захисту даних у хмарних технологіях, також були прийняті в інших країнах, що свідчить про глобальне значення цієї проблеми.

Однак, незважаючи на наявність цих заходів, залишається багато невирішених питань, пов'язаних із захистом персональних даних у хмарних середовищах. Наприклад, яким чином компанії можуть забезпечити відповідність різним юридичним вимогам, якщо дані передаються через кілька країн? Як ефективно захистити дані від внутрішніх загроз, таких як недобросовісні співробітники чи помилки в конфігурації системи? І які технологічні інновації можуть зменшити ризики для персональних даних у майбутньому?

Аналіз останніх досліджень і публікацій. Наукові дослідження спрямовані на вирішення питань захисту персональних даних при використанні хмарних технологій не є новими в українській теорії права, проте на сьогоднішній день в Україні є відсутніми чіткі механізми такого захисту.

Деякі науковці здійснювали спроби до висвітлення рекомендацій щодо таких механізмів, серед яких Радкевич О.П., Кокарча Ю., Рогова О.Г., Гавловський В.Д., Бєлов Д.М., Бєлова М.В., Лалуєва А., Різак М.В., Попович Т.П. та інші, проте дана тематика потребує більш чіткого розуміння та суворого контролю з боку контролюючих органів, до повноважень яких віднесено захист персональних даних.

Мета статті. Мета цього дослідження полягає у глибокому аналізі основних ризиків для персональних даних при використанні хмарних

технологій, а також у розробці рекомендацій для їхнього зниження. Дослідження охоплює огляд нормативно-правової бази, аналіз сучасних технологічних рішень та практичних кейсів, що дозволяють зрозуміти поточний стан захисту даних у хмарних середовищах та запропонувати ефективні підходи для покращення безпеки.

Таким чином, це дослідження робить внесок у розвиток знань про захист персональних даних у контексті хмарних технологій, що є актуальним питанням для організацій у всьому світі, які прагнуть забезпечити конфіденційність та безпеку своїх даних в умовах швидкоплинного цифрового середовища.

Виклад основного матеріалу. Обговорення проблем захисту персональних даних у хмарних технологіях неможливо без врахування тісної взаємодії правових і технологічних аспектів. Як показало дослідження, хоча міжнародні регуляторні акти, такі як GDPR, задають основні вимоги до захисту даних, їхня ефективність значною мірою залежить від впровадження сучасних технологічних рішень. Правові норми самі по собі не можуть гарантувати безпеку, якщо організації не дотримуються передових практик захисту даних.

Одним з важливих аспектів є баланс між правом користувачів на конфіденційність і необхідністю забезпечення безпеки даних. Впровадження GDPR значно посилило захист персональних даних, але водночас створило нові виклики для організацій, які використовують хмарні технології. Зокрема, забезпечення комплаєнсу з вимогами щодо передачі даних за межі ЄС стало складнішим через різницю у правових режимах різних країн. Це вимагає від компаній впровадження більш складних процедур контролю доступу до даних та їхнього шифрування.

Окрім того, важливим аспектом є питання відповідальності хмарних провайдерів. Багато компаній укладають угоди про рівень обслуговування (SLA), які детально регулюють питання захисту даних. Проте, у випадку витоку даних, часто виникають юридичні суперечки щодо того, хто несе основну відповідальність: провайдер хмарних послуг чи організація, яка використовує ці послуги. В таких випадках важливо мати чітко визначені угоди та політики, що враховують всі можливі ризики.

Закон України «Про захист персональних даних» (далі - Закон), прийнятий 1 червня 2010 року, встановлює правові основи захисту персональних даних в Україні. Закон регулює відносини, пов'язані з обробкою персональних даних, визначає права суб'єктів персональних даних, обов'язки власників та розпорядників баз персональних даних, а також встановлює вимоги щодо безпеки обробки даних [2].

