КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1358
УДК 004.056.5

Педченко Євгеній Максимович
доктор філософії, доцент
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0001-8436-5792
e.pedchenko@duikt.edu.ua

Іванченко Євгенія Вікторівна
доктор технічних наук, професор, Директор навчально-наукового інституту кібербезпеки та захисту інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-3017-5752
e.ivanchenko@duikt.edu.ua

Іванченко Ігор Сергійович
кандидат технічних наук, доцент, професор
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-3415-9039
i.ivanchenko@duikt.edu.ua

Педченко Марина Максимівна
студентка
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0007-8743-1821
st9763427@stud.duikt.edu.ua

МЕТОДИ ОЦІНЮВАННЯ СТАНУ ЗАХИЩЕНОСТІ МЕРЕЖ І СЕРЕДОВИЩА ЗБЕРІГАННЯ ДАНИХ У ХМАРНИХ СЕРВІСАХ

Анотація. Під час проведеного дослідження представлено критерії та метод оцінювання стану захищеності мереж хмарного сервісу та середовища зберігання даних як ключових лінійних компонентів системи оцінювання кібербезпеки хмарних сервісів. Дослідження виконано на основі розробленої узагальненої математичної моделі оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури. Обґрунтовано актуальність проблеми, пов'язаної зі зростанням кіберінцидентів у хмарних середовищах, що є спричиненими помилками конфігурації під час налаштування хмарних сервісів. Продемонстровано, що мережевий рівень і середовище зберігання даних є критичними складовими хмарної інфраструктури. Виявлено відсутність чітких рекомендацій під час проведеного аналізу існуючих міжнародних стандартів та регламентів щодо захисту хмарних сервісів. Під час представлення результатів дослідження формалізовано модуль оцінювання стану захищеності мережі (параметр N) та модуль оцінювання стану захищеності середовища зберігання даних (параметр S). Для кожного модуля визначено критерії оцінювання, варіанти відповідей та відповідні математичні формули, що детально представляють обсяг оцінювання для кожного хмарного сервісу. Розроблено алгоритмічні моделі для обох модулів, що забезпечують візуальне представлення структури критеріїв оцінювання рівня захищеності хмарних сервісів. Продемонстровано, що отримані значення параметрів N і S впливають на формування рівня кіберзахищеності хмарного сервісу та фінальної рекомендації щодо подальшого використання бізнесом. В дослідженні зазначено можливість практичного застосування розроблених критеріїв і методів, а всі подальші дослідження спрямовані на розробку повноцінного методу оцінювання, визначення вагових коефіцієнтів для отриманих відповідей від аудиторів, формування системи рекомендацій та створення захищеного мережевого застосунку.

Ключові слова: кібербезпека; інформаційна безпека; модель; метод; аудит; оцінювання хмарних сервісів; алгоритмічне забезпечення; мережа; зберігання даних.

ВСТУП

Стрімке поширення хмарних обчислень супроводжується зростанням кіберінцидентів, пов'язаних із помилками конфігурації, недостатнім захистом на мережевому рівні та проблемами із використанням застарілих методів шифрування в середовищі зберігання даних [1]. Опираючись на сучасні дослідження, більшість успішних кібератак на хмарні середовища виникають не через безпосередньо вразливості інфраструктури провайдера, а через некоректні налаштування замовника хмарних сервісів – наявність відкритих портів, відсутність мікро сегментації мережі, публічно доступні сховища даних, застарілі методи шифрування або відсутність резервування [2].

Мережевий рівень і середовище зберігання даних є одними із найкритичніших компонентів хмарної інфраструктури. Мережа є першою лінією захисту від зовнішніх атак (DDoS, сканування портів, експлуатація вразливостей на рівнях L3/L4/L7 моделі OSI), а також забезпечує ізоляцію між різними тенантами та сервісами, розгорнутими на хмарних обчисленнях [3]. Середовище зберігання даних безпосередньо відповідає за конфіденційність, цілісність і доступність інформації, і саме на даному рівні найчастіше фіксуються витоки через публічні бакети, відсутність шифрування даних у стані спокою та в транзиті, відсутність управління ключами шифрування [4].

Постановка проблеми. Попри наявність численних рекомендацій і стандартів (CIS Benchmarks, Microsoft Cloud Security Benchmark, AWS Well-Architected Framework, NIST SP 800-209 тощо), на практиці відсутній стандартизований і формалізований підхід до оцінювання стану захищеності мережі та середовища зберігання даних хмарних сервісів. Більшість існуючих рішень або є занадто загальними (охоплюють усю інфраструктуру), або обмежуються якісними чек-листами без можливості отримати обґрунтований рівень захищеності та чіткі рекомендації щодо покращення рівня захищеності хмарних сервісів.

У зв'язку з цим можна виділити такі ключові проблеми:

1. Відсутність стандартизованих критеріїв і метрик для оцінювання захищеності мережевої інфраструктури хмарних сервісів (захист від DDoS, сегментація, фільтрація трафіку, Zero-Trust підходи).

2. Відсутність стандартизованих критеріїв оцінювання середовища зберігання даних (шифрування at rest / in transit, управління ключами, блокування публічного доступу, резервування та відновлення).

Аналіз останніх досліджень і публікацій. Сучасні дослідження підтверджують, що DDoS-атаки продовжують зростати за частотою та інтенсивністю: у першому кварталі 2025 року Cloudflare зафіксував понад 20 млн атак, що перевищило показники всього 2024 року [5]. При цьому хмарні провайдери пропонують власні механізми захисту (AWS Shield, Azure DDoS Protection, Google Cloud Armor), проте ефективність їх використання залежить від коректності конфігурації з боку замовника, що зазвичай не виконується фахівцями замовників через складнощі налаштувань систем безпеки [6].

Щодо середовища зберігання даних, звіти Datadog (State of Cloud Security 2025) показують, що частка публічно доступних бакетів знижується, однак впровадження блокування публічного доступу все ще не є повсюдним, особливо в Azure [7]. Дослідження також підкреслюють важливість шифрування даних у стані спокою з використанням клієнтських ключів (CMEK/CMK) замість ключів, керованих провайдером [8,9].

