НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

СУВЕРЕННІ ХМАРНІ ІНФРАСТРУКТУРИ ЯК ОСНОВА ЦИФРОВОГО СУВЕРЕНІТЕТУ

Чанишев Рашид

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Поняття суверенна хмара (sovereign cloud) з'явилося не так давно. Під цим терміном розуміється створення спеціальної інфраструктури, призначеної для забезпечення відповідності використовуваних у конкретній країні сервісів хмарних обчислень певному набору вимог.

При цьому необхідно враховувати, що сам термін «суверенна хмара» може використовуватися в різних контекстах — як позначення технологічного сервісу, архітектурної або економічної моделі, а також як характеристика певної державної або регіональної політики.

Необхідність створення суверенних хмар обумовлена потребою в забезпеченні контролю над даними, що розміщуються і обробляються в хмарних сервісах, оскільки сама модель хмарних обчислень передбачає зберігання інформації у віддалених центрах обробки даних (ЦОД). При цьому центри обробки даних можуть фізично розташовуватися за межами юрисдикцій держав, в яких знаходяться користувачі відповідних хмарних послуг, що істотно ускладнює їх контроль над інформацією, що зберігається і обробляється в таких центрах.

Наразі більша частина хмарних обчислювальних ресурсів перебуває у власності та під управлінням кількох великих компаній світового рівня, таких як Amazon Web Services, Microsoft Azure та Google Cloud Platform (усі — США, сумарна частка американських компаній на світовому ринку становить 70%). Такі компанії відносять до категорії т.з. глобальних гіперскейлерів (hyperscalers, «гіпермасштабованість»). Ці компанії мають можливість надавати доступ до хмарних ресурсів практично в необмежених обсягах завдяки наявності безлічі великих центрів обробки даних, розподілених по всьому світу, а також за рахунок використання апаратних і програмних технологій власної розробки. Гіперскейлери здатні масштабувати свою інфраструктуру до рівнів, недосяжних для звичайних постачальників хмарних послуг. Саме гіперскейлери формують основу глобального ринку хмарних сервісів і забезпечують роботу більшості цифрових платформ, сервісів і додатків.

Оскільки діяльність гіперскейлерів регулюється законодавством тих країн, в яких вони зареєстровані (а це насамперед США), існує ризик того, що державні органи цих країн можуть у будь-який момент отримати доступ до будь-яких даних в ЦОД на підставі свого власного національного законодавства (наприклад, таких законів, як американський CLOUD Act - Федерального закону США, прийнятого в 2018 році, який регулює порядок

отримання американськими правоохоронними органами доступу до даних, що зберігаються у постачальників хмарних послуг, незалежно від того, чи знаходяться ці дані на території США або за її межами).

CLOUD Act має екстериторіальну дію і може мати пріоритет над місцевими законами про захист даних, якщо запитувана інформація пов'язана з кримінальним розслідуванням, що зачіпає інтереси США. Його положення застосовуються незалежно від фізичного місцезнаходження даних, за умови, що постачальник хмарних послуг зареєстрований у США або здійснює діяльність у правовому полі Сполучених Штатів. Цей Закон надає американській владі право отримати доступ до персональних, корпоративних і навіть конфіденційних даних на підставі судового ордера, причому без обов'язкового повідомлення зацікавлених користувачів або регулюючих органів інших країн [1].

Однак це докорінно суперечить законодавству інших країн. Наприклад, стаття 48 Загального регламенту ЄС щодо захисту персональних даних (GDPR) визначає, що судові розпорядження або вимоги державних органів третіх країн (наприклад, США) можуть бути визнані дійсними в ЄС тільки за наявності відповідної міжнародної угоди, такої як Договір про взаємну правову допомогу (MLAT) [2].

Однак закон CLOUD Act фактично обходить механізм MLAT, надаючи американським властям можливість безпосередньо запитувати дані у компаній, що підпадають під юрисдикцію США, незалежно від того, де фізично знаходяться дані і чи передбачені такі запити міжнародними угодами.

Правова невизначеність, що виникає в такій ситуації, прямо зачіпає питання цифрового суверенітету, оскільки не дозволяє однозначно визначити, правові норми якої юрисдикції — національної чи іноземної — регулюють можливість доступу до даних, що зберігаються у глобальних хмарних провайдерів.

Саме ця правова колізія стала одним із ключових факторів формування концепції «суверенних хмар», що дозволяє визначити та розробити механізми контролю над доступом до даних та їх використанням.

У звіті британської аналітичної компанії Omdia «Omdia Market Radar: Sovereign Cloud 2025» представлена шестирівнева модель можливих реалізацій концепції «суверенної хмари» [3].

Рівень 1 — «Data Residency» (вимога до територіального розміщення даних). На цьому рівні передбачається зобов'язання провайдера хмарних послуг забезпечувати зберігання даних виключно в дата-центрах, розташованих на території відповідної країни. При цьому оперативне управління інфраструктурою та ключовими сервісами може повністю залишатися у віданні зовнішнього постачальника.

