

УДК 342.371.64:378.14

DOI <https://doi.org/10.24144/2307-3322.2025.88.3.9>

СТАНДАРТИЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

Хімко Я.П.,

*аспірант кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ*

Хімко Я.П. Стандартизація інформаційної безпеки хмарних сервісів.

У статті розглянуто стандартизацію інформаційної безпеки хмарних сервісів. Актуальність характеризується необхідністю вивчення стандартів, які визначають організаційні, технічні та програмні аспекти інформаційної безпеки. Метою статті є формування наукового уявлення про природу та особливості стандартизації технічного регулювання та практичного втілення хмарних сервісів. Методологія дослідження включає загальнонаукові методи наукового пізнання, такі як аналіз, синтез, узагальнення, логічний метод, індукція, дедукція, класифікація, аналогія; приватно-наукові та спеціальні методи: порівняльно-правовий, формально-юридичний і інші методи дослідження. Об'єктом дослідження є правові відносини, що виникають під час стандартизації інформаційної безпеки хмарних сервісів. Предметом статті є норми законодавства України та низки зарубіжних держав, що регулюють відносини з приводу стандартизації інформаційної безпеки хмарних сервісів. Зазначено, що хмарні технології – це організаційна модель віддаленого використання елементів інформаційних систем, у зв'язку з чим дослідження інформаційної безпеки хмарних сервісів охоплює відносини забезпечення конфіденційності, цілості інформації, що знаходиться у хмарних сховищах. Об'єкт стандартизації інформаційної безпеки хмарних сервісів характеризується комплексністю, включає технологічні та технічні параметри безпеки інформаційних систем (інформаційні технології, технічні засоби та дані). Стандартизація передбачає прийняття стратегії правового регулювання відносин, що формуються під час використання хмарних технологій у контексті забезпечення інформаційної безпеки. Міжнародне співробітництво у сфері стандартизації інформаційної безпеки хмарних сервісів передбачає вироблення єдності підходів до регулювання конфіденційності, ідентифікації, доступу до даних. Стандарти установлюють вимоги дотримання запобіжних заходів при користуванні хмарною інформаційною системою (забезпечення конфіденційності паролів, запобігання несанкціонованому доступу до електронно-обчислювальних засобів, уважність до налаштувань доступу інформації).

Ключові слова: інформація, доступність, загрози, конфіденційність, послуги, цілісність, інформаційно-комунікаційні технології.

Khimko Ya.P. Standardization of information security of cloud services.

The article considers the standardization of information security of cloud services. The relevance is characterized by the need to study standards that determine the organizational, technical and programmatic aspects of information security. The purpose of the article is to form a scientific understanding of the nature and features of standardization of technical regulation and practical implementation of cloud services. The research methodology includes general scientific methods of scientific knowledge, such as analysis, synthesis, generalization, logical method, induction, deduction, classification, analogy; private scientific and special methods: comparative legal, formal legal and other research methods. The object of the study is legal relations that arise during the standardization of information security of cloud services. The subject of the article is the norms of the legislation of Ukraine and a number of foreign states that regulate relations regarding the standardization of information security of cloud services. It is noted that cloud technologies are an organizational model of remote use of elements of information systems, in connection with which the study of information security of cloud services covers the relations of ensuring confidentiality, integrity of information located in cloud storages. The object of standardization of information security of cloud services is characterized by complexity, includes technological and technical parameters of information system security (information technologies,

technical means and data). Standardization involves the adoption of a strategy for legal regulation of relations that are formed during the use of cloud technologies in the context of ensuring information security. International cooperation in the field of standardization of information security of cloud services involves the development of unity of approaches to regulating confidentiality, identification, and access to data. The standards establish requirements for compliance with precautionary measures when using a cloud information system (ensuring the confidentiality of passwords, preventing unauthorized access to electronic computing facilities, paying attention to information access settings).

Key words: information, availability, threats, confidentiality, services, integrity, information and communication technologies.

Постановка проблеми. Застосування хмарних технологій є одним із компонентів досягнення цілей сталого розвитку, надаючи широкі можливості в галузі зберігання, обробки даних і надання послуг користувачеві незалежно від громадянства та ступеня розвитку держави. Хмарні послуги пропонують майже всі загальновизнані ІТ-вендори. Однак під час використання хмарних сервісів виникають ризики, пов'язані з інформаційною безпекою даних: конфіденційністю, цілісністю та доступністю інформації. Необхідно розуміти та враховувати вразливості хмарних сервісів до різних загроз і атак зловмисників. Це потребує підвищеної уваги до проблеми інформаційної безпеки хмар.

