JEL: M15
DOI: https://doi.org/10.53920/ES-2024-4-14

Володимир Володимирович ШЕВЧЕНКО,
здобувач ступеня PhD за спеціальністю 073 – Менеджмент,
ПВНЗ «Європейський Університет»
ORCID ID: 0009-0008-5142-5208

ХМАРНІ РІШЕННЯ ТА КІБЕРБЕЗПЕКА: ІННОВАЦІЙНІ ПІДХОДИ ДО ЗАХИСТУ БІЗНЕСУ У НЕСТАБІЛЬНИХ УМОВАХ

Стаття присвячена дослідженню хмарних технологій як інструменту забезпечення кібербезпеки та економічної стабільності підприємств в умовах воєнної агресії російської федерації проти України та загальної глобальної нестабільності. Хмарні рішення розглядаються як стратегічний ресурс для підтримки безперервності бізнес-процесів, підвищення гнучкості операційної діяльності та стійкості до кіберзагроз, особливо в умовах підвищених ризиків і фізичного знищення інфраструктури. Основна увага приділяється кіберризикам і загрозам, які супроводжують впровадження хмарних рішень, а також шляхам мінімізації вразливостей завдяки багаторівневим підходам до захисту інформаційних активів.

Аналізуються практичні кейси українських компаній у сферах телекомунікацій, енергетики та фармацевтики, які успішно використовують хмарні технології для підтримки безпеки і стабільності, зокрема для резервування критичних бізнес-процесів та забезпечення швидкого відновлення інфраструктури. На основі методів аналізу і синтезу окреслено стратегії, які можуть покращити управління ризиками, включаючи впровадження архітектури нульової довіри (Zero Trust) та інтеграцію штучного інтелекту і блокчейн для підвищення прозорості й контролю. Окрему увагу приділено дотриманню міжнародних стандартів безпеки, таких як ISO/IEC 27001, що підвищує довіру клієнтів і партнерів до хмарних рішень і дозволяє підприємствам відповідати суворим регуляторним вимогам.

Отримані результати можуть слугувати основою для розробки стратегій кібербезпеки, адаптованих до викликів сучасних умов, та сприяти підвищенню конкурентоспроможності підприємств у високоризикових галузях. Висновки підкреслюють необхідність створення комплексних і адаптивних підходів до захисту інформаційних ресурсів, які дозволять

повною мірою скористатися перевагами хмарних технологій в умовах сучасного динамічного середовища.

Ключові слова: *хмарні технології, економічна безпека, кібербезпека, цифрова трансформація, стратегічне управління, інформаційна стійкість, адаптивний менеджмент, хмарна інфраструктура, захист даних, ризик-менеджмент, архітектура нульової довіри, штучний інтелект, інноваційні технології, блокчейн, безперервність бізнесу, хмарні сервіси, цифрова безпека, управління ризиками, криптографічний захист, хмарна стратегія.*

Volodymyr SHEVCHENKO,
PhD candidate in Management,
PHEE «European University»

CLOUD TECHNOLOGIES AND CYBERSECURITY: INNOVATIVE APPROACHES TO BUSINESS PROTECTION IN UNSTABLE CONDITIONS

The article is focused on the study of cloud technologies as a tool for ensuring cybersecurity and economic stability of enterprises in the context of the military aggression of the Russian Federation against Ukraine and general global instability. Cloud solutions are seen as a strategic resource for maintaining business continuity, increasing operational flexibility, and resilience to cyber threats, especially in the context of increased risks and physical destruction of infrastructure. The focus is on the cyber risks and threats accompanying cloud solutions and ways to minimize vulnerabilities through multi-level approaches to protecting information assets.

The article analyses practical cases of Ukrainian companies in the fields of telecommunications, energy, and pharmaceuticals that successfully use cloud technologies to maintain security and stability, particularly to back up critical business processes and ensure rapid infrastructure recovery. Based on the methods of analysis and synthesis, the article outlines strategies that can improve risk management, including the implementation of Zero Trust architecture and the integration of artificial intelligence and blockchain to increase transparency and control. Particular attention is paid to compliance with international security standards, such as ISO/IEC 27001, which increases customer and partner confidence in cloud solutions and allows businesses to meet strict regulatory requirements.