Міжнародні стандарти та регламенти (NIST SP 800-209 «Security Guidelines for Storage Infrastructure» [10], CSA Security Guidance v5 [11], Microsoft Cloud Security Benchmark [12]) надають детальні рекомендації щодо мережевої безпеки та захисту даних, проте не пропонують готової системи кількісного оцінювання з можливістю отримання якісного показника та чітких рекомендацій для усунення виявлених прогалин безпеки.

Таким чином, існує потреба у розробці підходу до оцінювання двох лінійних параметрів – стану захищеності мережі хмарного сервісу та стану захищеності середовища зберігання даних – з можливістю формалізації критеріїв оцінювання, обчислення отриманих балів за результатами аудиту і формування практичних рекомендацій для усунення виявлених вразливостей безпеки.

Мета статті. Метою роботи є розробка методу та критеріїв до оцінювання стану захищеності мережі хмарного сервісу та середовища зберігання даних як ключових компонентів системи оцінювання кібербезпеки хмарних сервісів.

Для досягнення мети необхідно визначити критерії оцінювання мережевої захищеності та середовища зберігання даних. На основі визначених критеріїв запропонувати метод оцінювання та запропонувати формули обчислення відповідних показників. Описати послідовність оцінювання та принципи формування рекомендацій на основі отриманих результатів. Для розроблених критеріїв і

методу оцінювання запропонувати алгоритмічну модель, що забезпечить візуальне представлення процесу оцінювання зазначених модулів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Опираючись на проведені дослідження в [13] та представлених всіх кроків проведення оцінювання захищеності хмарних сервісів у [14] – в даній статті буде представлено два модулі оцінювання стану захищеності мережі хмарного сервісу та середовища зберігання даних як ключових компонентів системи оцінювання кібербезпеки хмарних сервісів.

Модуль оцінювання стану захищеності мережі хмарного сервісу (має назву в [13] – «**Network module**», та маркується параметром – **N**) є одним із ключових лінійних компонентів узагальненої математичної моделі оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури. Основним призначенням даного параметру є кількісне визначення рівня захищеності мережевої інфраструктури, що забезпечує функціонування хмарного сервісу в мережі Інтернет та оцінка здатності протидіяти сучасним мережевим кіберзагрозам.

У межах зазначеного модуля здійснюється комплексний аналіз низки взаємопов'язаних характеристик. Зокрема, оцінюється гарантований рівень доступності сервісу (SLA), географічна розподіленість точок присутності постачальника, максимальна пропускна здатність каналів зв'язку, наявність та функціональні можливості рішень захисту від DoS/DDoS-атак (з урахуванням рівнів моделі OSI, на яких реалізовано захист, можливості налаштування правил, підтримки rate-limiting та захисту від різних типів flood-атак). Окрему увагу приділено механізмам управління DNS-записами (включаючи підтримку DNSSEC), засобам балансування навантаження між віртуальними середовищами, забезпеченню доступу до ресурсів виключно через захищені протоколи (SSH, SSL/TLS, IPSec, VPN), застосуванню систем виявлення мережевих аномалій поведінки (NBAD), рішень класу IPS/IDS, а також наявності та конфігурації мережевих екранів для контролю доступу до віртуальних приватних хмар і серверів.

Модуль оцінювання стану захищеності мережі хмарного сервісу з параметром **N** описується наступною узагальненою формулою:

$$\mathbf{N} = \left\{ \bigcup_{j=1}^{m_2} \mathbf{N_j} \right\} = \left\{ \mathbf{N_1}, \mathbf{N_2} \ldots, \mathbf{N_{m_2}} \right\}, \quad (1)$$

де: $\mathbf{N_j} \subseteq \mathbf{N}$ $(j = \overline{1, m_2})$ – j-й параметр відповідає за визначення набору критеріїв оцінюваного хмарного сервісу на мережевому рівні, а m_2 – їх кількість [15].

Зазначений модуль з параметром **N** зі всіма параметрами оцінювання буде мати наступний вигляд відповідно до наданої формули (2):

$$\mathbf{N} = \left\{ \bigcup_{j=1}^{10} \mathbf{N_j} \right\} = \left\{ \mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3}, \mathbf{N_4}, \mathbf{N_5}, \mathbf{N_6}, \mathbf{N_7}, \mathbf{N_8}, \mathbf{N_9}, \mathbf{N_{10}} \right\}, \quad (2)$$

де, відповідно: $\mathbf{N_1}$ = «Виберіть рівень доступності (у %), що гарантує постачальник хмарного сервісу:»; $\mathbf{N_2}$ = «Виберіть кількість країн, в яких присутній постачальник хмарних сервісів:»; $\mathbf{N_3}$ = «Виберіть максимальну пропускну здатність в GB/sec, що забезпечує постачальник хмарних сервісів:»; $\mathbf{N_4}$ = «Хмарний сервіс надає рішення для захисту від DoS/DDoS атак:»; $\mathbf{N_5}$ = «Хмарний сервіс забезпечує рішенням для управління DNS записами:»; $\mathbf{N_6}$ = «Хмарний сервіс забезпечує можливість використання Load-Balancing для балансування навантаження між VPC/VPS:»; $\mathbf{N_7}$ = «Хмарний сервіс забезпечує доступ до розгорнутих VPC/VPS виключно з використанням безпечних методів передачі даних (SSH, SSL/TLS, IPSec, VPN):»; $\mathbf{N_8}$ = «Хмарний сервіс забезпечує можливість використання

NBAD (Network Behavoir Anomaly Detection) рішення для виявлення аномалій (Бот мереж, зловмисного трафіку, шкідливого програмного забезпечення тощо) в сегменті мережі:»; $\mathbf{N_9}$ = «Хмарний сервіс забезпечує можливість використання IPS/IDS рішень:»; $\mathbf{N_{10}}$ = «Хмарний сервіс має вбудований мережевий екран (firewall) для контролю доступу до VPC/VPS:» [16].