Мета дослідження – розгляд стандартизації інформаційної безпеки хмарних сервісів.

Стан опрацювання проблематики. Вклад у розвиток досліджень забезпечення інформаційної безпеки хмарних технологій внесли праці: В. Бикова, Т. Вакалюка, А. Манна, Л. Соколової, С. Сисоевої, С. Сейтвелієвої, А. Стрюкаа, Ю. Трис, М. Шишкіної, А. Яцишин і інших вчених. Розвиток інформаційно-комунікаційних технологій вимагає проведення досліджень у сфері стандартизації забезпечення інформаційної безпеки.

Виклад основного матеріалу. Головними критеріями під час вибору хмарних сервісів для юридичних осіб, які працюють із критичною інформацією, є надійність і безпека надання послуг зберігання та обробки даних. Хмарні системи мають захисні контури на всіх рівнях, що приваблює та дає впевненість суб'єктам господарювання щодо забезпечення інформаційної безпеки даних. Одним з зазначених аспектів є помилки в налаштуваннях ІАМ (управління ідентифікацією і доступом). Це спричиняє інциденти інформаційної безпеки у хмарі вказує на необхідність ретельного керування доступом та ідентифікацією у хмарних середовищах. Але не тільки конкретна конфігурація управління ідентифікацією та доступом, тип сервісу, модель хмари, що використовується (приватна, колективна / суспільна, публічна / загальнодоступна, гібридна хмара) значною мірою впливають на рівень потенційного збитку, який буде мати суб'єкт господарювання в результаті наслідків ризиків, які є у хмарних сервісах.

Вирішення проблеми зниження ризиків і мінімізації можливих збитків забезпечується активним впровадженням системи безпеки. Система безпеки – це не тільки правильне управління ІАМ, але й використання багатьох різноманітних механізмів, що використовуються для забезпечення безпеки не інформаційно-комунікаційних системах. Регулярне резервування даних і проведення аудитів безпеки, використання шифрування даних – це абетка інформаційної безпеки. Одна з головних умов підтримки інформаційної безпеки – це забезпечення дотримання нормативних і законодавчих вимог та стандартів.

У сучасному інформаційному просторі, де постійно з'являються нові загрози, класичні загрози вдосконалюються і ускладнюються, стандартизація відіграє важливу роль у забезпеченні ефективного захисту даних і забезпеченні надійності хмарних послуг, оскільки в них відображені найкращі практики, техніки, процедури та вимоги інформаційної безпеки світової спільноти.

Стандартизація інформаційної безпеки – це процес розробки та дотримання уніфікованих стандартів і нормативів у галузі інформаційної безпеки. Метою стандартизації є забезпечення єдиних вимог та методології для захисту інформації та інформаційних послуг від загроз і ризиків [1, с. 82]. Це стосується хмарних сервісів. Стандарт інформаційної безпеки – це встановлений набір норм, правил, вимог, розроблених для забезпечення захисту інформації та даних від загроз, для управління ризиками в галузі інформаційної безпеки. Ці стандарти створюються з метою надання підприємствам, установам, організаціям (далі – організаціям), індивідуальним користувачам технік, принципів і методів для забезпечення конфіденційності, цілісності та доступності інформації.

Стандарти інформаційної безпеки включають рекомендації з управління та захисту даних, принципи автентифікації і авторизації, вимоги до фізичної та логічної безпеки, заходи запобігання та реагування на кібератаки.

Міжнародний стандарт – це документ з правилами, нормами чи вимогами, розроблений міжнародними організаціями та затверджений за Міждержавною радою із стандартизації, метрології і сертифікації [2]. Ці стандарти розробляються з метою єдиного підходу та узгодженості у різних галузях, щоб полегшити взаємодію та обмін інформацією між учасниками з різних країн.

Національний стандарт – це стандарт, прийнятий уповноваженим органом зі стандартизації конкретної держави та чинний на її території [2].

У сфері інформаційної безпеки хмарних сервісів важливе місце займають організації стандартизації. Ці організації розробляють документи, що визначають вимоги та методології у сфері безпеки інформації, що сприяє розвитку єдиних стандартів та нормативів. Діапазон документів широкий: починаючи з базових стандартів безпеки та керівних принципів для забезпечення конфіденційності, цілісності та доступності даних у хмарних середовищах.

Світовими провідними організаціями, що займаються питаннями безпеки в хмарі, є CSA, ENISA і NIST. Кожна з організацій створила відповідний документ з класифікацією всіх існуючих проблем інформаційної безпеки в хмарі.