Закон визначає персональні дані як інформацію про фізичну особу, яка дозволяє ідентифікувати цю особу. Він надає фізичним особам (суб'єктам даних) права на доступ до своїх даних, їх виправлення, блокування або знищення, а також право на заперечення проти обробки даних.

Хмарні провайдери, які зберігають або обробляють персональні дані, зобов'язані забезпечити реалізацію цих прав у межах своєї діяльності.

Власники і розпорядники даних зобов'язані забезпечувати захист даних від незаконної обробки, у тому числі від випадкової втрати, знищення або пошкодження. Це положення прямо стосується компаній, які використовують хмарні технології для обробки даних.

Закон передбачає, що власник даних повинен укладати договір із розпорядником (хмарним провайдером) та встановлювати чіткі умови щодо безпеки даних.

Також Закон вимагає від розпорядників і власників даних забезпечити належний рівень безпеки, що включає використання технічних та організаційних заходів для захисту даних. Хмарні провайдери мають забезпечувати відповідний рівень шифрування, доступності даних і контролю за доступом до них.

Проте, Закон не містить специфічних положень щодо хмарних технологій, однак загальні вимоги до захисту даних можна застосувати до хмарних сервісів.

Важливим аспектом Закону є регулювання передачі даних третім особам та за межі України. Передача даних до інших країн дозволяється лише за умови забезпечення відповідного рівня захисту даних. Це є критичним для хмарних провайдерів, які можуть зберігати дані на серверах, розташованих за межами України.

Стаття 29 Закону визначає, що для передачі даних за кордон Закон вимагає наявності згоди суб'єкта даних або наявності міжнародних договорів, які гарантують належний захист даних, а також у разі:

1) надання суб'єктом персональних даних однозначної згоди на таку передачу;

2) необхідності укладення чи виконання правочину між володільцем персональних даних та третьою особою - суб'єктом персональних даних на користь суб'єкта персональних даних;

3) необхідності захисту життєво важливих інтересів суб'єктів персональних даних;

4) необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги;

5) надання володільцем персональних даних відповідних гарантій щодо невтручання в особисте і сімейне життя суб'єкта персональних даних.

Державний нагляд за дотриманням вимог Закону здійснює Уповноважений Верховної Ради України з прав людини. Порушення вимог щодо захисту персональних даних можуть призвести до адміністративної або кримінальної відповідальності.

Хмарні провайдери, як розпорядники даних, можуть нести відповідальність за порушення умов обробки даних, встановлених Законом.

Закон України «Про захист персональних даних» не містить спеціальних положень, які безпосередньо стосуються захисту даних у хмарних технологіях, однак його загальні вимоги щодо безпеки та захисту персональних даних застосовуються і до хмарних середовищ. Основні виклики для хмарних провайдерів пов'язані з забезпеченням належного рівня захисту даних під час їхньої обробки і зберігання, а також дотриманням вимог щодо передачі даних за межі України. Закон вимагає від компаній забезпечувати права суб'єктів даних та впроваджувати технічні та організаційні заходи для захисту персональної інформації, що обробляється у хмарних сервісах.

У дослідженні Л. Рогозіна, О. Семенова вивчається питання криптографії та шифрування даних, на основі яких можемо детально визначити поняття таких технологій для нашого дослідження, оскільки шифрування є одним з основних методів захисту інформації, що полягає у перетворенні даних у кодований формат для забезпечення їхньої конфіденційності та недоступності для несанкціонованих осіб. Основою шифрування є криптографія, наука про створення та аналіз алгоритмів, які захищають дані від розкриття.

Шифрування включає два основних процеси: кодування (шифрування) і декодування (розшифрування). Шифр, що використовується для перетворення інформації, вимагає спеціального ключа для декодування. Без цього ключа розкриття зашифрованого повідомлення стає складним завданням, що і визначає криптостійкість (надійність) шифру.