Враховуючи те, що у формулі (2) вказані загальні критерії оцінювання мережевого модуля хмарного сервісу у вигляді запитань, то у формулі (3) представлено варіанти відповідей:

$$\mathbf{N} = \left\{\bigcup_{j=1}^{10}\mathbf{N_j}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{2j}} N_{jk}\right\}\right\} = \{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16}\},$$
$$\{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36}\},$$
$$\{N_{41}, N_{42}\}, \{N_{51}, N_{52}\}, \{N_{61}, N_{62}\}, \{N_{71}, N_{72}\}, \{N_{81}, N_{82}\},$$
$$\{N_{91}, N_{92}\}, \{N_{101}, N_{102}\}\}, \quad (3)$$

де: N_{11} = «99.9999% (простій в рік 31,5 секунд)»; N_{12} = «99.999% (простій в рік 5,26 хвилин)»; N_{13} = «99.99% (простій в рік 52,56 хвилин)»; N_{14} = «99.9% (простій в рік 8,76 годин)»; N_{15} = «99% (простій в рік 3,65 днів)»; N_{16} = «90% і менше (простій в рік 36,5 днів)»; N_{21} = «більше 30»; N_{22} = «21-30»; N_{23} = «11-20»; N_{24} = «6-10»; N_{25} = «2-5»; N_{26} = «1»; N_{31} = «301-400 і більше»; N_{32} = «201-300»; N_{33} = «101-200»; N_{34} = «51-100»; N_{35} = «2-50»; N_{36} = «1 і менше»; N_{41} = «Так»; N_{42} = «Ні»; N_{51} = «Так»; N_{52} = «Ні»; N_{61} = «Так»; N_{62} = «Ні»; N_{71} = «Так»; N_{72} = «Ні»; N_{81} = «Так»; N_{82} = «Ні»; N_{91} = «Так»; N_{92} = «Ні»; N_{101} = «Так»; N_{102} = «Ні» [16].

Варто врахувати, що підпараметри N_{41} та N_{51} мають власні уточнюючі запитання по даному модулю, то оновлений варіант модуля представлено у формулі (4):

$$\mathbf{N} = \left\{\bigcup_{j=1}^{10}\mathbf{N_j}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{2j}} N_{jk}\right\}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{2j}}\left\{\bigcup_{l=1}^{m_{2jk}}\mathbf{N_{jkl}}\right\}\right\}\right\} =$$
$$\{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16}\},$$
$$\{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36}\},$$
$$\{\{\mathbf{N_{411}}, \mathbf{N_{412}}, \mathbf{N_{413}}, \mathbf{N_{414}}, \mathbf{N_{415}}, \mathbf{N_{416}}, \mathbf{N_{417}}, \mathbf{N_{418}}, \mathbf{N_{419}}, \mathbf{N_{4110}}, \mathbf{N_{4111}}\}, N_{42}\},$$
$$\{\{\mathbf{N_{511}}\}, N_{52}\}, \{N_{61}, N_{62}\}, \{N_{71}, N_{72}\}, \{N_{81}, N_{82}\},$$
$$\{N_{91}, N_{92}\}, \{N_{101}, N_{102}\},\}, \quad (4)$$

де: $\mathbf{N_{411}}$ = «Рішення для захисту від DoS/DDoS атак:»; $\mathbf{N_{412}}$ = «Виберіть рівні моделі OSI, на яких працює захист від DoS/DDoS атак:»; $\mathbf{N_{413}}$ = «Рішення для захисту від DoS/DDoS атак налаштовується:»; $\mathbf{N_{414}}$ = «Рішення для захисту від DoS/DDoS атак забезпечує попередньо-

налаштованими правила:»; $\mathbf{N}_{415}$ = «Рішення для захисту від DoS/DDoS атак забезпечує можливість створення індивідуальних правил:»; $\mathbf{N}_{416}$ = «Рішення для захисту від DoS/DDoS атак забезпечує можливість в реальному часі відслідковувати об'єм аномального трафіку:»; $\mathbf{N}_{417}$ = «Рішення для захисту від DoS/DDoS атак забезпечує можливість встановлювати власні rate-контролі для окремих IP-адрес/FQDN:»; $\mathbf{N}_{418}$ = «Рішення для захисту від DoS/DDoS атак забезпечує захист від UDP Flood атак:»; $\mathbf{N}_{419}$ = «Рішення для захисту від DoS/DDoS атак забезпечує захист від TCP SYN Flood атак:»; $\mathbf{N}_{4110}$ = «Рішення для захисту від DoS/DDoS атак забезпечує захист від DNS query Flood атак:»; $\mathbf{N}_{4111}$ = «Рішення для захисту від DoS/DDoS атак забезпечує захист від HTTP Flood атак:»; $\mathbf{N}_{5111}$ = «Хмарний сервіс забезпечує захист DNSSEC для рішення DNS» [16].

Оскільки в формулі (4) представлено додаткові критерії для модуля оцінювання стану захищеності мережі хмарного сервісу, то в формулі (5) представлено розширені набори відповідей:

$$\mathbf{N} = \left\{ \bigcup_{j=1}^{10} \mathbf{N}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{2j}} N_{jk} \right\} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{2j}} \left\{ \bigcup_{l=1}^{m_{2jk}} \mathbf{N}_{\mathbf{jkl}} \right\} \right\} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{2j}} \left\{ \bigcup_{l=1}^{m_{2jk}} \left\{ \bigcup_{p=1}^{m_{2jkl}} N_{jklp} \right\} \right\} \right\} \right\}$$

$$\begin{gathered}
\{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16}\}, \\
\{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36}\}, \\
\{\{\{N_{4111}, N_{4112}\}, \{N_{4121}, N_{4122}, N_{4123}, N_{4124}, N_{4125}, N_{4126}, N_{4127}, N_{4128}, N_{4129}\}, \\
\{N_{4131}, N_{4132}\}, \{N_{4141}, N_{4142}\}, \{N_{4151}, N_{4152}\}, \{N_{4161}, N_{4162}\}, \{N_{4171}, N_{4172}\}, \\
\{N_{4181}, N_{4182}\}, \{N_{4191}, N_{4192}\}, \{N_{41101}, N_{41102}\}, \{N_{41111}, N_{41112}\}\}, N_{42}\}, \\
\{\{\{N_{5111}, N_{5112}\}\}, N_{52}\}, \{N_{61}, N_{62}\}, \{N_{71}, N_{72}\}, \{N_{81}, N_{82}\}, \\
\{N_{91}, N_{92}\}, \{N_{101}, N_{102}\}\},
\end{gathered} \tag{5}$$