EuroCloud є європейською асоціацією, яка займається хмарним технологіям і послугам [3]. Вона об'єднує підприємства, що займаються хмарними обчисленнями, з метою сприяння розвитку, впровадженню та популяризації хмарних технологій у європейських країнах. EuroCloud активно працює над стандартизацією у сфері хмарних технологій, пропонуючи правила та рекомендації для покращення сумісності та безпеки. Її основне завдання полягає у забезпеченні відкритого доступу до хмарних ресурсів для досліджень. EuroCloud об'єднує установи та лабораторії, надаючи вченим доступ до великих обчислювальних ресурсів та ресурсів сховища. Організація бере активну участь у проєктах та дослідницьких ініціативах, спрямованих на розвиток хмарних технологій, та сприяє встановленню технічних стандартів у цій галузі. Підтримує співпрацю з науковою спільнотою, підтримує поширення знань та проведення наукових досліджень у галузі хмарних обчислень.

Міжнародна спілка електрозв'язку (International Telecommunication Union – ITU) – це міжнародна організація, що об'єднує держави та компанії для розробки стандартів та регулювання в галузі телекомунікацій [4]. ITU був створений у 1865 році та є спеціалізованим агентством Організації Об'єднаних Націй.

Сектор стандартизації телекомунікації (ITU-T), що входить до складу організації ITU, розробив низку стандартів та рекомендацій у галузі безпеки хмарних сервісів: Cloud computing Infrastructure requirements -Cloud computing, Overview and high-level requirements of distributed cloud, Security frame work for cloud computing, Cloud Computing Framework & high-level requirements і інші.

До основних стандартів інформаційної безпеки, орієнтованих на хмарні сервіси включені ISO/IEC27017 та ISO/IEC27018 Інформаційна технологія сервіс. Міжнародний стандарт надає рекомендації з управління інформаційною безпекою хмарних сервісів на основі стандарту ISO/IEC27002. Стандарт розроблений до застосування для постачальників хмарних послуг (CSP), та для кінцевих користувачів з метою забезпечення безпеки хмарного середовища шляхом впровадження додаткових контрольних заходів і рекомендацій, орієнтованих на специфічні аспекти безпеки у хмарних середовищах [5].

Стандарт включає набір керівних принципів і механізмів контролю, які організації можуть застосовувати при використанні хмарних послуг. Він надає конкретні рекомендації безпечного використання хмарних сервісів, охоплюючи управління доступом, шифрування даних, моніторинг, управління інцидентами.

ISO/IEC 27018:2019 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) в громадських clouds acting як PII processors. Це міжнародний стандарт із рекомендаціями та практиками з управління інформаційною безпекою у хмарних послугах з урахуванням захисту персональних даних.

У центрі уваги стандарту ISO/IEC27018 – забезпечення конфіденційності при обробці персональних даних у хмарних середовищах. Основні положення стандарту включають заходи контролю та захисту персональних даних, обробка яких здійснюється в хмарі. Визначено вимоги до хмарних постачальників послуг для забезпечення прозорості та контролю за даними клієнтів, у

тому числі заходи щодо шифрування, забезпечення доступності, регулювання субпідрядників. Цей стандарт призначений для покращення довіри споживачів до хмарних послуг, особливо щодо обробки персональних даних. Він надає для хмарних постачальників рекомендації щодо ефективного управління інформаційною безпекою та захистом даних клієнтів відповідно до вимог конфіденційності [8].

Існують інші стандарти ISO/IEC, які стосуються хмарних середовищ і торкаються питань інформаційної безпеки хмарних систем: ISO/IEC 23751:2022, ISO/IEC 29151:2017, ISO/IEC 19944:2020, ISO/IEC 22624:20 .

Документи описує п'ять основних характеристик, три моделі обслуговування та чотири моделі розгортання хмарних обчислень. До основних характеристик відносяться самообслуговування на запит, широкий мережевий доступ, пулінг ресурсів, швидка еластичність та вимірюване обслуговування.

Три моделі обслуговування включають програмне забезпечення як послугу (SaaS), платформу як послугу (PaaS) та інфраструктуру як послугу (IaaS). Чотири моделі розгортання – це приватна хмара, публічна хмара/загальнодоступна, колективна/суспільна хмара та гібридна хмара.

Cloud Computing Synopsis and Recommendations спеціальна публікація NIST 800-146, під назвою «Короткий виклад та рекомендації щодо хмарних обчислень», випущена NIST (Національний інститут стандартів і технологій США) забезпечує короткий огляд і рекомендації щодо хмарних обчислень.