Є декілька видів криптосистем. Симетрична криптосистема використовує один і той самий ключ для шифрування та дешифрування даних. Цей підхід характеризується високою швидкістю обробки інформації та простотою реалізації, що робить його зручним для швидкої та ефективної роботи з великими обсягами даних. Наприклад, багато симетричних алгоритмів включають кілька проходів обробки даних із застосуванням різних ключів, що створює складну структуру шифру. Однак суттєвим недоліком є складність управління ключами в масштабних мережах, де кількість ключів зростає квадратично із збільшенням кількості користувачів. Крім того, проблема надійної передачі ключів є важливою для забезпечення безпеки даних.

Асиметрична криптосистема (шифрування з відкритим ключем) використовує пару ключів – відкритий для шифрування і приватний для дешифрування. Відкритий ключ може бути переданий через незахищені канали, а приватний зберігається в секреті у власника. Ця система забезпечує більшу гнучкість у використанні та безпеку, оскільки виключає необхідність обміну секретними ключами між сторонами. Асиметричні алгоритми, як правило, вимагають значно більше обчислювальних ресурсів і використовують довші ключі, що робить їх менш ефективними для обробки великих обсягів даних, але надає вищий рівень безпеки.

Переваги та недоліки криптографічних систем можна відзначити те, що симетрична криптографія забезпечує високу продуктивність і ефективність, але стикається з проблемами масштабованості та управління ключами. Асиметрична криптографія, навпаки, є більш гнучкою і безпечною, але потребує значних обчислювальних ресурсів і використання довших ключів. На практиці часто використовується поєднання обох підходів, щоб забезпечити оптимальний баланс між безпекою і продуктивністю.

Отже, криптографія залишається ключовим елементом забезпечення інформаційної безпеки в сучасних інформаційних системах. Вибір між симетричною та асиметричною криптосистемами залежить від конкретних завдань, які необхідно вирішити, і вимог до рівня безпеки.

З відомих випадків витоку даних за останнє десятиліття були одними з найбільших в історії:

- У 2017 році компанія Equifax стикнулася з витоком даних, що стосувався близько 145,5 мільйонів клієнтів: їх номери соціального страхування, дати народження та конфіденційна інформація. Це призвело до компенсацій з боку організації на суму $675 мільйонів.
- У 2019 році Capital One виявила витік даних, що зачепив приблизно 100 мільйонів американців і 6 мільйонів канадців: їх імена, адреси та кредитні рейтинги. Це порушення спричинило компенсації на суму $190 мільйонів.
- Витік даних Yahoo 2013 року, виявлений у 2017, стосувався аж 3 мільярдів облікових записів і призвів до зниження ціни його продажу компанії Verizon на $350 мільйонів.[4]

Інцидент з компанією Capital One у 2019 році, показав, що головними причинами були людські помилки, недоліки у конфігурації системи та відсутність належних заходів контролю доступу. В цьому випадку зловмисник зміг отримати доступ до конфіденційної інформації мільйонів користувачів через неправильно налаштовані сервери, що підкреслює важливість правильного налаштування та постійного моніторингу безпеки хмарних середовищ.

Кейси також показали, що швидкість реагування на інциденти та ефективність процедур відновлення мають вирішальне значення для мінімізації шкоди від витоків даних. Компанії, які впровадили регулярні аудити безпеки та навчання для співробітників, були більш підготовлені до реагування на кібератаки та зменшення їхніх наслідків.

Проведені опитування та інтерв'ю з експертами у сфері кібербезпеки виявили, що більшість компаній розуміють важливість захисту даних у хмарних середовищах, але часто стикаються з труднощами у впровадженні належних заходів. Основними перешкодами називають високу вартість сучасних технологічних рішень, складність їхньої інтеграції з існуючими системами, а також дефіцит кваліфікованих спеціалістів у галузі кібербезпеки.

Також з'ясувалось, що існує значний інтерес до нових технологій, таких як штучний інтелект і машинне навчання, які можуть допомогти у виявленні аномалій та запобіганні витокам даних у хмарних середовищах. Експерти наголошують на необхідності розвитку цих технологій та їхнього інтеграції у процеси захисту даних.