де: N_{4111} = «Постачається в комплекті»; N_{4112} = «Постачається як окремий платний модуль»; N_{4121} = «Layer 3, 4, 7»; N_{4122} = «Layer 3, 4»; N_{4123} = «Layer 3, 7»; N_{4124} = «Layer 4, 7»; N_{4125} = «Тільки Layer 3»; N_{4126} = «Тільки Layer 4»; N_{4127} = «Тільки Layer 7»; N_{4128} = «На жодному з вище перелічених»; N_{4131} = «Виробником»; N_{4132} = «Замовником»; N_{4141} = «Так»; N_{4142} = «Ні»; N_{4151} = «Так»; N_{4152} = «Ні»; N_{4161} = «Так»; N_{4162} = «Ні»; N_{4171} = «Так»; N_{4172} = «Ні»; N_{4181} = «Так»; N_{4182} = «Ні»; N_{4191} = «Так»; N_{4192} = «Ні»; N_{41101} = «Так»; N_{41102} = «Ні»; N_{41111} = «Так»; N_{41112} = «Ні»; N_{5111} = «Так»; N_{5112} = «Ні» [16].

Для можливості візуального представлення модуля оцінювання стану захищеності мережі хмарного сервісу, а саме розроблених критерії оцінювання та представлення послідовних кроків проведення оцінювання було розроблено алгоритмічне забезпечення, що представлено на Рисунку 1:

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

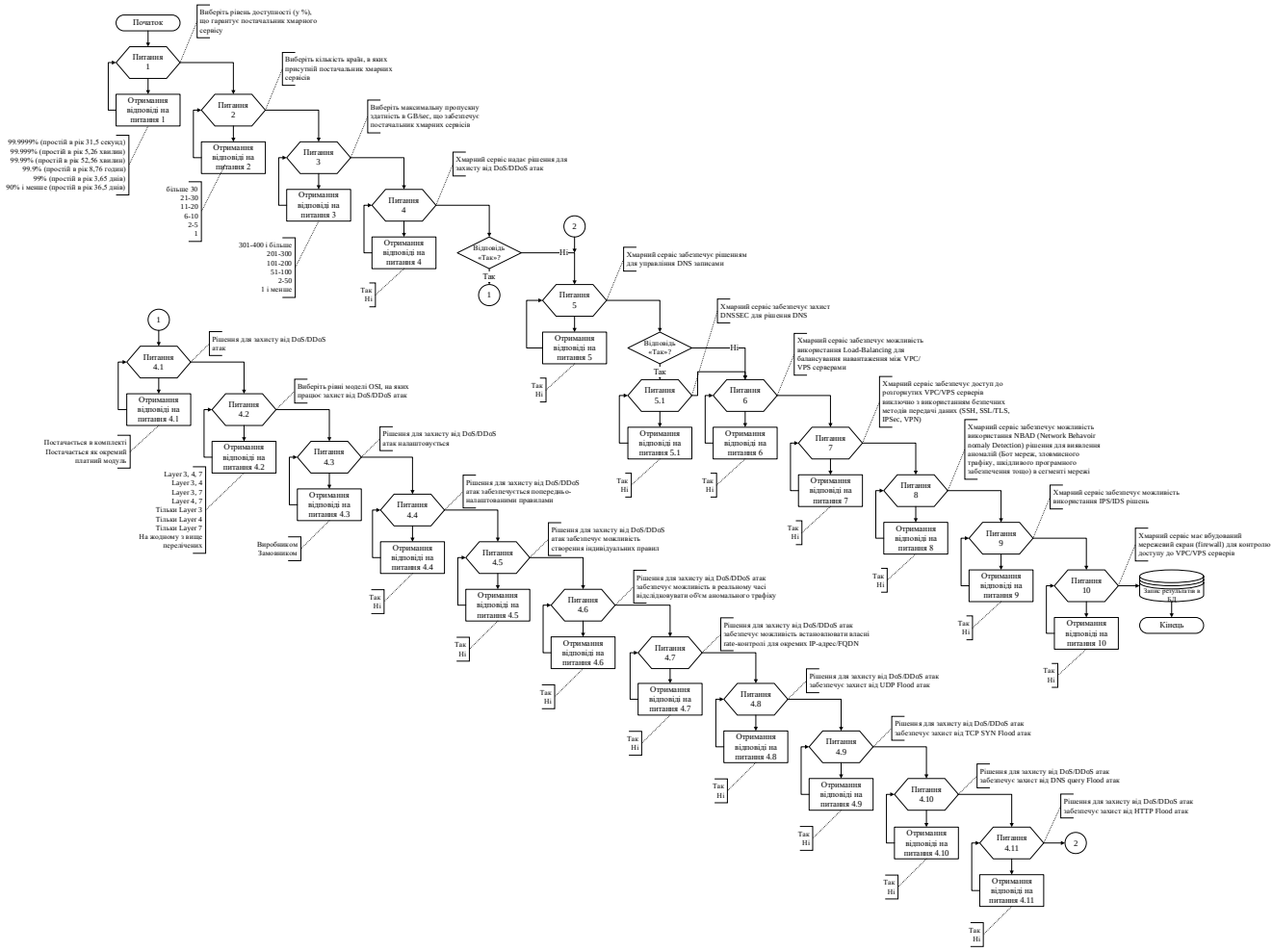

Рис. 1. Загальна структура параметру «N» для оцінювання стану захищеності мережі хмарного сервісу

Модуль оцінювання стану захищеності середовища зберігання даних (має назву в [13] – «**Storage module**», та маркується параметром – **S**) спрямований на визначення рівня захищеності, цілісності, конфіденційності та відмовостійкості систем зберігання даних, що використовуються в межах хмарного сервісу. Модуль дозволяє оцінити можливість систем зберігання даних забезпечувати збереження конфіденційних даних замовника навіть в умовах виникнення збоїв, атак або необхідності швидкого відновлення чи застосування підходу DRP (Data Recovery Plan).