The results serve as a basis for developing cybersecurity strategies adapted to the challenges of modern conditions and help increase

enterprises' competitiveness in high-risk industries. The conclusions highlight the need to create comprehensive and adaptive approaches to protecting information resources that will allow taking full advantage of the benefits of cloud technologies in today's dynamic environment.

Keywords: *Cloud technologies, Economic security, Cybersecurity, Digital transformation, Strategic management, Information resilience, Adaptive management, Cloud infrastructure, Data protection, Risk management, Zero Trust architecture, Artificial intelligence, Innovative technologies, Blockchain, Business continuity, Cloud services, Digital security, Risk management, Cryptographic protection, Cloud strategy.*

Постановка проблеми. В умовах глобальної невизначеності та зростання геополітичних ризиків, особливо на тлі воєнної агресії російської федерації проти України, забезпечення безперервності бізнес-операцій стає критично важливим і вимагає адаптації управлінських підходів та впровадження технологічних інновацій. Хмарні технології, які забезпечують масштабованість, гнучкість та швидке реагування на зміни ринку, набувають стратегічного значення як інструмент підтримки стабільності бізнесу в умовах підвищених ризиків. Їх використання мінімізує можливість втрати бізнесу, оскільки вони дозволяють підтримувати безперервність операцій навіть за умов фізичного знищення інфраструктури чи інших критичних ситуацій.

Однак перенесення бізнес-процесів у хмарне середовище створює нові виклики та потребує ретельного управління ризиками. Перш за все, безпека даних і кіберзахист стають пріоритетними питаннями, адже саме надійний захист інформації є основою збереження репутації та економічної стабільності компанії. Незважаючи на численні переваги, хмарні сервіси також можуть бути джерелом загроз: у випадках неефективного управління хмарними ресурсами або недосконалих налаштувань зростає ризик кіберзломів, витоків даних й інших видів несанкціонованого доступу. Це вимагає від компаній розробки адаптованих стратегій кібербезпеки, які враховують особливості роботи з хмарними технологіями, а також впровадження багаторівневих систем захисту.

Крім того, виникає залежність від надійності та стабільності обраних постачальників хмарних послуг, що висуває додаткові вимоги до управління бізнес-ризиками. Впровадження хмарних рішень передбачає комплексний підхід до кібербезпеки, який містить оцінку потенційних загроз, постійний моніторинг безпеки та адапта-

цію корпоративних політик у відповідь на нові виклики. З огляду на складність впровадження цих технологій, компанії також стикаються з необхідністю навчання персоналу та розвитку компетенцій у сфері кіберзахисту й управління хмарними середовищами.

Таким чином, хмарні технології пропонують бізнесу широкі можливості для розвитку та адаптації в умовах нестабільності, але водночас висувають до компаній складні вимоги щодо управління кіберризиками та розробки передових методів захисту інформаційних активів.

Метою статті є дослідження основних кіберзагроз і викликів, пов'язаних із впровадженням хмарних технологій, а також розробка практичних рекомендацій щодо забезпечення надійного захисту інформаційних активів і безперервності бізнес-процесів. Особлива увага приділяється аналізу кіберризиків, методам управління ними та застосуванню передових підходів до кібербезпеки для мінімізації вразливостей у хмарних середовищах, що стають критично важливими в умовах сучасної нестабільності та загроз інформаційній інфраструктурі.

Об'єктом дослідження у цій роботі є хмарні технології як інструмент для забезпечення кібербезпеки підприємств в умовах воєнного конфлікту. Основна увага зосереджена на вивченні впливу хмарних сервісів на інформаційну стійкість бізнесу, його адаптивність і здатність до захисту від кіберзагроз в умовах підвищеного ризику та нестабільності.