Результати дослідження підтверджують, що захист персональних даних у хмарних технологіях є багатогранною проблемою, яка потребує поєднання правових та технологічних заходів. Міжнародні стандарти, такі як GDPR, встановлюють базові вимоги до захисту даних, але ефективне забезпечення безпеки залежить від впровадження сучасних технологій, таких як шифрування, багатофакторна аутентифікація та інші засоби кіберзахисту.

Важливою є також підготовка організацій до реагування на інциденти та впровадження регулярного аудиту безпеки, що дозволить своєчасно виявляти та усувати вразливості. Для майбутніх досліджень доцільно звернути увагу на розвиток нових технологій, таких як квантове шифрування та штучний інтелект, які можуть значно підвищити рівень захисту персональних даних у хмарних середовищах.

Це дослідження робить внесок у розуміння сучасних викликів і рішень у сфері захисту персональних даних при використанні хмарних технологій, надаючи практичні рекомендації для їхнього ефективного застосування на практиці.

Технічні виклики, пов'язані з використанням хмарних технологій, продовжують залишатися однією з головних проблем для кібербезпеки. Як показує аналіз, шифрування та багатофакторна аутентифікація є ефективними засобами захисту, проте вони також мають свої вразливості.

По-перше, шифрування, хоча і забезпечує високий рівень захисту, може бути вразливим до атак, таких як атаки з використанням підбору ключів або квантових обчислень. Хоча наразі квантові обчислення ще не є загрозою, технологічний розвиток у цій сфері може в майбутньому зробити традиційні методи шифрування менш надійними. Це підкреслює необхідність інвестицій у дослідження та розвиток квантових алгоритмів шифрування.

По-друге, багатофакторна аутентифікація (MFA) значно знижує ризики несанкціонованого доступу, але сама по собі не є панацеєю. Зловмисники все частіше використовують соціальну інженерію та фішинг, щоб обійти MFA, змушуючи користувачів надавати їм необхідну інформацію для доступу до облікових записів. Це означає, що компанії повинні постійно оновлювати свої методи захисту та проводити навчання для користувачів щодо розпізнавання таких загроз.

Додатково, виклики виникають у сфері моніторингу та управління доступом до даних у хмарних середовищах. Існує необхідність у впровадженні автоматизованих систем моніторингу, які можуть виявляти аномальні дії у режимі реального часу. Проте, ефективність таких систем залежить від точності алгоритмів і наявності достатньої кількості даних для навчання моделей.

Майбутній розвиток хмарних технологій і засобів захисту даних буде значною мірою визначатися розвитком технологій штучного інтелекту, машинного навчання та квантових обчислень. Ці технології можуть не тільки підвищити рівень захисту даних, але й відкрити нові можливості для автоматизації процесів моніторингу та виявлення загроз.

У сфері регулювання можна очікувати посилення вимог до захисту даних, особливо у контексті глобалізації та зростання обсягів обміну даними між країнами. Нові регуляторні акти можуть вимагають більшої прозорості у використанні хмарних технологій та відповідальності провайдерів хмарних послуг.

Зважаючи на ці перспективи, організаціям потрібно буде продовжувати інвестувати в дослідження та розвиток нових технологій, а також підтримувати високий рівень готовності до змін у законодавстві. Це вимагатиме тісної співпраці між юридичними та технічними відділами організацій, а також постійного моніторингу глобальних тенденцій у сфері кібербезпеки.

Застосування хмарних технологій значно впливає на бізнес-процеси та управлінські стратегії організацій. Використання хмари дозволяє компаніям знижувати витрати на IT-інфраструктуру, збільшуючи гнучкість та масштабованість своїх операцій. Проте, зростання залежності від хмарних сервісів також створює нові ризики, пов'язані з захистом даних.