Під час проведення оцінювання проводиться аналіз можливості створення резервних копій (snapshots) та клонів віртуальних середовищ, підтримки різних схем реплікації даних (локальної, регіональної та георозподіленої), реалізації шифрування дискового простору, способи управління криптографічними ключами (включаючи застосування алгоритмів не нижче AES-256), а також відповідність інфраструктури зберігання даних вимогам міжнародних стандартів і регуляторних документів (FIPS 140-2, PCI-DSS, GDPR, FedRAMP, HIPAA/HITECH, серія стандартів ISO 27000). Оцінювання зазначених характеристик надає змогу виявити як сильні сторони системи зберігання, так і потенційні ризики, пов'язані з відсутністю резервування, слабким шифруванням або невідповідністю вимогам регуляторів чи міжнародних стандартів.

Модуль оцінювання стану захищеності середовища зберігання даних **S** описується наступною узагальненою формулою:

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{m_3} \mathbf{S_j} \right\} = \left\{ \mathbf{S_1}, \mathbf{S_2} \ldots, \mathbf{S_{m_3}} \right\}, \quad (6)$$

де: $\mathbf{S_j} \subseteq \mathbf{S}$ $(j = \overline{1, m_3})$ – j-й параметр відповідає за визначення рівня захищеності середовища зберігання даних хмарного сервісу оцінювання якого проводиться, а m_3 – їх кількість [15].

Зазначений модуль з параметром **S** зі всіма параметрами оцінювання буде мати наступний вигляд відповідно до наданої формули (7):

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{10} \mathbf{S_j} \right\} = \left\{ \mathbf{S_1}, \mathbf{S_2}, \mathbf{S_3}, \mathbf{S_4}, \mathbf{S_5}, \mathbf{S_6}, \mathbf{S_7}, \mathbf{S_8}, \mathbf{S_9}, \mathbf{S_{10}} \right\}, \quad (7)$$

де, відповідно: $\mathbf{S_1}$ = «Рішення підтримує метод реплікації даних:»; $\mathbf{S_2}$ = «Рішення підтримує можливість створення резервних копій (snapshots) VPC/VPS, розгорнутих на ресурсах хмарного сервісу:»; $\mathbf{S_3}$ = «Рішення підтримує можливість створення копій (clones) VPC/VPS, розгорнутих на ресурсах хмарного сервісу:»; $\mathbf{S_4}$ = «Рішення підтримує можливість шифрування дискового простору, виділеного під VPC/VPS:»; $\mathbf{S_5}$ = «Рішення відповідає вимогам стандарту FIPS 140-2:»; $\mathbf{S_6}$ = «Рішення відповідає вимогам стандарту PCI-DSS:»; $\mathbf{S_7}$ = «Рішення відповідає вимогам стандарту GDPR:»; $\mathbf{S_8}$ = «Рішення відповідає вимогам стандарту HIPAA/HITECH:»; $\mathbf{S_9}$ = «Рішення відповідає вимогам стандарту FedRAMP:»; $\mathbf{S_{10}}$ = «Інфраструктура постачальника хмарних сервісів відповідає серії стандартів ISO 27000:»

Враховуючи те, що у формулі (7) вказані загальні критерії оцінювання модуля зберігання даних на базі хмарного сервісу у вигляді запитань, то у формулі (8) представлено варіанти відповідей:

$$\begin{aligned} \mathbf{S} = \left\{ \bigcup_{j=1}^{10} \mathbf{S_j} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{3j}} S_{jk} \right\} \right\} = \{ \{S_{11}, S_{12}\}, \\ \{S_{21}, S_{22}\}, \{S_{31}, S_{32}\}, \{S_{41}, S_{42}\}, \{S_{51}, S_{52}\}, \\ \{S_{61}, S_{62}\}, \{S_{71}, S_{72}\}, \{S_{81}, S_{82}\}, \{S_{91}, S_{92}\}, \\ \{S_{101}, S_{102}\}\}, \end{aligned} \quad (8)$$

де: S_{11} = «Так»; S_{12} = «Ні»; S_{21} = «Так»; S_{22} = «Ні»; S_{31} = «Так»; S_{32} = «Ні»; S_{41} = «Так»; S_{42} = «Ні»; S_{51} = «Так»; S_{52} = «Ні»; S_{61} = «Так»; S_{62} = «Ні»; S_{71} = «Так»; S_{72} = «Ні»; S_{81} = «Так»; S_{82} = «Ні»; S_{91} = «Так»; S_{92} = «Ні»; S_{101} = «Так»; S_{102} = «Ні» [15].

Варто врахувати, що підпараметри S_{11} та S_{41} мають власні уточнюючі запитання по даному модулю, то оновлений варіант модуля представлено у формулі (9):

ISSN 2663 – 4023

$$\mathbf{S} = \left\{\bigcup_{j=1}^{10} \mathbf{S}_{\mathbf{j}}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{3j}} S_{jk}\right\}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{3j}}\left\{\bigcup_{l=1}^{m_{3jk}} \mathbf{S}_{\mathbf{jkl}}\right\}\right\}\right\} =$$

$$\{\{\{\mathbf{S}_{\mathbf{111}}, \mathbf{S}_{\mathbf{112}}, \mathbf{S}_{\mathbf{113}}, \mathbf{S}_{\mathbf{114}}\}, S_{12}\}, \{S_{21}, S_{22}\}, \{S_{31}, S_{32}\},$$
$$\{\{\mathbf{S}_{\mathbf{411}}, \mathbf{S}_{\mathbf{412}}, \mathbf{S}_{\mathbf{413}}, \mathbf{S}_{\mathbf{414}}, \mathbf{S}_{\mathbf{415}}\}, S_{42}\}, \{S_{51}, S_{52}\}, \{S_{61}, S_{62}\},$$
$$\{S_{71}, S_{72}\}, \{S_{81}, S_{82}\}, \{S_{91}, S_{92}\}, \{S_{101}, S_{102}\}\}, \quad (9)$$