Аналіз останніх досліджень і публікацій. Наукове співтовариство активно досліджує різні аспекти використання хмарних рішень, зосереджуючись на їхніх перевагах і ризиках у контексті кібербезпеки, регуляторного середовища та технологічних інновацій. У численних публікаціях увага приділяється надійності хмарних сервісів та захисту даних, що стає особливо актуальним на тлі загроз, спричинених воєнною агресією російської федерації проти України. Зокрема Ч. Рупа та інші (Індія, 2023) [7] досліджують інноваційні криптографічні підходи до захисту даних у хмарних середовищах, що значно знижують ризики, пов'язані з компроментацією інформації під час її зберігання та обробки. Інші дослідження зосереджуються на викликах, що виникають при адаптації хмарних технологій у корпоративні структури, враховуючи культурні та організаційні бар'єри. Наприклад, Насір І. (Пакистан, 2023) [6] аналізує можливості адаптації корпоративних інформаційних систем до хмарних технологій з урахуванням

потреби дотримання високих стандартів безпеки та регуляторних вимог. Водночас В. Богом'я та інші (Україна, 2023) [1] досліджують криптографічні методи боротьби з кіберзлочинністю з урахуванням специфіки інформаційних систем, а Р. Бандура та інші (США, 2023) [4] підкреслюють значення цифрових технологій для забезпечення кіберстійкості та стабільності під час воєнної агресії російської федерації проти України, де цифрові платформи стали важливим інструментом підтримки критичних служб навіть у кризових умовах.

Отже, сучасні дослідження у сфері хмарних технологій демонструють широкий спектр можливостей та викликів, з якими стикаються організації. Ці праці створюють важливу базу знань для подальшого аналізу й оцінки того, як хмарні технології можуть сприяти забезпеченню кібербезпеки та мінімізації ризиків втрати інформаційних активів у сучасних умовах глобальної нестабільності.

Виклад основного матеріалу дослідження. Кібератаки на великі українські компанії створили серйозні загрози для їхньої цифрової безпеки та стабільності бізнес-процесів, підкреслюючи критичну важливість розумного впровадження хмарних технологій як засобу захисту інформаційних активів у сучасних умовах. Наприклад, під час атаки на телекомунікаційного оператора «Київстар» у грудні 2023 р. відбулися багаторівневі спроби проникнення та виведення з ладу ключових елементів інфраструктури, що підкреслює високий рівень організації зловмисників. Це вказує на необхідність впровадження таких технологій, які дозволили б швидко адаптувати інфраструктуру до умов ризику та захищати її від втрат контролю. В такій ситуації використання хмарних технологій могло б суттєво зменшити наслідки атаки, забезпечуючи високий рівень стійкості та гнучкості у керуванні інформаційними потоками.

З огляду на це, компаніям доцільно впроваджувати хмарні рішення для резервування критично важливих бізнес-процесів. Це дозволить швидко відновити доступ до даних і сервісів у разі атак, водночас забезпечуючи більш ефективний моніторинг трафіку та виявлення аномалій, що мінімізує негативний вплив на операційну діяльність. Подібні хмарні рішення також сприяють розширенню можливостей організації для своєчасної реакції на загрози, що є важливим аспектом кібербезпеки.

Інший приклад – атака вірусу Petya у 2017 році, яка вплинула на роботу багатьох українських компаній, зокрема в фінансовій, енергетичній та логістичній галузях. Вірус зашифрував важливі дані, пара-

лізувавши бізнес-процеси, що підкреслює ризики, пов'язані з відсутністю відповідних механізмів безпеки. Це наочно ілюструє можливі фінансові втрати та порушення операційної діяльності, які виникають через відсутність правильно побудованих кіберзахисних інструментів.

Також варто згадати атаку угрупування Black Energy на енергетичні об'єкти в Прикарпатті у 2015 році, яка призвела до відключення електроенергії для понад 80 тисяч споживачів. Це знову показує вразливість критичної інфраструктури перед кіберзагрозами, особливо в умовах воєнної агресії російської федерації проти України. Таким чином, саме впровадження хмарних технологій може забезпечити необхідну захищеність і гнучкість, що підвищує стійкість компаній до атак.