У документі наведено основні аспекти хмарних обчислень, включаючи їх визначення, основні характеристики, моделі обслуговування та моделі розгортання. Містить рекомендації для організацій щодо ефективного використання хмарних обчислень, застереження від ризиків, пов'язаних з ними. NIST 800-146 служить довідковим ресурсом для тих, хто цікавиться основами хмарних обчислень, надає рекомендації для забезпечення безпеки та ефективності використання хмарних ресурсів [6].

Національний Institute of Standards and Technology Special Publication 500-292. NIST Cloud Computing Reference Architecture. NIST 500-292 представляє документ, який описує архітектурний підхід до хмарних обчислень у межах стандартів NIST. Цей документ надає основну архітектурну модель, яка допомагає організаціям краще зрозуміти та впроваджувати хмарні обчислення. Він включає ключові компоненти, зв'язки та процеси, що характеризують архітектуру хмарних обчислень.

Специфікація NIST 500-292 призначена для забезпечення загального розуміння термінів і концепцій, пов'язаних з хмарними обчисленнями, може бути використана як основа для розробки та впровадження хмарних рішень відповідно до принципів NIST [7].

Наведені вище стандарти у сфері хмарних обчислень відіграють важливу роль у формуванні єдиного підходу до безпеки та стандартизації у використанні хмарних сервісів. Ці стандарти надають рекомендації, тактики, техніки, процедури та вимоги, але й сприяють підвищенню довіри до хмарних технологій. Їхнє активне впровадження в практику забезпечує узгодженість і безпеку у розгортанні хмарних систем.

Національна економічна стратегія на період до 2030 року передбачає розвиток хмарних технологій, наголошує на збільшенні частки використання хмарних сервісів в інформаційно-комунікаційному забезпеченні діяльності органів влади, реалізація сервісної моделі надання хмарних послуг суб'єктах бізнесу [8]. Закон України «Про хмарні послуги» відповідає вимогам Європейського Союзу, що дає змогу використання хмарних послуг у всіх галузях економіки [9].

Проводиться робота з гармонізації та адаптації затребуваних міжнародних стандартів з IT-технологій, у тому числі щодо безпеки хмарних сервісів. Одним із стандартів інформаційної безпеки хмарних сервісів, є стандарт ISO/IEC 27017:2017. В Україні діє ДСТУ ISO/IEC 27017:2017 [10]. Зміст стандарту включає аспекти інформаційної безпеки: починаючи від організації інформаційної безпеки та закінчуючи криптографією. Це враховує забезпечення безперервності ділової діяльності та відповідності законодавчо-нормативним вимогам. Стандарт включає програми з набором заходів контролю та управління для хмар.

У 2016 році вперше запроваджено стандарти з інформаційної безпеки та хмарних послуг ДСТУ ISO/IEC TR 26905:2016 (ISO/IEC TR 26905:2006, IDT) ДСТУ ISO/IEC 26907:2016 (ISO/IEC 26907:2009, IDT) ДСТУ ISO/IEC 26908:2016 (ISO/IEC 26908:2009, IDT) кількістю 26 [11].

Для спільного використання ресурсів та віддаленого доступу до даних в Україні існує ряд хмарних сервісів, серед них Диск Google, OneDrive, Dropbox, Box, Mega, Sugar Sync та інші.

Забезпечити надійний захист даних і застосунків у хмарі завжди було непростим і з року у рік ця задача ускладнюється. Адже, з одного боку, все більше навантажень мігрує на хмарні платформи, а з іншого – зловмисники стають дедалі винахідливішими. Проте, технології кібербезпеки також активно розвиваються [12]. Якщо порівняти вимоги до забезпечення інформаційної безпеки, які мали місце у 2015 році з вимогами поточного періоду то витрати на забезпечення інформаційної безпеки значно зросли, обладнання у технічному плані ускладнилось, але проблема залишається актуальною [13, с. 270; 14, с. 75].

Інформаційну безпеку підприємства в умовах війни слід трактувати ширше. Під час воєнного стану доцільно поширити організаційно-правові засади інформаційної безпеки підприємств за межі інформаційного права та використання імперативних норм адміністративного та кримінального права [15, с. 173].

У даний час проблеми інформаційної безпеки хмарних технологій вирішуються за рахунок ряду концепцій. Концепція ZTS («безпека з нульовим рівнем довіри»), яка допомагає протидіяти прихованим та невідомим загрозам.