Рівень 2 — «Data Processing» (вимога обробки даних всередині національної юрисдикції). На цьому рівні передбачається обов'язкове виконання всіх операцій з обробки даних в межах юрисдикції конкретної держави, що дозволяє знизити ризики несанкціонованого доступу або втручання з боку інших держав. При цьому управління платформою і частиною інфраструктурних процесів все ще може залишатися у віданні зовнішнього постачальника.

Рівень 3 — «Data Privacy» (контроль доступу до даних і захист від зовнішнього втручання). На цьому рівні вимоги суверенітету виходять за рамки фізичного розміщення та обробки даних і включають забезпечення суворих механізмів захисту конфіденційності. Хмарний провайдер зобов'язаний гарантувати, що доступ до даних може здійснюватися виключно уповноваженими суб'єктами, які знаходяться в межах відповідної юрисдикції.

Рівень 4 — «Generated Data Access & Control» або «Cloud Resiliency» (доступ і контроль над створюваними даними та стійкість хмари). На цьому рівні суверенність охоплює не тільки вихідні дані, але й похідні дані, що генеруються в процесі роботи хмарних сервісів: такі, наприклад, як журнали подій, метадані, системні логи, дані аналітики, дані моніторингу, телеметрії та інші дані, пов'язані з експлуатацією та адмініструванням хмарного середовища.

Рівень 5 — «Cloud as Critical Infrastructure» (хмара як критична інфраструктура). На цьому рівні хмарна платформа розглядається як елемент критичної інформаційної інфраструктури держави, нарівні з енергетичними, транспортними, фінансовими та комунікаційними системами. Внаслідок цього до хмари висуваються підвищені вимоги в частині безпеки, стійкості, управління та відповідності національному законодавству.

Рівень 6 — «Self-sufficient Cloud» або «Operational Jurisdiction» (повний операційний суверенітет, контроль ланцюгів поставок та експлуатація на рівні держави). Цей рівень являє собою максимальний ступінь суверенітету хмарної інфраструктури, при якому держава отримує повний контроль над усіма аспектами роботи хмари — від апаратних компонентів до експлуатаційних процесів і оперативного управління.

В рамках запущеної в 2019 році франко-німецької ініціативи GAIA-X AISBL було покладено початок побудові федеративної хмарної інфраструктури ЄС. [4]

За даними звіту Omdia, на даний час позиція, яку займає суверенна хмара ЄС, відповідає лише 3 рівню («Data Privacy») даної моделі. При цьому реалізації повноцінної суверенної хмари в ЄС перешкоджає висока фрагментарність нормативного середовища безлічі держав, що входять до нього.

Однак справжній цифровий суверенітет не може бути забезпечений, поки управління даними залишається у постачальників. Формальне перенесення зберігання даних в ЦОД, територіально розташованих в країнах ЄС, не усуває юридичних ризиків і проблеми безпеки даних, створюючи лише видимість контролю. Справжній суверенітет даних може бути досягнутий лише при використанні власної європейської інфраструктури, доповненої використанням шифрування даних на стороні клієнта, використанням відкритого програмного забезпечення і моделей нульової довіри. Тільки такий комплекс заходів дозволить гарантувати захист даних і створити повноцінне суверенне хмара.

Список використаних джерел

1. OpenCloud. US law in European data centres? The CLOUD Act makes it possible. [Електронний ресурс]. URL: https://opencloud.eu/en/the-cloud-act-makes-it-possible (дата звернення: 10.11.2025).
2. Art. 48 GDPR: Transfers or disclosures not authorised by Union law. [Електронний ресурс]. URL: https://gdpr-info.eu/art-48-gdpr/ (дата звернення: 10.11.2025).
3. Навігація в майбутньому цифрового суверенітету. Omdia Market Radar: Sovereign Cloud 2025. [Електронний ресурс]. URL: https://discover.vultr.com/omdia-sovereign-cloud-2025 (дата звернення: 11.11.2025).
4. Чанишев Р.І. Федеративна європейська інфраструктура даних Gaia-X як інструмент технологічного суверенітету Європи: досвід для України. *Системи та технології*. 2022. №2 (64). С. 48-55. DOI https://doi.org/10.32782/2521-6643-2022.2-64.6/.
5. European Cloud services operate in a largely fragmented environment that poses major challenges in terms of complexity, performance and security [Електронний ресурс]. URL: https://surl.li/kwwbph (дата звернення: 11.11.2025).

Ключові слова: sovereign cloud, цифровий суверенітет, юрисдикція даних, гіперскейлери, моделі можливих реалізацій концепції «суверенної хмари», досвід побудови суверенного хмарного сервісу в ЄС.
Keywords: sovereign cloud, digital sovereignty, data jurisdiction, hyperscalers, models of possible implementations of the “sovereign cloud” concept, experience in building a sovereign cloud service in the EU.

ГРАФОВІ МОДЕЛІ ДЛЯ ВАЛІДАЦІЇ ВРАЗЛИВОСТЕЙ

Денисюк Владислав

Національний технічний університет «Харківський Політехнічний Інститут», аспірант кафедри кібербезпеки

Традиційні методи виявлення та валідації вразливостей – статичний аналіз, динамічне тестування, сканування забезпечують лише локальний погляд на безпеку інформаційної системи. Вони визначають наявність

ЗМІСТ