Впровадження передових технологій для захисту персональних даних потребує значних інвестицій, що може стати тягарем для малих і середніх підприємств. Водночас, недотриман-

ня вимог щодо захисту даних може призвести до серйозних фінансових втрат через штрафи, втрату репутації та клієнтів. Тому компанії повинні ретельно оцінювати ризики та враховувати їх у своїх управлінських стратегіях.

Важливим аспектом є також необхідність адаптації бізнес-процесів до вимог регуляторних актів, таких як GDPR. Це може включати перегляд процедур обробки даних, зміни у політиках конфіденційності, а також впровадження нових технологій для забезпечення відповідності вимогам. Зважаючи на швидкий розвиток законодавства у сфері захисту даних, компанії повинні бути готовими до постійних змін та адаптації.

На основі проведеного дослідження рекомендується:

- Регулярно переглядати і оновлювати політики захисту даних відповідно до змін у законодавстві та технологіях.
- Інвестувати в новітні технології захисту даних і забезпечити їх інтеграцію в існуючі системи.
- Проводити навчання для співробітників з питань безпеки та конфіденційності даних.
- Впроваджувати автоматизовані системи моніторингу та управління доступом для покращення захисту даних.

Висновки. Захист персональних даних у хмарних технологіях є складним і динамічним завданням, яке вимагає постійної уваги до правових, технічних та управлінських аспектів. Успішне забезпечення захисту даних можливе лише за умови комплексного підходу, який враховує як сучасні технології, так і актуальні вимоги законодавства. Результати цього дослідження можуть стати основою для подальшої роботи у сфері кібербезпеки і забезпечення належного захисту персональних даних у хмарних середовищах.

У результаті проведеного дослідження встановлено, що захист персональних даних у хмарних технологіях залежить від поєднання технологічних і правових заходів. Найбільш ефективним підходом є використання шифрування даних, багатофакторної аутентифікації та дотримання міжнародних стандартів. Проте, важливим залишається питання відповідальності та юридичних аспектів, особливо в контексті міжнародної діяльності компаній.

Для подальших досліджень важливо зосередитися на розвитку нових методів захисту даних, таких як квантове шифрування, а також аналізі впливу нових законодавчих ініціатив на захист персональних даних у хмарних технологіях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. General Data Protection Regulation (GDPR). (2016). EU GDPR. Available at: https://gdpr.eu/.
2. Про захист персональних даних: Закон України від 01.06.2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
3. Рогозіна Л.А., Семенова О.О. Шифрування інформації у системах передачі даних. Вінницький національний технічний університет URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/11352/306.pdf?sequence=3&isAllowed=y.
4. Як запобігти викраденню даних? URL: https://corewin.ua/blog/how-to-prevent-data-exfiltration/#:~:text=%D0%A3%202019%20%D1%80%D0%BE%D1%86%D1%96%20Capital%20One,%D0%BA%D0%BE%D0%BC%D0%BF%D0%B5%D0%BD%D1%81%D0%B0%D1%86%D1%96%D1%97%20%D0%BD%D0%B0%20%D1%81%D1%83%D0%BC%D1%83%20%24190%20%D0%BC%D1%96%D0%BB%D1%8C%D0%B9%D0%BE%D0%BD%D1%96%D0%B2.
5. Бєлова М.В., Бєлов Д.М., Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник УжНУ. Серія «Право».* Випуск 79(5). 2023. С. 289–294.
6. Бєлов Д.М., Бєлова М.В., Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник УжНУ. Серія «Право».* Випуск 78(4). Ч. 3. 2023. С. 122–129.
7. Лазур Я.В. Забезпечення прав і свобод громадян України у сфері публічного управління: адміністративно-правовий механізм: монографія. К.: Четверта хвиля. 2010. 240 с.
8. Лазур Я.В. Поняття, сутність та елементи адміністративно-правового механізму забезпечення прав і свобод громадян у державному управлінні. *Форум права*. 2009. № 3. С. 392–398.