Ці приклади вказують на критичну потребу перегляду безпекових підходів і використання хмарних технологій як одного з основних компонентів стратегій кіберзахисту. Сучасні організації, особливо у високоризикових умовах, мають потребу в технологіях, які не лише мінімізують ризики, але й дозволяють розширити цифрові можливості підприємства. Водночас важливо підкреслити, що для успішного впровадження та захисту даних необхідно правильно користуватися хмарними рішеннями та враховувати їх можливі ризики.

У цьому контексті ефективне застосування хмарних сервісів, таких як Azure, вже продемонстровано на прикладах українських компаній та державних установ, що забезпечує стійкість і безперервність роботи інфраструктури під час фізичних атак. Кредобанк, який розпочав перенесення інфраструктури до хмари ще до повномасштабного вторгнення рф у 2022 р. після дозволу Національного банку України на переміщення даних за кордон 24 лютого 2022 р., зміг забезпечити архітектурну і безпекову адаптацію до нових умов. Це підтверджує, що хмарні технології відкривають нові можливості для управління ресурсами, інноваційного розвитку та впровадження штучного інтелекту, що підвищує конкурентоспроможність компаній.

Також компанія ДТЕК інвестує в інновації та цифровізацію, оптимізуючи процеси управління енергоресурсами, підвищуючи ефективність та надійність. Використання штучного інтелекту (ШІ) енергогенерації та кращого балансування енергосистеми, дозволяє прогнозувати поломки обладнання для своєчасного ремонту та запобігання аваріям, а також вирішувати інші завдання управління енергетичними активами.

Поряд з цим, фармацевтична компанія «Дарниця» використовує аналітичні інструменти Microsoft Big Data та Synapse для обробки даних, завдяки чому здобуває можливості для прогнозування наявності своєї продукції в аптеках, оптимізації ланцюгів поставок, прогнозування попиту на продукцію, розробки нових продуктів та формування цін [2]. Це підвищує точність рішень і забезпечує продуктивність, надаючи компанії конкурентну перевагу.

Широке впровадження хмарних технологій наочно демонструє їхній вплив на економічну безпеку підприємств. Майже 92% організацій інтегрували ту чи іншу форму хмарної інфраструктури, що відображає високий рівень залежності від цієї технології. Приблизно 50% компаній використовують хмарні платформи для зберігання конфіденційної інформації як у зашифрованому, так і в незашифрованому вигляді. Проте, поряд із широкими можливостями, хмарні технології несуть значні ризики, спричинені недостатнім або неправильним дотриманням правил кібербезпеки: близько 83% компаній зазнали принаймні одного випадку витоку даних. Середня вартість таких інцидентів у 2023 році досягла 3,6 млн доларів США, що вказує на суттєві фінансові загрози, обумовлені недотриманням або недосконалістю заходів кіберзахисту у хмарних середовищах [5].

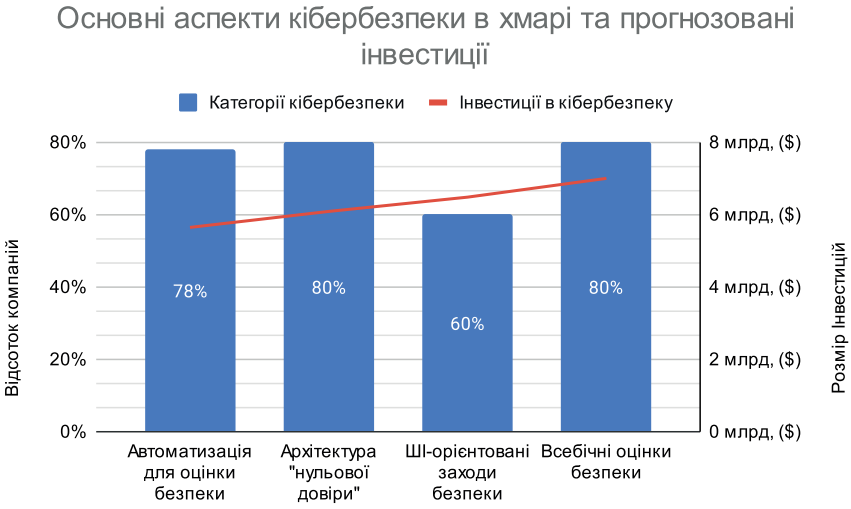

Рис. 1. Основні аспекти кібербезпеки в хмарі

Джерело: складено на основі [8]