Стандарт NIST 800-200 з 2021 року застосовують всі Федеральні агентства США при необхідності реалізації ZTS. Концепція Multi-Factor Authentication використовується у процесі реалізації системи доступу з «нульовою довірою» суб'єкти господарювання та державні установи. MFA значно знижує ризик несанкціонованого доступу.

Застосовується для захисту хмарних інфраструктур штучний інтелект для виявлення та усунення кіберзагроз AI-Driven Threat Detection and Response або AI XDR. Штучний інтелект застосовується для аналізу даних з метою виявлення аномалій, прогнозування можливих векторів атак і способів швидшої протидії зловмисникам.

Технологія конфіденційних обчислень (Confidential Cloud Computing) базується на тому, що для обробки критичних даних у процесорі на апаратному рівні створюється спеціальне захищене середовище – TEE (hardware-based Trusted Execution Environment), до якого мають доступ авторизовані програми.

На ринку почали з'являтися комплексні рішення безпеки, адаптовані для роботи з хмарними платформами – Cloud Native Application Protection Platforms. Перевагою CNAPP є забезпечення можливості реагування на загрози, що виникають від розробки до середовища виконання [16].

Висновки. В інформаційному суспільстві важливість та актуальність стандартизації інформаційної безпеки хмарних сервісів стають важливими аспектами розвитку цифрових технологій. Організації, що займаються стандартизацією у сфері хмарних сервісів, відіграють ключову роль у розробці стандартів, спрямованих на безпеку, сумісність та результативність хмарних рішень. Їхня робота з розробки стандартів сприяє створенню єдиних підходів до безпеки інформації в хмарних середовищах, взаєморозумінню між постачальниками та споживачами хмарних сервісів. Діяльність спрямована не тільки на розробку стандартів, а й на постійне оновлення і адаптацію до умов інформаційної безпеки, що змінюються, до появи нових загроз і ризиків, на підвищення кваліфікації фахівців у цій галузі. Визнані стандарти здатні забезпечити високий рівень довіри та надійності у сфері хмарних обчислень, особливо для споживачів України в умовах воєнного стану.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Дикий О., Флюнт М. Стандарти інформаційної безпеки: компаративне дослідження. *Право та державне управління*. 2019. № 2 (35). Том 1. С. 80–87.
2. Про стандартизацію: Закон України від 05.06.2014 р. № 1315-VII. URL. <https://zakon.rada.gov.ua/laws/card/1315-18>.
3. EuroCloud Trusted Digital Competence Platform. URL. <https://eurocloud.org>.
4. Міжнародний союз електрозв'язку (MCE). URL. <https://geneva.mfa.gov.ua/posolstvo/2616-itu>.
5. Використання комерційних хмарних технологій для обробки даних державних реєстрів України. Міжнародна фундація виборчих систем, 2023. URL. <https://www.ifesukraine.org/wp-content/uploads/2024/01/ifes-ukraine-the-use-of-commercial-cloud-technologies-for-processing-data-from-state-registers-of-ukraine-1.pdf>.
6. Cloud Computing Synopsis and Recommendations. URL. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf>.

7. NIST Cloud Computing Reference Architecture. URL. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf>.
8. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL. <https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text>.
9. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX. URL. <https://zakon.rada.gov.ua/laws/show/2075-20#Text>.
10. Про прийняття національних нормативних документів, гармонізованих з міжнародними та європейськими нормативними документами, скасування чинності національних нормативних документів та змін до національних нормативних документів: Наказ державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 19.12.2017 р. № 428. URL. <https://zakon.rada.gov.ua/rada/show/v0428774-17#Text>.
11. Про прийняття національних стандартів України, змін та поправок до національних стандартів України, гармонізованих з міжнародними нормативними документами: Наказ державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 07.10.2016 р. № 307. URL. <https://zakon.rada.gov.ua/rada/show/v0307774-16#Text>.
12. Кібербезпека у хмарі – п'ять актуальних технологій у 2024 році. 24.05.2024. URL. <https://denovo.ua/blog/cloud-security-top5-2024>.
13. Середа В.В., Ковалів М.В., Єсімов С.С., Гурковський М.П. Правові основи захисту України від зовнішньої та внутрішньої агресії: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2015. 518 с.
14. Єсімов С.С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. *Наукові записки Львівського університету бізнесу та права*. 2013. Випуск 11. С. 73–76.
15. Melnychenko B., Tsebenko S., Khomyshyn I., Sirant M., Yesimov S. Organizational and legal principles of information security of enterprises in the conditions of martial law in Ukraine. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 2024, № 1. С. 167–174.
16. What is CNAPP? [Cloud-Native Application Protection Platform].