де: $\mathbf{S}_{\mathbf{111}}$ = «Рішення підтримує локальну реплікацію (Local Replication) в тому ж регіоні, що і знаходиться VPC/VPS:»; $\mathbf{S}_{\mathbf{112}}$ = «Рішення підтримує регіональну реплікацію (Regional Replication), в мінімум ніж 2-х інших містах, окрім тих, де розташовані VPC/VPS:»; $\mathbf{S}_{\mathbf{113}}$ = «Рішення підтримує GEO-розподілену реплікацію (Geo-Redundant Replication), в мінімум ніж 2-х інших країнах, окрім тих, де розташовані VPC/VPS:»; $\mathbf{S}_{\mathbf{114}}$ = «Виберіть який метод реплікації підтримує хмарний сервіс:»; $\mathbf{S}_{\mathbf{411}}$ = «Представники постачальника хмарних сервісів мають доступ до наповнення шифрованого дискового простору:»; $\mathbf{S}_{\mathbf{412}}$ = «Вкажіть, ким забезпечується управління ключами шифрування дискового простору:»; $\mathbf{S}_{\mathbf{413}}$ = «Рішення має готовий функціонал управління та зберігання ключів шифрування:»; $\mathbf{S}_{\mathbf{414}}$ = «Вкажіть метод шифрування, що використовується хмарним сервісом:»; $\mathbf{S}_{\mathbf{415}}$ = «Рішення підтримує метод симетричного шифрування не нижче ніж AES-256:» [16].

Оскільки в формулі (9) представлено додаткові критерії для модуля оцінювання стану захищеності середовища зберігання даних то в формулі (10) представлено розширені набори відповідей:

$$\mathbf{S} = \left\{\bigcup_{j=1}^{10} \mathbf{S}_{\mathbf{j}}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{3j}} S_{jk}\right\}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{3j}}\left\{\bigcup_{l=1}^{m_{3jk}} \mathbf{S}_{\mathbf{jkl}}\right\}\right\}\right\} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{3j}}\left\{\bigcup_{l=1}^{m_{3jk}}\left\{\bigcup_{p=1}^{m_{3jkl}} S_{jklp}\right\}\right\}\right\}\right\} =$$

$$\{\{\{\{S_{1111}, S_{1112}\}, \{S_{1121}, S_{1122}\}, \{S_{1131}, S_{1132}\}, \{S_{1141}, S_{1142}, S_{1143}, S_{1144}\}\}, S_{12}\},$$
$$\{S_{21}, S_{22}\}, \{S_{31}, S_{32}\}, \{\{\{S_{4111}, S_{4112}\}, \{S_{4121}, S_{4122}, S_{4123}\}, \{S_{4131}, S_{4132}\},$$
$$\{S_{4141}, S_{4142}, S_{4143}, S_{4144}\}, \{S_{4151}, S_{4152}\}\}, S_{42}\}, \{S_{51}, S_{52}\}, \{S_{61}, S_{62}\},$$
$$\{S_{71}, S_{72}\}, \{S_{81}, S_{82}\}, \{S_{91}, S_{92}\}, \{S_{101}, S_{102}\}\}, \quad (10)$$

де: S_{1111} = «Так»; S_{1112} = «Ні»; S_{1121} = «Так»; S_{1122} = «Ні»; S_{1131} = «Так»; S_{1132} = «Ні»; S_{1141} = «Synchronous Replication»; S_{1142} = «Asynchronous Replication»; S_{1143} = «Всі вище перелічені»; S_{1144} = «Жодного зі вище перелічених»; S_{4111} = «Так»; S_{4112} = «Ні»; S_{4121} = «Постачальником»; S_{4122} = «Замовником»; S_{4123} = «Постачальником і замовником»; S_{4131} = «Так»; S_{4132} = «Ні»; S_{4141} = «Симетричне шифрування»; S_{4142} = «Асиметричне шифрування»; S_{4143} = «Симетричне та асиметричне шифрування»; S_{4151} = «Так»; S_{4152} = «Ні» [16].

Для можливості візуального представлення модуля оцінювання стану захищеності середовища зберігання даних, а саме розроблених критерії оцінювання та представлення послідовних кроків проведення оцінювання було розроблено алгоритмічне забезпечення, що представлено на Рисунку 2:

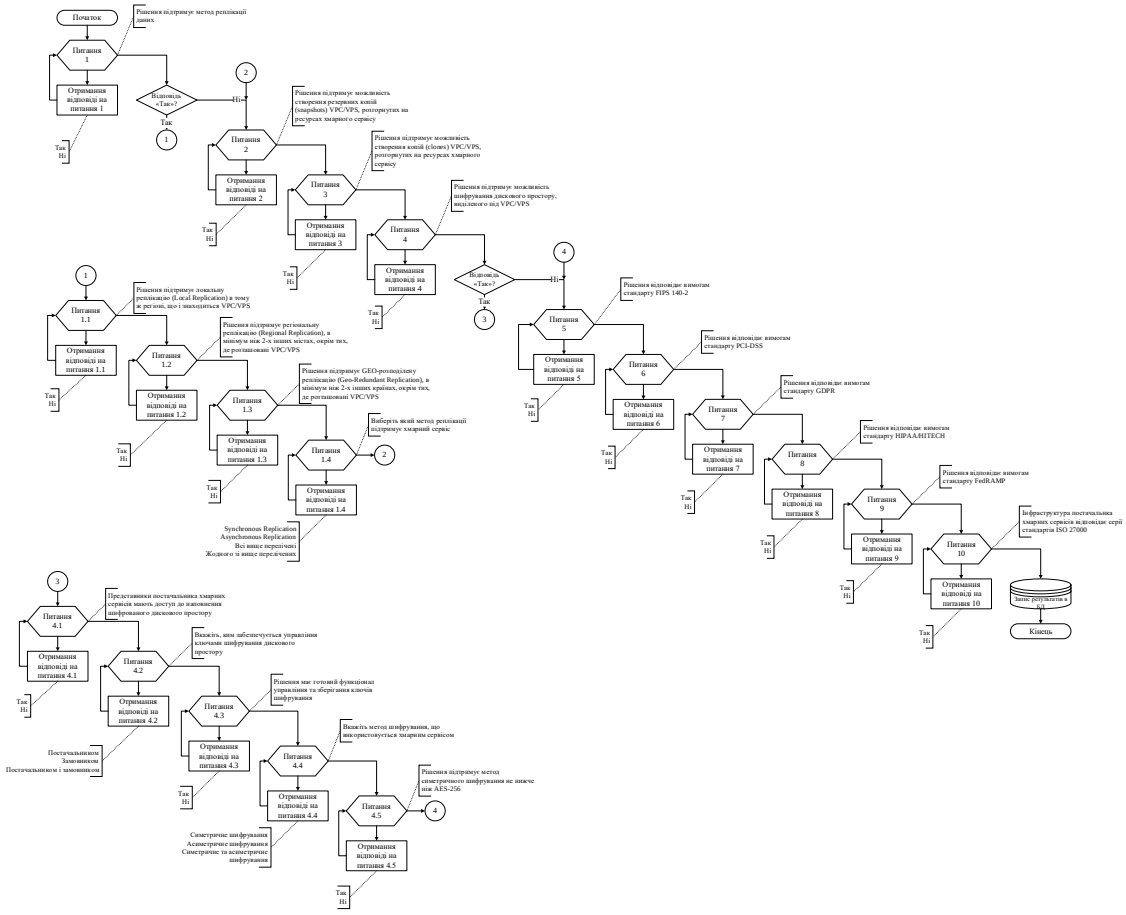

Рис. 2. Загальна структура параметру «S» для оцінювання стану захищеності середовища зберігання даних

Обидва модулі оцінювання стану захищеності мережі хмарного сервісу та середовища зберігання даних є обов'язковими складовими процесу оцінювання для оцінюваних типів хмарних сервісів (IaaS, PaaS, CaaS, FaaS, SaaS) і забезпечують системний підхід до аналізу критичних з точки зору кібербезпеки компонентів хмарних провайдерів послуг та інфраструктури.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У даній роботі розроблено критерії та метод оцінювання стану захищеності мережі хмарного сервісу (параметр N) і середовища зберігання даних (параметр S) як ключових лінійних компонентів системи оцінювання кібербезпеки хмарних сервісів. Модулі створено на основі узагальненої математичної моделі оцінювання стану кіберзахисту хмарних сервісів і призначені для кількісного визначення рівня захищеності мережевої інфраструктури та систем зберігання даних. Для обох розроблених модулів оцінювання розроблено критерії оцінювання із визначеними запитання та варіантами відповідей. Розроблено алгоритмічні моделі обох модулів, що забезпечують візуальне представлення процесу оцінювання. Отримані значення параметрів N і S впливають на формування інтегрального показника кіберзахищеності та фінальної рекомендації щодо використання хмарного сервісу. Подальші дослідження спрямовані на розробку методу оцінювання, визначення ваги кожної із відповідей, розробку рекомендацій та створення захищеного мережевого застосунку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Datadog. (n.d.). *State of cloud security*. https://www.datadoghq.com/state-of-cloud-security/

2. Gartner. (n.d.). *Cloud security requires refined incident response strategies.* https://www.gartner.com/en/documents/5400963
3. Cloud Security Alliance. (n.d.). *Security guidance for cloud computing v5*. https://cloudsecurityalliance.org/artifacts/security-guidance-v5
4. National Institute of Standards and Technology. (2020). *Security guidelines for storage infrastructure* (NIST Special Publication 800-209). https://csrc.nist.gov/pubs/sp/800/209/final
5. Kentik. (2026). *DDoS protection and mitigation: A 2026 guide to defending modern networks*. https://www.kentik.com/kentipedia/ddos-protection/
6. Microsoft. (n.d.). *Microsoft cloud security benchmark: Network security*. Microsoft Learn. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security
7. Tafani-Dereeper, C. (2025). *Key learnings from the 2025 State of Cloud Security study*. Datadog. https://www.datadoghq.com/blog/cloud-security-study-learnings-2025/
8. Amazon Web Services. (n.d.). *Encryption best practices for AWS services*. AWS Prescriptive Guidance. https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/services-best-practices.html
9. Google Cloud. (n.d.). *Cloud Storage threat model report*. Google Cloud Documentation. https://docs.cloud.google.com/docs/security/threat-model/storage-threat-model
10. National Institute of Standards and Technology. (n.d.). *Security guidelines for storage infrastructure* (NIST Special Publication 800-209 Rev. 1, Initial Public Draft). https://csrc.nist.gov/pubs/sp/800/209/r1/ipd
11. Wiz. (n.d.). *How to evaluate CSP security: A checklist*. https://www.wiz.io/academy/cloud-security/how-to-evaluate-cloud-service-provider-security
12. Microsoft. (n.d.). *Microsoft cloud security benchmark: Data protection*. Microsoft Learn. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection
13. Pedchenko, Y. M. (2025). *Methods and models for assessing the cybersecurity state of cloud services of information infrastructure objects* [Doctoral dissertation, Kyiv]. https://vchenarada.nau.edu.ua/wp-content/uploads/2025/05/Disertatsiya_Pedchenko_YEM_125_Kiberbezpeka.pdf
14. Ivanchenko, Y., et al. (2025). The mathematical method for assessing the cybersecurity state of cloud services. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska*, *15*(4), 137–141. https://doi.org/10.35784/iapgos.7555
15. Pedchenko, Y., Shulha, V., Korchenko, O., Ivanchenko, Y., Vyshnevska, N., & Petrovska, M. (2024). Mathematical model of security cloud services assessment. In S. Semenov & M. Muchacki (Eds.), *Problems of scientific, technical and legal support for cybersecurity in the modern world* (pp. 13–21). Krakow. https://doi.org/10.24917/9788668020861
16. Pedchenko, Y. M., & Ivanchenko, I. S. (2024). Model of a secure network application for assessing the cybersecurity of cloud service providers. *Scientific Notes of the State University of Information and Communication Technologies*, *6*(2), 116–134. https://doi.org/10.31673/2518-7678.2024.025842