Згідно з експертними прогнозами, витрати на кібербезпеку хмарних середовищ сягнуть 7 млрд дол. (рис. 1), що підкреслює важливість цієї галузі. Близько 78% компаній вже використовують автоматизацію для оцінки безпеки своїх хмарних рішень і ця тенденція лише зростатиме, що дозволить компаніям швидше реагувати на загрози та ефективніше управляти безпекою. Важливу роль відіграватиме архітектура «нульової довіри» (Zero Trust), яка стає все більш популярною серед підприємств. Приблизно 80% підприємств розглядають можливість впровадження або вже впроваджують цю модель, що свідчить про тренд зміщення у бік більш жорстких моделей кібербезпеки. Крім того, інновації в технологіях, такі як штучний інтелект (ШІ) та блокчейн, стають важливим фактором у боротьбі з кіберзагрозами. ШІ зможе виявляти загрози та реагувати на них у режимі реального часу, аналізувати величезні обсяги даних для виявлення закономірностей та аномалій, а також автоматизувати процеси безпеки, щоб зменшити кількість людських помилок та пришвидшити час реагування. Децентралізована і незмінна природа блокчейну здатна забезпечити прозорі та стійкі до підробки реєстри транзакцій, поліпшити управління ідентифікацією і доступом, а також підвищити цілісність і відстежуваність даних у хмарних середовищах.

З огляду на високий рівень впровадження хмарних технологій, дедалі важливішим стає питання управління відповідними ризиками та забезпечення безпеки таких рішень. Аналізуючи практики провідних світових компаній, можна зробити висновок, що інвестування в хмарні рішення є економічно доцільним у довгостроковій перспективі. Наприклад, згідно з аналітичними даними компанії Expert Insights, витрати на впровадження та підтримку хмарних технологій поступово знижуються при одночасному істотному підвищенні ефективності та гнучкості операційних процесів [5].

Варто також відзначити, що сучасні підприємства активно застосовують гібридні хмарні моделі, що дозволяють збалансувати використання публічних і приватних ресурсів і дають можливість одночасно скористатися перевагами масштабованості публічної хмари та забезпечити підвищений рівень безпеки для критично важливих даних у приватній інфраструктурі. Такі підходи сприяють формуванню більш гнучкої системи управління інформаційними ресурсами, швидкій адаптації підприємств до змін зовнішньої кон'юнктури.

Підвищення ролі автоматизації та використання штучного інтелекту в хмарних технологіях також стає ключовим фактором у бо-

ротьбі з кіберзагрозами. Згідно з прогнозами, понад 80% підприємств будуть використовувати автоматизовані системи моніторингу безпеки, що дозволить значно скоротити час реагування на потенційні загрози та мінімізувати ризики несанкціонованого доступу [8]. Це свідчить про необхідність розвитку компетенцій персоналу в галузі хмарної безпеки та оптимізації процесів кіберзахисту з використанням передових технологій.

Окремої уваги заслуговує питання регуляторної відповідності та дотримання міжнародних стандартів безпеки, таких як ISO/IEC 27001, які встановлюють вимоги до системи управління інформаційною безпекою (СУІБ). Впровадження цих стандартів забезпечує системний підхід до захисту інформаційних активів, включаючи дані клієнтів, фінансову інформацію та комерційні таємниці, що є критично важливим для хмарних технологій. Окрім підвищення прозорості процесів управління та захисту даних, стандарти ISO/IEC 27001 допомагають підприємствам визначати, оцінювати та мінімізувати ризики інформаційної безпеки, що підвищує їхню стійкість до кіберзагроз.

Дотримання цих стандартів також значно полегшує відповідність регуляторним вимогам, наприклад, щодо Загального регламенту захисту даних (GDPR), що є особливо важливим для компаній, які оперують на міжнародному ринку. Це знижує ймовірність юридичних санкцій і підвищує довіру до компанії з боку інвесторів і партнерів, що вважають важливим наявність надійних засобів захисту інформаційних систем.