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Yevhenii M. Pedchenko
Doctor of Philosophy, Associate Professor
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-8436-5792
e.pedchenko@duikt.edu.ua

Yevheniia V. Ivanchenko
Doctor of Technical Sciences, Professor, Director of Institute
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-3017-5752
e.ivanchenko@duikt.edu.ua

Ihor S. Ivanchenko
Candidate of Technical Sciences, Associate Professor, Professor
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-3415-9039
i.ivanchenko@duikt.edu.ua

Maryna M. Pedchenko
Student
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0007-8743-1821
st9763427@stud.duikt.edu.ua

METHODS FOR ASSESSING THE SECURITY STATE OF NETWORKS AND DATA STORAGE ENVIRONMENTS IN CLOUD SERVICES

Abstract. The conducted research presents the criteria and method for assessing the security state of cloud service networks and data storage environments as key linear components of the cloud services cybersecurity assessment system. The study is based on the developed generalized mathematical model for assessing the cybersecurity state of cloud services of information infrastructure objects. The relevance of the problem related to the growing number of cyber incidents in cloud environments caused by configuration errors during the setup of cloud services is substantiated. It is demonstrated that the network level and the data storage environment are critical components of cloud infrastructure. The analysis of existing international standards and regulations on cloud service protection revealed the absence of clear recommendations. In the presentation of the research results, the module for assessing the network security state (parameter N) and the module for assessing the data storage environment security state (parameter S) were formalized. For each module, assessment criteria, answer options, and corresponding mathematical formulas were defined that detail the scope of assessment for each cloud service. Algorithmic models were developed for both modules to provide a visual representation of the structure of criteria for assessing the security level of cloud services. It is shown that the obtained values of parameters N and S influence the formation of the cybersecurity level of a cloud service and the final recommendation regarding its further use by business. The study notes the possibility of practical application of the developed criteria and methods, while all further research is aimed at developing a comprehensive assessment method, determining weighting coefficients for the answers received from auditors, forming a recommendation system, and creating a secure web application.

Keywords: cybersecurity; information security; model; method; audit; cloud service assessment; algorithmic support; network; data storage.

REFERENCES

1. Datadog. (n.d.). *State of cloud security*. https://www.datadoghq.com/state-of-cloud-security/
2. Gartner. (n.d.). *Cloud security requires refined incident response strategies.* https://www.gartner.com/en/documents/5400963

3. Cloud Security Alliance. (n.d.). *Security guidance for cloud computing v5*. https://cloudsecurityalliance.org/artifacts/security-guidance-v5
4. National Institute of Standards and Technology. (2020). *Security guidelines for storage infrastructure* (NIST Special Publication 800-209). https://csrc.nist.gov/pubs/sp/800/209/final
5. Kentik. (2026). *DDoS protection and mitigation: A 2026 guide to defending modern networks*. https://www.kentik.com/kentipedia/ddos-protection/
6. Microsoft. (n.d.). *Microsoft cloud security benchmark: Network security*. Microsoft Learn. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security
7. Tafani-Dereeper, C. (2025). *Key learnings from the 2025 State of Cloud Security study*. Datadog. https://www.datadoghq.com/blog/cloud-security-study-learnings-2025/
8. Amazon Web Services. (n.d.). *Encryption best practices for AWS services*. AWS Prescriptive Guidance. https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/services-best-practices.html
9. Google Cloud. (n.d.). *Cloud Storage threat model report*. Google Cloud Documentation. https://docs.cloud.google.com/docs/security/threat-model/storage-threat-model
10. National Institute of Standards and Technology. (n.d.). *Security guidelines for storage infrastructure* (NIST Special Publication 800-209 Rev. 1, Initial Public Draft). https://csrc.nist.gov/pubs/sp/800/209/r1/ipd
11. Wiz. (n.d.). *How to evaluate CSP security: A checklist*. https://www.wiz.io/academy/cloud-security/how-to-evaluate-cloud-service-provider-security
12. Microsoft. (n.d.). *Microsoft cloud security benchmark: Data protection*. Microsoft Learn. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection
13. Pedchenko, Y. M. (2025). *Methods and models for assessing the cybersecurity state of cloud services of information infrastructure objects* [Doctoral dissertation, Kyiv]. https://vchenarada.nau.edu.ua/wp-content/uploads/2025/05/Disertatsiya_Pedchenko_YEM_125_Kiberbezpeka.pdf
14. Ivanchenko, Y., et al. (2025). The mathematical method for assessing the cybersecurity state of cloud services. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska*, *15*(4), 137–141. https://doi.org/10.35784/iapgos.7555
15. Pedchenko, Y., Shulha, V., Korchenko, O., Ivanchenko, Y., Vyshnevska, N., & Petrovska, M. (2024). Mathematical model of security cloud services assessment. In S. Semenov & M. Muchacki (Eds.), *Problems of scientific, technical and legal support for cybersecurity in the modern world* (pp. 13–21). Krakow. https://doi.org/10.24917/9788668020861
16. Pedchenko, Y. M., & Ivanchenko, I. S. (2024). Model of a secure network application for assessing the cybersecurity of cloud service providers. *Scientific Notes of the State University of Information and Communication Technologies*, *6*(2), 116–134. https://doi.org/10.31673/2518-7678.2024.025842

Отримано редакцією журналу / Received: 07.03.26
Прорецензовано / Revised: .25.03.26
Схвалено до друку / Accepted: 24.09.26