До того ж, впровадження ISO/IEC 27001 може надати компанії конкурентну перевагу на ринку, особливо в галузях з підвищеними вимогами до інформаційної безпеки, таких як фінансовий сектор, охорона здоров'я та державні установи.

Підвищення рівня довіри клієнтів до безпеки хмарних рішень сприяє покращенню репутації компанії та залученню нових клієнтів, що дозволяє зміцнити позиції на ринку та поліпшити фінансові показники. Таким чином, дотримання стандартів безпеки стає не лише засобом для мінімізації ризиків, але й стратегічним інструментом, що забезпечує зростання бізнесу, підвищення ефективності управління ризиками і довіри до компанії на глобальному рівні.

Впровадження хмарних технологій в умовах сучасних економічних і геополітичних викликів є важливим чинником для забезпечення кібербезпеки та економічної стабільності підприємств. Завдяки ретельно розробленим стратегіям управління ризиками та забезпечен-

ня відповідності міжнародним стандартам, компанії можуть значно підвищити захист своїх інформаційних ресурсів, мінімізувати ймовірність порушення бізнес-процесів та одночасно скористатися можливостями хмарних технологій для розвитку та інновацій.

Висновки та пропозиції. Хмарні технології є стратегічно важливим інструментом для забезпечення стійкості та безперервності роботи підприємств, особливо в умовах воєнної агресії російської федерації проти України та глобальної невизначеності. Їхнє впровадження дозволяє оптимізувати бізнес-процеси, забезпечити гнучкість і масштабованість, а також підвищити конкурентоспроможність організацій. Проте, поряд із численними перевагами, зростання використання хмарних рішень створює підвищені ризики кібербезпеки, здатні спричинити значні фінансові втрати та порушення операційної діяльності. Тому доцільним є розроблення комплексних стратегій управління ризиками, які містять застосування передових методів захисту даних, запровадження архітектури «нульової довіри» (Zero Trust) і автоматизацію процесів безпеки із використанням штучного інтелекту.

Зважаючи на це, рекомендується підприємствам активно інвестували в розвиток хмарної інфраструктури, приділяючи особливу увагу системам моніторингу й виявлення загроз у режимі реального часу. Необхідно також створювати умови для безперервного підвищення кваліфікації персоналу в галузі кібербезпеки, розробляти політики інформаційної безпеки з урахуванням особливостей роботи в хмарних середовищах. Ключовим аспектом залишається інтеграція хмарних технологій з іншими інноваційними рішеннями, такими як блокчейн, що посилить цілісність і прозорість даних та підвищить надійність захисту інформаційних активів.

Враховуючи актуальні виклики, пов'язані з кіберзагрозами, компаніям слід розглянути застосування багаторівневих стратегій кібербезпеки, що охоплюють не лише технологічні аспекти, але й організаційні й людські фактори. Такий підхід забезпечить комплексне управління ризиками та дасть можливість швидше реагувати на потенційні загрози. Крім того, особлива увага має приділятися дотриманню міжнародних стандартів безпеки, таких як ISO/IEC 27001, що сприятиме зміцненню довіри з боку клієнтів та партнерів.

Підсумовуючи вище викладене, доходимо висновку, що хмарні технології в умовах сучасних економічних та геополітичних викликів є важливим чинником зміцнення економічної стабільності підпри-

ємств. Їхнє впровадження має здійснюватися на основі продуманих стратегій, які враховують не лише технологічні аспекти, але й організаційні, культурні та регуляторні фактори. Лише такий системний підхід дозволить підприємствам повноцінно використовувати переваги хмарних технологій, забезпечуючи при цьому надійний захист своїх інформаційних ресурсів у сучасних високоризикових умовах.

ЛІТЕРАТУРА

1. Богом'я В. І., Кочегаров В. С. Кібербезпека в хмарних сервісах за допомогою застосування криптографічних методів. *Водний транспорт*. 2023. № 1(37). С. 239 – 246. URL: https://doi.org/10.33298/2226-8553.2023.1.37.27 (дата звернення: 01.10.2024).

2. Хмарна трансформація – які можливості відкриваються перед бізнесом. Європейська Бізнес Асоціація. URL: https://eba.com.ua/hmarna-transformatsiya-yaki-mozhlyvosti-vidkryvayutsya-pered-biznesom/ (дата звернення: 01.10.2024).

3. Юрасов С. «Київстар» хотіли знищити. Наш великий розбір, як це могло статися. dev.ua. URL: https://dev.ua/news/kyivstar-1702659220 (дата звернення: 01.10.2024).

4. Bandura R., Staguhn J. Digital will drive ukraine's modernization. Center for Strategic and International Studies. URL: https://www.csis.org/analysis/digital-will-drive-ukraines-modernization (дата звернення: 01.10.2024).

5. Harris C. 50 cloud security stats you should know in 2024. Expert Insights. URL: https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/ (дата звернення: 01.10.2024).

6. Iqra Naseer. AWS cloud computing solutions: optimizing implementation for businesses. *Statistics, computing and interdisciplinary research*. 2023. Т. 5, № 2. С. 121 – 132. URL: https://doi.org/10.52700/scir.v5i2.138 (дата звернення: 01.10.2024).

7. Rupa C., Greeshmanth, Shah M. A. Novel secure data protection scheme using Martino homomorphic encryption. *Journal of cloud computing*. 2023. Т. 12, № 1. URL: https://doi.org/10.1186/s13677-023-00425-7 (дата звернення: 01.10.2024).

8. The future of cloud security: 20 statistics & trends to track. CyberTalk. URL: https://www.cybertalk.org/2024/01/24/the-future-of-cloud-security-20-statistics-trends-to-track/ (дата звернення: 01.10.2024).

REFERENCES

1. Bohom'ia V. I., Kocheharov V. S. Kiberbezpeka v khmarnykh servisakh za dopomohoiu zastosuvannia kryptohrafichnykh metodiv [Cybersecurity in Cloud Services Using Cryptographic Methods]. *Vodnij transport*. 2023. No. 1(37). Pp. 239 – 246. URL: https://doi.org/10.33298/2226-8553.2023.1.37.27 (date of access: 01.10.2024).

2. Khmarna transformatsiia – yaki mozhlyvosti vidkryvaiut'sia pered biznesom [Cloud Transformation – What Opportunities Open Up for Business]. European Business Association. URL: https://eba.com.ua/hmarna-transformatsiya-yaki-mozhlyvosti-vidkryvayutsya-pered-biznesom/ (date of access: 01.10.2024).

3. Yurasov S. «Kyivstar» khotily znyshchyty. Nash velykyi rozbir, yak tse mohlo statysia [«Kyivstar» Was Meant to Be Destroyed. Our In-depth Analysis of How It Could Have Happened]. dev.ua. URL: https://dev.ua/news/kyivstar-1702659220 (date of access: 01.10.2024).

4. Bandura R., Staguhn J. Digital will drive ukraine's modernization. Center for Strategic and International Studies. URL: https://www.csis.org/analysis/digital-will-drive-ukraines-modernization (date of access: 01.10.2024).

5. Harris C. 50 cloud security stats you should know in 2024. Expert Insights. URL: https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/ (date of access: 01.10.2024).

6. Iqra Naseer. AWS cloud computing solutions: optimizing implementation for businesses. *Statistics, computing and interdisciplinary research*. 2023. Vol. 5, No. 2. Pp. 121 – 132. URL: https://doi.org/10.52700/scir.v5i2.138 (date of access: 01.10.2024).

7. Rupa C., Greeshmanth, Shah M. A. Novel secure data protection scheme using Martino homomorphic encryption. *Journal of cloud computing*. 2023. Vol. 12. No. 1. URL: https://doi.org/10.1186/s13677-023-00425-7 (date of access: 01.10.2024).

8. The future of cloud security: 20 statistics & trends to track. CyberTalk. URL: https://www.cybertalk.org/2024/01/24/the-future-of-cloud-security-20-statistics-trends-to-track/ (date of access: 01.10.2024).

СТАТТЯ НАДІЙШЛА 20.10.24.
ОПУБЛІКОВАНА В АВТОРСЬКІЙ РЕДАКЦІЇ.